Resilienz dank Digitalisierung

– für Bund, Länder und Kommunen –

Impulse zur Verwaltungsdigitalisierung aus den Kongressen und Online-Veranstaltungen des Behörden Spiegel

Behörden Spiegel

1.000 FRAGEN AN DIE ZUKUNFT
Nr. 495

WELCHE SEITE HAT DIE ZUKUNFT?

Die Zukunft hat viele Seiten. Wir kennen sie alle. Bei Bechtle unterstützen über 13.000 Kolleginnen und Kollegen in Deutschland und ganz Europa Unternehmen, Bildungseinrichtungen, das Gesundheitswesen und andere öffentliche Auftraggeber bei dem, was sie heute brauchen und was morgen wichtig wird. Von Digitalisierung bis Cloud, von Mobility bis ITSecurity finden wir immer den besten Weg. Nämlich den, der Sie voranbringt. Denn mit der Zukunft kennen wir uns aus – als größtes deutsches ITSystemhaus und ITZukunftspartner in Ihrer Nähe.

Kontakt:
Bechtle ITSystemhaus Bonn/Köln
Telefon: +49 228 68880
E-Mail: bonn@bechtle.com

bechtle.com

Ihr starker IT-Partner.
Heute und morgen.

BECHTLE

Leitbild und Standards

Resilienz braucht Plan und Flexibilität

Dr. Eva-Charlotte Proll
Herausgeberin und
CDO Behörden Spiegel

2022 waren zu Jahresbeginn viele Stakeholder auf Bundes- und Landesebene positiv gestimmt, was das Erreichen der Umsetzungsfrist des OZG betraf. Einzig die Kommunen beklagten von Anfang an einen falschen Ansatz bei der Finanzierung und mangelndes Verständnis für die kommunalen Realitäten. Der Ukraine-Krieg überraschte zur zweiten Hälfte des ersten Quartals und mit ihm nahm (neben der Bedeutung einer Zeitenwende für die deutsche Sicherheitspolitik) das Bewusstsein für Cyber-Risiken zu. Zahlreiche Angriffe auf Kritische Infrastrukturen und Verwaltungen zeigten jedoch, dass ein Großteil staatlicher Akteure nicht unmittelbar nach einer Cyber-Attacke wieder handlungsfähig war. Wegen Corona war ein Austausch innerhalb und außerhalb von Verwaltungen von Angesicht zu Angesicht erst im Frühling 2022 wieder möglich. Der Digitale Staat 2022 (mehr dazu lesen Sie ab Seite 12) brach als erstes das Eis der Videokonferenzen. Im persönlichen Austausch konnte die Verwaltung alle aus den vorvergangenen zwei Jahren angestauten Themen adressieren. Die Notwendigkeit einer digital erreichbaren und digital arbeitenden Verwaltung schien offensichtlich.

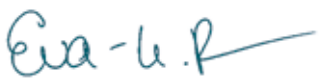
Mittlerweile können wir sicher sagen: Die Ziele des OZG wurden verfehlt, so auch die des OZG-Boosters, bei der Finanzierung musste nachgebessert werden. Die Gremien zur Steuerung der Verwaltungsdigitalisierung sollen einer Neuaufstellung unterzogen werden. Registermodernisierung, eID, besserer Datenaustausch im Gesundheitssektor, der Aufbau eines digitalen Immunsystems in Sachen Cyber-Sicherheit und eine OZG-Novelle beschäftigen die Verwaltungen landauf und -ab auch in diesem Jahr. Beim Thema Cloud sind die Erwartungen hoch. Neue Projekte, eine strategische Vorausschau und ein damit verbundenes Betriebskonzept auf der Basis von Standards für die Verwaltungsdigitalisierung müssen 2023 identifiziert und erarbeitet werden.

Resilient zu sein, erfordert zwar Pläne und verlässliche Strukturen, aber Verwaltung muss auch auf Unvorhersehbares reagieren können. Zahlreiche Herausforderungen zu identifizieren, Evaluationen anzustoßen und Konzepte zur Weiterentwicklung zu initiieren – das bietet der Austausch bei unseren Kongressen und Veranstaltungen. Er erlaubt, Impulse zur Verwaltungsdigitalisierung zu setzen. Ich freue mich daher sehr, Ihnen mit der vorliegenden Publikation einen Einblick in unser breit gefächertes Themen- und Veranstaltungsspektrum geben zu können.

Neben ganzjährigen Online-Veranstaltungen auf unseren Plattformen www.digitalerstaat.online und www.neuestadt.org gibt es die Regionalkongresse, die wir auch 2023 durchführen. Dies sind der „Zukunftskongress Bayern“, „Baden-Württemberg 4.0“, „Digitale Verwaltung Rheinland-Pfalz“, „Nordl@nder Digital“, „e-nrw“ und „HEssenDIGITAL“ sowie der „CyberSicherheitsTag Niedersachsen“ und der „IT-Sicherheitstag“ im Freistaat Sachsen. Dazu kommen die überregionalen Kongresse „Digitaler Staat“ und „Public IT-Security“ (PITS).

All diese Veranstaltungen werden auch 2023 für Expertinnen und Experten der Verwaltungsdigitalisierung sowie Interessierte wieder inhaltliche Highlights und Begegnungsmöglichkeiten bieten.

Ich freue mich darauf, vielen von Ihnen bei unseren Veranstaltungen – ob virtuell oder persönlich – begegnen zu dürfen. Nun wünsche ich Ihnen eine angenehme und erkenntnisreiche Lektüre.



Inhalt

6 Auf die Kommunen kommt es an
Es braucht Unterstützung und eine EfA-Weiterentwicklung

8 Amberg und der Weg zur Smart City
Breite Vernetzung notwendig

10 Mehr Tempo aufnehmen
Mit dem DigitalStore Online-Services in die Fläche bringen

12 Kritik in beide Richtungen
Kommunen im Fokus der OZG-Umsetzung

14 Resiliente Clouds für die Verwaltung
Innovationen finden in der Cloud statt

16 Digitale Verwaltung im Aufbruch
Rückblick auf den Vorsitz im IT-Planungsrat 2022

18 Künstliche Intelligenz massenhaft
Der Weg vorwärts für die öffentliche Verwaltung

19 Alle mitnehmen
Digitalisierung selbst macht noch keine smarte Stadt

20 Basis moderner Verwaltung
Welche Herausforderungen bietet die E-Akte?

22 Es kommt auf die Standards an
Wie der Staat leistungsfähiger und intelligenter werden kann

24 Kulturwandel dringend benötigt
Hilft der Generationenwechsel?

26 Mehr Mut zur Veränderung
Gießkannen-Förderung wird kritisiert

28 Schwerpunkte für das Vorsitzjahr 2023
Handlungsfähigkeit sicherstellen

30 Gemeingefährliche IT-Sicherheitsmuffel
Der menschliche Faktor

32 Eine Lücke geschlossen …
… tausend neue geöffnet

34 Live-Hackings für Schülerinnen und Schüler
Sächsische Staatsregierung sensibilisiert für IT-Sicherheit

36 Es brodelt im Kessel
Nur punktuelle Einigkeit zwischen Land und Kommunen

38 Smarte Infrastruktur im Ländle
Wie sie gelingt und was sie verhindert

40 Positive Bilanz von digital@bw
Prävention und Kooperation zentrale Bausteine der Cyber-Sicherheit

42 Vom Bund ins Land und in die Kommune
(Sichere) digitale Verwaltung für alle

43 Digital und kommunal?
Best Practice, Denkanstöße und Problemerörterungen

44 Kommunale IT wird geprüft
Es besteht starker Nachholbedarf

45 Oder Licht aus
Richter fordert mehr Kooperation für mehr IT-Sicherheit

46 Ausbau der Cyber-Sicherheitsarchitektur
Niedersachsen plant robustes Cyber-Sicherheitszentrum

48 Es ist immer noch der Anwender
Cyber-Risiken entstehen zum Großteil vor dem Computer

50 Fehlerkultur und Vertrauen entscheidend
Auch interdisziplinäres Arbeiten fördern

52 Denkmodell Netzwerkkommune
Digitale Daseinsvorsorge im Fokus

54 OZG-Finanzierungsdebatte
Unklarheiten deutlich erkennbar

56 Gelebte Transformation
Mit effizienten Strukturen und Prozessen zum Erfolg

58 Enormer Vertrauensverlust droht
Kommunen im Fadenkreuz von Cyber-Kriminellen

60 Einer muss sagen: „Jetzt alle raus!“
Zwei Grundgesetzänderungen zum Preis von einer

62 Computerhirne für Behörden
Ist KI in der Verwaltung eine Chance oder Herausforderung?

63 Wir müssen es habitualisieren
Wie die digitale Selbstverteidigung gestärkt werden kann

64 Gemeinsam stark sein
Wie kann sich Deutschland gegen Attacken aus dem Cyber-Raum schützen?

66 Hohe Anfälligkeit
Cyber Security als ungelöstes Problem

68 Verschiedene Ebenen der IT-Sicherheit
Nur weil es Compliance gibt, wird nicht sicher gehandelt!

70 Resilienz im Fokus
Sozialer Aspekt muss mitgedacht werden

72 Zukunft nach dem OZG
Es muss noch viel getan werden

73 Eine gute Bilanz
Neuer Ressortzuschnitt hat sich bewährt

76 „Deutschland kann Krise!“
Qualität schafft Vertrauen – Vertrauen schafft Nutzung

80 Unverhofft digital kommt nur einmal
Ein Erfahrungsbericht aus der digitalen Modellkommune Soest

82 Impressum

83 Veranstaltungsübersicht 2023

CAk
Cyber Akademie

Sind Sie da sicher?

IT-Sicherheit und Datenschutz im Jahre 2023:
Entdecken Sie unsere neuen Seminare
zu diesen und anderen Themen auf

www.cyber-akademie.de

8. Zukunftskongress Bayern

Oans, Zwoa, Zack, OZG is!

Mit neuem Schwung in die digitale Verwaltung

17. Februar 2022

www.zukunftskongress.bayern #zkonbayern22

ZUKUNFTSKONGRESS BAYERN

Auf die Kommunen kommt es an

Es braucht Unterstützung und eine EfA-Weiterentwicklung

⟩⟩⟩ von **Matthias Lorenz,** Behörden Spiegel

„2022 ist ein entscheidendes Jahr für die Verwaltungsdigitalisierung“ – so drückte es Judith Gerlach, bayerische Staatsministerin für Digitales und Schirmherrin des Zukunftskongresses Bayern, zu Beginn des Online-Events aus. Denn: Man befinde sich inzwischen auf der Zielgeraden des Onlinezugangsgesetzes (OZG), dessen Umsetzungsfrist Ende des Jahres 2022 abgelaufen ist. Doch wie war in Bayern der Stand der Umsetzung zum Zeitpunkt des Kongresses?

Was die Digitalisierung der Leistungen angeht, sah Gerlach Bayern auf einem guten Weg: „Was den Freistaat anbelangt, werden wir alle für das OZG relevanten staatlichen Leistungen bis Ende 2022 digitalisiert haben.“ Die Ministerin identifizierte als größte Herausforderung die Flächendeckung. Der Erfolg des OZG entscheide sich auf der kommunalen Ebene. Die Kommunen müssten bei der Umsetzung nun mitziehen. Um einen weiteren Ansporn zu geben, habe man die Auszeichnung „Digitales Amt“ ins Leben gerufen, die Kommunen erhielten, die mindestens 50 Leistungen digital anböten.

Unterstützungsangebote für Kommunen

Dr. Vanessa Greger, die im Bayerischen Staatsministerium für Digitales (StMD) die Abteilung „Digitale Verwaltung, Onlinezugangsgesetz, Identitätsmanagement“ leitet, beschrieb weitere Maßnahmen, mit denen der Freistaat die Kommunen bei der OZG-Umsetzung unterstützt. Neu etabliert habe man zum Beispiel OZG-Checklisten sowie ein „OZG-Monitoring“, mit welchem die Kommunen immer den aktuellen Umsetzungsstand einzelner Leistungen verfolgen könnten. Außerdem gebe es mit dem „BayernLOZe“ einen Leitfaden zur OZG-Umsetzung. Des Weiteren habe man zentral In-

formationsveranstaltungen durchgeführt, die sehr gut angenommen worden seien. Immer drängender wurde im Kontext der Umsetzung jedoch die Frist Ende 2022. Schon Anfang des Jahres 2022 warnten den meisten OZG-Verantwortlichen mehr oder weniger deutlich, dass sie die Einhaltung der Frist für unrealistisch halten. Doch wie könnte man auf diese Situation reagieren? An diesem Punkt sah Dr. Greger vor allem die Herausforderung, die kommunalen Leistungen, welche den Großteil der OZG-Leistungen ausmachten, in die Fläche zu kriegen. „Das bedeutet, dass hier priorisiert werden muss", schlussfolgerte die Abteilungsleiterin. Das Motto der Priorisierung sollte laut Dr. Greger „Konzentration auf das, was gefragt ist" lauten. Heißt: Der Fokus müsse jetzt auf Leistungen mit einer großen Wirkorientierung gelegt werden. „Es gibt viele Leistungen, die gar kein Digitalisierungspotenzial haben", erklärt Greger. Als Beispiel nennt sie Leistungen, die nicht in jeder Kommune angeboten würden (Stichwort Anwohnerparkausweis) oder solche, die nur eine geringe Nachfrage hätten. „Diese Leistungen kann man getrost erst mal hintenanstellen", so Greger.

Trotzdem stellt gerade die OZG-Umsetzung die Kommunen weiterhin vor große Herausforderungen, wie auf dem Kongress durch Chatbeiträge und Aussagen von Kommunalvertretern deutlich wurde. Thomas Bönig, ehemaliger CIO/CDO der Landeshauptstadt München, kritisierte das Gesetz scharf: „Das OZG geht zulasten der Kommunen." Schließlich schreibe es ja gerade nicht die Digitalisierung der Verwaltung vor, sondern nur die der Antragsstellung. München setze deswegen auf eine eigene Digitalisierungsplattform. Auch Olaf Kuch, Leiter des Direktoriums für Bürgerservice, Digitalisierung und Recht der Stadt Nürnberg, hält das OZG nicht für eine „echte Digitalisierung". Deswegen betrachte man in Nürnberg bei der Digitalisierung von Leistungen immer den gesamten Prozess. „Die Prozessveränderung muss immer von Anfang an mitgedacht werden, ansonsten bauen wir altbackene analoge Prozesse einfach nur mühsam digital nach", warnte Kuch. Auch versuche man, direkt die Fachverfahren mit einzubinden, was sich aber unter anderem aufgrund der starken Auslastung der Fachverfahrenshersteller als eine große Herausforderung darstelle.

Kritik an EfA

Die Beispiele aus München und Nürnberg zeigen: Kommunen wurden selbst aktiv, weil ihnen die Vorgaben des OZG nicht weit genug gingen oder sie diese sogar kontraproduktiv fanden. Dies widerspricht teilweise dem Einer-für-Alle (EfA)-Prinzip, welches dafür sorgen soll, dass Leistungen möglichst einheitlich sind und nicht jeder alle Leistungen selbst digitalisiert. Während Bönig große Zweifel an dem Konzept äußert, sieht Ministerin Gerlach EfA zumindest für Bereiche, in denen es eine große Einheitlichkeit braucht, positiv. „Bei diesen Leistungen ist EfA super." Als Beispiel nannte die CSU-Politikerin das Unternehmenskonto. Da Unternehmen meist deutschlandweit agierten und einen Single Point of Contact bräuchten, sei es unsinnig, wenn jedes Land eine eigene Lösung baue.

Was folgt?

Trotzdem meinte auch Gerlach: „Das EfA-Prinzip sorgt bei Kommunen für Verunsicherung." Dies liege zu einem großen Teil daran, dass es nicht klar sei, wie es nach 2023 weitergehe. Stichwort ist hier die Folgefinanzierung, also die Frage, wie man Betrieb und Wartung einer Leistung regelt, falls man eine Leistung als Nachnutzer im Sinne des EfA-Prinzips übernimmt. Hier, so Gerlachs Forderung, müsse der Bund klare Regelungen treffen. Vom „Dogma EfA", so die Ministerin, müsse man sich ein Stück weit lösen und mehr Flexibilität zulassen. E-Government sei zu 90 Prozent kommunal und damit sehr heterogen. „In diesen Bereichen wird es sehr schwierig, eine komplette Vereinheitlichung zu erreichen", analysiert Gerlach. Gerlach plädiert deswegen dafür, das EfA-Prinzip in diesen Fällen durch andere Nachnutzungsmodelle abzulösen, etwa unter dem Stichwort „Einer-für-viele".

Derweil muss auch die Frage diskutiert werden, wie es nach dem OZG weitergeht. StMD-Abteilungsleiterin Greger sagt, man werde viele Erkenntnisse aus dem OZG mitnehmen und in einem Nachfolgegesetz fortschreiben. Hier würden dann die Weichen in Richtung Ende-zu-Ende, Registermodernisierung und weiterer Aspekte gestellt. Laut Ansicht vieler Expertinnen und Experten ist es für diese Weichenstellung auch höchste Zeit. „Bis jetzt wird meist nur der Online-Zugang gesehen", kritisiert etwa Torsten Frenzel von der Stabstelle Digitale Verwaltung der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB). Je mehr Fachverfahren allerdings in eine digitale Leistungsbearbeitung integriert würden oder je sauberer die digitalen Prozesse an sich gestaltet würden, desto mehr Vorteile bringe die Digitalisierung auch für die Verwaltungsmitarbeitenden selbst.

Bei der AKDB arbeitet man laut Frenzel deswegen bereits an sogenannten „GenerationM- Fachdiensten". Für diese werde es kein eigenes Portal mehr brauchen, vielmehr könnten sie beliebig in Websites oder andere Portale eingebunden werden, kündigt Frenzel an. Des Weiteren könnten die Kunden diese Fachdienste individuell nach ihren Vorstellungen konfigurieren, sowohl in den Bereichen Layout/Design als auch Text. Alle GenerationM-Fachdienste würden EfA-konform umgesetzt, basierten auf Open Source und verfügten über Fachverfahrens-Schnittstellen.

Amberg und der Weg zur Smart City

Breite Vernetzung notwendig

⟩⟩⟩ von **Paul Schubert,** Behörden Spiegel

Um Aushängeschilder für die erfolgreiche Digitalisierung von Kommunen und Städten zu etablieren, können derzeit nur die über die Bundesförderung finanzierten Modellprojekte wirklich durchstarten, den anderen Kommunen fehlt es oft an den finanziellen Kapazitäten – gerade in der Zeit nach der Corona-Pandemie. Smart Citys können als Vorzeigeprojekt dienen und eine große Außenwirkung entwickeln, das gilt für kleinere wie größere Kommunen. Die bayerische Stadt Amberg befindet sich seit 2021 auf dem Weg zur Smart City. Die Voraussetzungen dafür scheinen ideal, aber es gibt noch einige Hürden. Auch die Stadt Regensburg verfolgt einen Smart-City-Ansatz und setzt dabei auf kreative Bürgerbeteiligung.

Amberg ist eine Bildungsstadt und Standort der ostbayerischen technischen Hochschule und bietet mit Studiengängen wie Digital Business, Digital Technology, Digital Healthcare und Künstliche Intelligenz Fächer an, die sich der Entwicklung des Digitalisierungsprozesses und neuer Technologien verschrieben haben. Julia Schönhärl, die Leiterin Smart City der Kreisstadt, sieht die Voraussetzungen für das Modellprojekt als gegeben an: „Wir haben hier flächendeckende Breitbandraten von 50mbit/s und können auch mit der Initiative der nachhaltigen Entwicklungsziele eine gemeinwohnorientierte, nachhaltige Stadtentwicklung anstreben." Als Leiterin des Prozesses möchte Schönhärl die Prozesskosten in der Verwaltung reduzieren und Wirtschaft, Wissenschaft und Verwaltung zusammenschließen – ein Vorgehen, das durch die Smart City gestärkt werden könnte. Besonders wichtig ist Schönhärl die Etablierung von Bürgerbeteiligung als Schlüsselelement – nur so könnten Digitalisierung und Smart City auf die angezielte Akzeptanz stoßen.

Smart City zu werden, hat sich die bayerische Kreisstadt Amberg seit 2021 auf die Fahne geschrieben und sich auf den Weg gemacht. Die Voraussetzungen scheinen gut, auch wenn das Vorgehen unter den üblichen schwierigen Vorzeichen zu leiden scheint.

Foto: BS/Graf Vishenka , stock.adobe.com

Auch Franziska Meier, Smart-City-Koordinatorin der Stadt Regensburg, ordnet Bürgerbeteiligung eine hohe Relevanz zu, wenn es um Smart-City-Ansätze geht. Dabei fordert Meier, die Vernetzung auch vor Ort stattfinden zu lassen und bestimmte Zielgruppen nicht von der Diskussion auszuschließen: „Die Diskussion muss dort stattfinden, wo die Menschen schon jetzt unterwegs sind und bereits kreative Prozesse gestartet haben." In Regensburg sei dafür ein Gestaltungsraum eingerichtet worden, in dem sich Bürgerinnen und Bürger beteiligen könnten und in dem auch Workshops stattfänden. Studierende der Uni Regensburg unterstützen dort das Projekt unter anderem bei der Erprobung eines neuen Partizipationsformates. Des Weiteren merkte die Projektleiterin Schönhärl auf dem Zukunftskongress Bayern an, dass eine traditionell starke Vernetzung als Basis für breit angelegten Austausch und Wissenstransfer auf regionaler, nationaler und internationaler Ebene vonnöten sei: „Denn nur gemeinsam können wir innovative Lösungen für die Stadt finden und das Ganze sozial und insbesondere auch gerecht gestalten."

Noch viele Steine im Weg

Es gebe allerdings einige Herausforderungen, sagte Schönhärl: „Der Mehrwert der Digitalisierung ist landesweit zu wenig transparent kommuniziert. Die Motivation der Akteure zur Nutzung ist viel zu gering. Die BayernApp und das Bayernportal für den digitalen Verwaltungsservice werden nur von einem geringen Prozentsatz der Bevölkerung aktiv genutzt." Auch weil die Registrierung aufwendig sei. Weitere Probleme seien die knappen Ressourcen. Ohne Fördermittel könne der Öffentliche Dienst bei den Gehältern der Fachkräfte kaum mithalten, kritisierte die Projektleiterin auf dem Zukunftskongress. Damit fehlten aktuell die nötigen Kompetenzen zur ganzheitlichen Umsetzung, schlussfolgert Schönhärl: „Die Modelle allein sind nicht ausreichend. Ein flächendeckender Support wäre nötig, insbesondere von kleineren Kommunen." Doch man hat sich auf den Weg gemacht – und Schönhärl kann auf viele engagierte Kolleginnen und Kollegen bauen. Auch wenn sich die meisten sicher erst noch anfreunden müssen, auch „smart" zu nennen, was smart ist. Eine Strategie soll den Mehrwert klar erkennbar machen, den die Verwaltung und die kommunalen Unternehmen haben müssen: „Wir müssen alle Mitarbeitenden mitnehmen", so die Projektleiterin. Zeitnah solle dann die Stadtgesellschaft zur Mitgestaltung eingeladen werden. Schließlich, so äußerte sich Schönharl weiter, müsse man den Nachhaltigkeitsaspekt im Vordergrund sehen: „Ein wichtiger Punkt ist die Vernetzung mit allen relevanten Akteuren des urbanen Ökosystems. Die Smart City muss ein Ziel haben, das werden wir gemeinsam definieren."

VPN und die Cloud

Vereinen Sie maximale Flexibilität mit höchster Sicherheit!

Insbesondere das Thema „Cloud“ hat in den letzten Jahren dazu beigetragen, dass IT-Security-Netzwerke flexibler und digitaler werden. Schlagwörter wie „Zero Trust“, „Single Sign On“ oder „SD-WAN“ scheinen dabei den klassischen VPN-Tunnel immer weiter abzulösen. Doch wieso eigentlich, wenn es doch viel sinnvollere Lösungen gibt?

Wo früher ein einfacher VPN-Server noch das Maß aller Dinge in Sachen professioneller IT-Sicherheit darstellte, steht mittlerweile alles unter dem Zeichen „Cloud“. Der Serverraum weicht vielerorts einem entfernten Rechenzentrum, verwaltet von einem firmenfremden Managed Service Provider. Statt „VPN-Tunnel“ säumen Schlagwörter wie „Zero Trust“, „Single Sign On“ oder „SD-WAN“ die IT-Security-Berichterstattung. Entscheidet man sich allerdings für die richtige Lösung, harmonieren zeitgemäße VPN-Strukturen und digitale Cloud-Technik ganz wunderbar. Mehr noch: Richtig eingesetzt lassen sich sogar ihre jeweiligen Stärken zu einem mächtigen IT-Security-Instrument kombinieren.

Security auf einer neuen Stufe

Damit dies gelingt, müssen vor allem zwei Punkte erfüllt sein: hochsichere Datenkommunikation über einen IPsec-Tunnel und vollständige Kompatibilität mit allen gängigen Cloud-Technologien. Das entsprechende Sicherheitslevel kommt bei einer cloud-integrierten VPN-Lösung durch das Gateway in Verbindung mit einem Management-System zustande. Dieser Zusammenschluss hat zwei große Vorteile: Zum einen werden darüber geleitete Verbindungen IPsec-basiert und somit hochsicher sowie mit voller Geschwindigkeit übertragen. Zum anderen liegt das Gateway nicht direkt in der Cloud, sondern bildet hinter der Firewall eine abgesicherte Umgebung direkt auf dem Server. In puncto Server empfiehlt es sich außerdem, ein Rechenzentrum in Deutschland zu wählen. So erhalten Sie die maximale Transparenz über Ihre Datenflüsse und bewahren Ihre digitale Souveränität ohne Backdoors. Dies ist unter anderem auch in der öffentlichen Verwaltung von entscheidender Bedeutung, da hier täglich mit sensiblen Daten hantiert wird, die für eine digitale Übertragung nicht selten Lösungen mit BSI-Zulassung für VS-NfD vorschreiben.

VPN kann auch Cloud!

Wie eingangs erwähnt, müssen VPNs nicht nur hochsicher sein, sondern sich vor allem nahtlos mit den mittlerweile etablierten Cloud-Services verwenden lassen. Dies ist unter anderem bei den VPN-Lösungen von NCP gegeben, die z. B. mühelos als Teil einer SASE- oder SD-WAN-Infrastruktur eingesetzt werden können. Auch hier stehen Gateway und VPN-Management im Zentrum, die als reine Software-Komponenten auf praktisch jeder Server-Hardware lauffähig sind. Dadurch ist diese Art von VPN bereits von Natur aus „cloudfähig“ und fügen sich auch in komplexe SD-WAN-Verbünde ein. Die Integration in ein SAML-System ist ebenfalls kein Problem. Hier gilt die Authentisierung des Nutzers am SSO-Portal dank des Tunnels dann sowohl für interne Dienste als auch externe Cloudanwendungen. So genießen Administratoren und Nutzer weiterhin alle Vorteile ihrer SAML-Schnittstelle, können Daten allerdings über einen hochsicheren IPsec-Tunnel mit voller Geschwindigkeit übertragen.

Volle Kontrolle dank Zero Trust

Technologien wie SAML/SSO sind oft auch Bestandteil einer übergeordneten Zero-Trust-Strategie, bei der Nutzer durch granulare Firewall-Regeln nur Zugriff auf für sie relevante Anwendungen haben (Least-privilege-Prinzip). Mithilfe einer zentralen Management-Komponente definieren Administratoren alle Zugriffsrechte ihrer Anwender mit wenig Aufwand. Zusätzlich profitieren Sie von einem großen Funktionsumfang der VPN-Software: Der NCP VPN-Bypass oder Split Tunneling helfen dabei, den VPN-Server zu entlasten, indem datenhungrige Anwendungen ohne Sicherheitsrelevanz am Tunnel vorbeigeleitet werden. Für die Sicherheit des gesamten Netzes sind auch Endpoint Policy Checks unerlässlich, die Endgeräte vor jedem Login-Versuch auf vordefinierte Security-Parameter hin überprüft. Stellt das System z. B. veraltete Software auf einem Laptop fest, wird die Verbindung erst nach Abschluss der notwendigen Updates aufgebaut. Da der Administrator sowohl Policies als auch Updates mit wenigen Klicks an einzelne Nutzergruppen oder die gesamte Organisation verteilt, bleiben so auch große Anwenderzahlen immer auf dem neuesten Sicherheitsstand!

Mehr Informationen zu den modernen Cloud-VPN-Lösungen von NCP lesen Sie unter:

Mehr Tempo aufnehmen

Mit dem DigitalStore Online-Services in die Fläche bringen

Die bayerische Digitalministerin Judith Gerlach und der Bayerische Landkreistag stellten im Juli 2022 den DigitalStore vor. Um schneller zusätzliche digitale Verwaltungsleistungen in die Fläche zu bringen, können die bayerischen Landratsämter nun über diese neue Plattform digitale Verwaltungsangebote herunterladen und ihren Bürgerinnen und Bürgern zur Verfügung stellen. Über den DigitalStore sprach Behörden Spiegel-Redakteur Guido Gehrt mit Digitalisierungsministerin Gerlach und Josef Niedermaier, Landrat des Landkreises Bad Tölz-Wolfratshausen. Das Interview wurde im Sommer 2022 geführt.

***Behörden Spiegel:** Was sind die Motivation und die Zielsetzung des DigitalStores?*

Gerlach: Wir müssen digitale Verwaltungsleistungen zum Nutzen der Bürgerinnen und Bürger sowie der Unternehmen in die Fläche bringen. Wir werden nur dann erfolgreich sein, wenn wir den Service für die Menschen verbessern. Mit dem DigitalStore nehmen wir jetzt noch mehr Tempo auf. Unser Fokus liegt hierbei insbesondere auf der Förderung des ländlichen Raums.

Wie ist die Aufgabenverteilung zwischen Digitalministerium und Innovationsring im Projekt?

Gerlach: Wir stellen die finanziellen Mittel und Expertise für den DigitalStore bereit, der Landkreis sorgt für die praktische Umsetzung. Was mich besonders freut: Diese Zusammenarbeit wurde preisgekrönt. Die Jury beim renommierten „eGovernment-Wettbewerb" 2021 unter Schirmherrschaft von Bundesinnenministerin Faeser zeichnete es zum „Besten Kooperationsprojekt" des Jahres aus.

Digitalministerin Judith Gerlach und der Leiter des Innovationsrings des Landkreistags, Josef Niedermaier, Landrat des Landkreises Bad Tölz-Wolfratshausen (rechts), präsentierten gemeinsam mit Thomas Karmasin (links), Landrat des Kreises Fürstenfeldbruck und Präsident des Bayerischen Landkreistages, den DigitalStore der Öffentlichkeit.

Foto: BS/Bayerisches Staatsministerium für Digitales

Wie lange dauerte die Entwicklung, wer war daran beteiligt und wie wird nun der weitere Betrieb organisiert?

Niedermaier: Wir haben das aktuelle Projekt „Digitaler Werkzeugkasten 2.0" im März 2021 gestartet. Gemeinsam mit den 25 Projektlandkreisen wurden bis zum Start des DigitalStores im Juli 2022 bereits 77 Online-Anträge umgesetzt. Die Online-Anträge werden allen bayerischen Landkreisen zur Verfügung gestellt. Mit dem DigitalStore wollen wir die Nachnutzung dieser Online-Anträge vereinfachen und damit auch beschleunigen. Den DigitalStore selbst konnten wir mit dem technischen Dienstleister, der XIMA MEDIA GmbH, innerhalb weniger Monate umsetzen. Der weitere Betrieb des DigitalStores wird vom Innovationsring des Bayerischen Landkreistags koordiniert.

Der DigitalStore wurde im Rahmen des Gesamtprojektes „Digitaler Werkzeugkasten" erarbeitet. Was kennzeichnet dieses Vorhaben und welche weiteren Angebote wurden dort bereits erstellt bzw. sind in Planung?

Niedermaier: Die Digitalisierung fordert die Landratsämter mit ihren zahlreichen Bürger- und Unternehmenskontakten in ganz besonderer Weise. Dieser Kraftakt kann nur gemeinsam gelingen. Mit dem Projekt „Digitaler Werkzeugkasten 2.0" setzen die 25 Projektlandkreise die notwendigen Online-Anträge daher arbeitsteilig und nach nutzerorientierten Standards um. Der Innovationsring des Bayerischen Landkreistags koordiniert das Projekt und stellt die Ergebnisse allen Landkreisen zur weiteren Nachnutzung zur Verfügung. Bei den bereits umgesetzten 77 Online-Anträgen lag der Fokus auf Leistungen für die Bürgerinnen und Bürger.

In welchem Verhältnis steht der DigitalStore zum Fit-Store der FITKO bzw. zum Marktplatz von govdigital? Ist er als Konkurrenz oder komplementäres Angebot zu verstehen?

Gerlach: Der DigitalStore soll die Digitalisierung der kommunalen Verwaltung in Bayern erleichtern. Der FitStore und der Marktplatz von govdigital dagegen dienen dem Austausch von digitalen Leistungen zwischen den verschiedenen Bundesländern. Dementsprechend ist der DigitalStore ein komplementäres Angebot, da es dabei ausschließlich um die innerbayerische Nutzung geht.

Bislang sind am DigitalStore ausschließlich Landkreise beteiligt. Ist geplant, dieses Angebot auch auf andere Kommunen auszuweiten?

Niedermaier: Mit dem Gesamtprojekt „Digitaler Werkzeugkasten" setzen wir Online-Leistungen aus dem Aufgabenbereich der Landratsämter um. Diese können auch für die bayerischen Städte interessant sein. Wir haben den DigitalStore daher von Beginn an so eingerichtet, dass die Leistungen auch von interessierten bayerischen Städten nachgenutzt werden können.

Zum Start des DigitalStores Mitte Juli waren dort 77 digitale Verwaltungsservices verfügbar. Gibt es Meilensteine für den weiteren Ausbau des Angebots? Wo würden Sie persönlich gerne am Jahresende 2022 mit dem DigitalStore stehen?

Niedermaier: Wir werden das Angebot bis Ende 2022 um weitere rund 30 Online-Anträge mit Schwerpunkt auf Unternehmensleistungen ausbauen. Ab 2023 stehen der weitere Ausbau des Angebots, die breite Nachnutzung der Online-Anträge sowie die inhaltliche Erweiterung auf interne Prozessbausteine „vom Antrag zum Bescheid", etwa Rückfragen, digitale Bescheide etc., und rein interne Anträge – Urlaub, Dienstreisen etc. – im Fokus.

Gerlach: Grundsätzlich gilt: Jede digitalisierte Leistung ist ein Mehr an Service für den Bürger. Wir werden bis Ende des Jahres rund 30 weitere digitale Serviceleistungen anbieten, vorwiegend für Unternehmen. Ab 2023 sollen dann auch weitere Landkreise mit eingebunden werden, damit das Projekt auch in seiner Breite immer größer wird. Wie gesagt: Wir wollen in die Fläche. Da sind wir auf einem guten Weg.

Der Bayerische Landtag hat am 20. Juli ein Digitalgesetz beschlossen, welches u. a. ein neues Kompetenzzentrum zur Unterstützung der Kommunen vorsieht. Wie soll diese Institution und deren Hilfestellung konkret aussehen?

Gerlach: Das neue Kompetenzzentrum soll als Vermittler auftreten. Die Einheit soll vor allem EfA-Leistungen anderer Länder in die bayerischen Kommunen bringen, digitale Verwaltungsleistungen durch bayerische IT-Dienstleister für Kommunen vermitteln sowie die bayerischen Kommunen bei der Umsetzung dieser Aufgaben beraten. Mit unserem neuen Digitalgesetz schaffen wir den rechtlichen Rahmen, damit alle Menschen von den Vorteilen der Digitalisierung profitieren.

HiScout

Ein Datenpool
für Grundschutz,
Datenschutz und
Notfallmanagement

SecurITy made in Germany

- **HiScout Grundschutz**
  IT-Grundschutz und Risikoanalyse nach BSI 200-2 und 200-3
- **HiScout Datenschutz**
  Datenschutzmanagement nach EU-DSGVO
- **HiScout ISM**
  Informationssicherheitsmanagement nach ISO 27001/2
- **HiScout BCM**
  Business Continuity Management nach ISO 22301:2019 und BSI 200-4

www.hiscout.com

Integriertes Managementsystem für IT-Governance, Risk & Compliance

DIGITALER STAAT

Kritik in beide Richtungen

Kommunen im Fokus der OZG-Umsetzung

⟩⟩⟩ von **Matthias Lorenz,** Behörden Spiegel

Je näher die (nicht mehr zu haltende) Umsetzungsfrist des Onlinezugangsgesetzes (OZG) Ende 2022 rückte, desto hitziger wurden die Diskussionen über die Gründe des Scheiterns. Neben dem Sinn einer solchen Frist rückte dabei vor allem ein föderaler Akteur in den Fokus: die Kommunen. Noch immer, so lauteten die Vorhaltungen von Bundes- oder Landesebene, zögen nicht alle Kommunen beim OZG mit. Andersherum bemängelte die kommunale Seite unter anderem, in Entscheidungen nicht gut genug eingebunden zu sein. Auf dem Digitalen Staat 2022 spitzte sich die Debatte zu.

Gleich in seinem Auftaktstatement legte der Staatssekretär im Bundesinnenministerium (BMI) und Bundes-CIO, Dr. Markus Richter, die Grundlage der scharfen OZG-Diskussionen auf dem Kongress, bei denen die Kommunen im Mittelpunkt standen. „So richtig zufrieden können wir nicht sein", konstatierte Richter. Zwar seien digitale Lösungen oft und schnell verfügbar. Die OZG-Umsetzung scheitere jedoch meist an anderen Dingen, wie zum Beispiel der flächendeckenden Implementierung. Gerade die kommunale Vernetzung laufe in vielen Teilen immer noch nicht gut.

Neben vielen kommunalen Positivbeispielen gebe es heute immer noch Rathäuser und Landratsämter, die völlig isoliert arbeiteten, kritisierte Richter. Diese hätten die Zeichen der Zeit nicht erkannt. Wenn sich Städte oder Landkreise nicht wenigstens mit zwei anderen Kommunen vernetzten, seien Digitalisierungsvorhaben zum Scheitern verurteilt. „Dann reden wir nicht von kommunaler Selbstverwaltung, sondern von kommunaler Selbstzerstörung", so die drastische Warnung des Staatsekretärs. Es gebe Fälle, wo entschieden werde, nicht mit der Nachbargemeinde zusammenzuarbeiten, man gleichzeitig aber nur vier Mitarbeitende in der IT habe. So könne Digitalisierung nicht funktionieren.

Die Kritik von kommunaler Seite am Onlinezugangsgesetz ist jedoch nicht weniger deutlich. Prominent wird sie beispielsweise von Thomas Bönig, damals Leiter des Referats

für Informations- und Kommunikationstechnik der Stadt München und jetzt in ähnlicher Funktion in Stuttgart, geäußert. „Das OZG hat nach meiner persönlichen Einschätzung nichts mit Digitalisierung zu tun", sagt Bönig. Moderne Digitaltechnologien wie Künstliche Intelligenz oder Cloud würden im OZG nicht berücksichtigt. Aus Sicht der Kommunen sei es darüber hinaus verheerend, nicht zu wissen, wie es beispielsweise mit der Finanzierung der Leistungen oder mit Lieferterminen stehe.

In der Bundespolitik scheint diese Kritik zumindest teilweise Gehör zu finden. Tabea Rößner, Bundestagsabgeordnete für Bündnis 90/Die Grünen und Vorsitzende des Digitalausschusses, fordert, die Kommunen müssten nun auch vom Gesetzgeber stärker in den Fokus genommen werden. Sie bräuchten Planungssicherheit. „Natürlich müssen wir uns auch mit der Finanzierung nach 2022 auseinandersetzen", so Rößner im Frühjahr 2022. Sie scheint sich bewusst zu sein, dass hierfür auch nach 2022 Bundesmittel gebraucht werden. Trotzdem betont die Abgeordnete auch, dass langfristige Lösungen gefunden werden müssten. So stelle sich beispielsweise die Frage, ob Kommunen irgendwann in der Lage seien, den Betrieb der Leistungen selbst zu tragen.

Auch auf Länder-Ebene ist das Bewusstsein für die schwierige OZG-Situation in den Städten und Landkreisen vorhanden. „Viele Kommunen sagen mir, das Digitale ist eine Riesenbelastung, weil sie ja gleichzeitig auch noch das Analoge abbilden müssen", berichtet Stefan Krebs, CIO des Landes Baden-Württemberg. Trotzdem findet er das OZG nicht grundsätzlich schlecht: „Dieses Gesetz bietet auch einen Vorteil für die Verwaltung." Beispielsweise könnten sich Verwaltungsmitarbeitende ihre Zeit mit Online-Anträgen besser einteilen, weil nicht mehr morgens alle Bürgerinnen und Bürger Schlange stünden und dafür nachmittags niemand mehr einen Termin wolle.

Dagegen glaubt Bönig nicht, dass das OZG den Kommunen eine Entlastung bringe, weil es nur für Online-Anträge sorge. Eine digitale Verwaltung charakterisiert sich für den CIO dadurch, dass Prozesse vollautomatisiert im Hintergrund liefen, es vollautomatische Anträge gebe und Erinnerungen an Bürger, wenn zum Beispiel deren Personalausweis ablaufe. Bei einem möglichen OZG 2.0 müsse in die eigentliche Digitalisierung investiert werden. Nur so könnten Kommunen Zeit sparen, die dann in Leistungen investiert werden könnten, die man nicht digitalisieren könne, wie beispielsweise im sozialen Bereich.

Des Weiteren kritisiert Bönig, dass die Kommunen dem IT-Planungsrat nicht konkret sagen könnten, was sie eigentlich bräuchten. „Wir sind dort nicht vertreten, obwohl wir meistens diejenigen sind, welche die Beschlüsse umsetzen müssen." CIO Krebs stimmt hier insofern zu, als dass die Diskussion geführt werden müsse, wie man die Kommunen in Zukunft besser mitnehmen könne.

Eine weitere Frage, die sich im Spannungsfeld zwischen OZG und Kommunen stellt, ist die Frage der Nachnutzung von Leistungen. Stichwort ist das Einer-für-Alle Prinzip (EfA-Prinzip). Problematisch ist hier, dass den Kommunen der Überblick fehlt, welche Leistungen vielleicht schon woanders vorhanden sind und zur Nachnutzung bereitstehen. Die Folge können unter anderem Doppelentwicklungen sein.

„Wir haben uns gefragt, wie man mit EfA auch die Kommunen erreichen kann", erzählt Ulrike Klocke, Abteilungsleiterin Recht und Bund-Länder-Zusammenarbeit im Amt IT und Digitalisierung der Senatskanzlei Hamburg. Der Stadtstaat hatte im vergangenen Jahr den Vorsitz des IT-Planungsrates inne. Entstanden war die Idee des EfA-Marktplatzes der Genossenschaft govdigital.

„Der Marktplatz widmet sich zum einen der Frage der Nachnutzung, zum anderen aber auch der Frage der technischen Bereitstellung", erläutert Jens Fromm, der Gesamtprojektleiter bei der govdigital. Die Frage der Nachnutzung müsse unter anderem geklärt werden, weil Kommunen beispielsweise über den FIT-Store der Föderalen IT-Kooperation (FITKO) nur schwer erreicht werden könnten. Der FIT-Store richtet sich explizit an die Bundesländer, wird allerdings auch in den Marktplatz eingebunden. Im Moment befindet sich der Marktplatz im Status eines Minimum Viable Products (MVP), also einer ersten lauffähigen Version. „Vor der Sommerpause wollen wir mit dem Marktplatz in einer ersten Ausbaustufe, dem Schaufenster, live gehen", so Fromm im Frühjahr 2022. Man hoffe, dann mehr als die vier Leistungen zeigen zu können, die momentan schon im FIT-Store stünden.

Auf dem Digitalen Staat wurde angeregt über die Rolle der Kommunen im OZG-Kontext diskutiert. Mittendrin: Stefan Krebs und Tabea Rößner. Foto: BS/Trenkel

Resiliente Clouds für die Verwaltung

Innovationen finden in der Cloud statt

⟩⟩⟩ von **Paul Schubert,** Behörden Spiegel

Die Arbeit in der Cloud bietet viele Vorteile. Prozesse können schnell verarbeitet werden und die Skalierbarkeit ist gegeben. Vor allem in Krisenzeiten sind diese Komponenten sehr wichtig. Aber wie kann verhindert werden, dass Rechenzentrumsausfälle den Betrieb lahmlegen? Und welche Rolle spielen Hyperscaler dabei?

Obwohl eine Ausfallsicherheit nie komplett garantiert werden könne, sei durch die „Deutsche Verwaltungscloud-Strategie" (DVS) dieser Aspekt so gut wie möglich austariert, erklärt Jutta Cordt, Unterabteilungsleiterin im Bundesministerium des Innern und für Heimat (BMI). Sie mache die Verwaltung „robuster" und garantiere „Ausfallsicherheit auf einem hohen Niveau". Am wichtigsten sei an der DVS die Multi-Cloud-Strategie. Cordt erklärte, dass es durch dieses Vorgehen möglich sei, Anwendungen, die von DVS-Rechenzentren aus betrieben würden, in andere Rechenzentren zu verschieben. Dabei stehe die Verwaltung auch mit den Hyperscalern in Kontakt, um „IT-Sicherheit und Datenschutz gleichermaßen zu garantieren". Zusammen mit der Schaffung des Zentrums für digitale Souveränität und der DVS wolle der Bund die Verwaltung krisensicherer und innovationsfreudiger gestalten, so die Unterabteilungsleiterin des BMI.

Darüber hinaus sollte die Innovationsfreudigkeit einer Cloud effektiver genutzt werden, findet Nikolaus Hagl, Leiter Geschäftsbereich Public & Energy und Mitglied der Geschäftsleitung bei SAP Deutschland. Dabei könnten Innovationen auch im Bereich Künstlicher Intelligenz (KI) und datengetriebener Ansätze entstehen, folgerte Hagl: „Beides gehört aber zusammen, das eine funktioniert nicht ohne das andere." Ein weiterer großer Vorteil der Cloud sei die Vernetzung. Beim Thema Impfen und Lieferketten hätten die Entwicklungen der letzten Monate gezeigt, dass transparente Verknüpfungen durch Cloud-basierte Technologien „uns gut durch Krisen leiten können", so Hagl. Ferner könne eine souveräne Cloud auch Bürgerinnen und Bürgern den vertrauenswürdigen Rahmen bieten, der für sie nützlich und verständlich sei. Auch Holger Lehmann, Chef des Leitungsstabs und Pressesprecher des ITZBund, spricht sich für eine vermehrte Cloud-Nutzung aus – einerseits, um den Bürgern einen Mehrwert zu bieten, andererseits auch aus Wettbewerbsaspekten: „Neben der Skalierbarkeit des Cloud- Konzepts ist auch die Wirtschaftlichkeit wichtig. Beides ist in einer Cloud-Umgebung gegeben und bietet einen erhöhten Mehrwert", erklärte Lehmann.

Ein Panel auf Digitaler Staat gingen der Fragestellung nach, ob man Souveränität mit Resilienz gleichsetzen kann und inwiefern eine sichere Cloud beides gewährleisten kann. Foto: BS/Trenkel

Als Vertreter der Hyperscaler versucht auch T-Systems – dass auf die Google-Cloud setzt –, den Nutzenden „souveräne Kontrolle" zu gewährleisten. Nach Florian Jeggle, Strategic Business Executive von Google, ist dies in Deutschland für den privaten und öffentlichen Bereich möglich. Über die Cloud-Infrastruktur könne des Weiteren sichergestellt werden, dass die Daten und Metadaten „Deutschland nicht verlassen werden", erklärt Jeggle. T-Systems versuche demnach, die Google-Cloud souveräner zu machen und sie auch für deutsche Bürger sowie die Verwaltung attraktiv zu machen. Ob die Cloud auch Teil der Multi-Cloud-Strategie des Bundes wird, ist noch nicht zu sagen. Ein Proof-of-Concept ist bei diesen Versprechungen allerdings wohl zu erwarten.

Wir lotsen Sie durch den digitalen Wandel.

Durch unsere langjährige Erfahrung in der Zusammenarbeit mit Staat und Verwaltung kennen und verstehen wir Ihre Bedarfe und begleiten Sie auf Ihrem Weg zu menschenzentrierten und risikominimierten Innovationen – ob Leuchtturm oder gesamte Organisation. Wir sind IBM iX – die Experience Agency für den öffentlichen Sektor.

Mehr zu unseren Lösungen für den öffentlichen Sektor finden Sie unter: staat-digital.de

IBM iX

Digitale Verwaltung im Aufbruch

Rückblick auf den Vorsitz im IT-Planungsrat 2022

⟩⟩⟩ Gastbeitrag von **Dr. Markus Richter,** CIO des Bundes

Das Jahr 2022 war ein besonderes Vorsitzjahr im IT-Planungsrat. Der Endspurt bei der Umsetzung des Onlinezugangsgesetzes (OZG), aber auch äußere Einflüsse wie der Angriffskrieg in der Ukraine und anhaltende Herausforderungen durch die Corona-Pandemie prägten die Agenda des IT-Planungsrates und führten in diesem Jahr zu besonders vielen Sitzungen. Neben den drei regulären Sitzungen haben wir uns dreimal zu Sonderterminen zusammengefunden und im November zudem erstmals eine Klausurtagung abgehalten. Im Zentrum der Arbeit des IT-Planungsrates standen dabei die Priorisierung der OZG-Leistungen, der Aufbau eines Online-Marktplatzes mit der govdigital eG und die Entwicklung strategischer Schwerpunktthemen für die kommenden Jahre.

Die Mitglieder des IT-Planungsrats während der 38. Sitzung im Sommer 2022 Foto: BS/BMI

Dauerhaften Betrieb von EfA-Lösungen ermöglichen

Bund und Länder haben sich in diesem Jahr gemeinsam verpflichtet, 35 besonders wichtige OZG-Leistungen für die EfA-nachnutzungsfähige Bereitstellung beziehungsweise in der flächendeckenden Nachnutzung zu priorisieren. Die Priorisierung war uns wichtig, um vorhandene Ressourcen zu bündeln und so einen sichtbaren Fortschritt im Programm zu erzielen. Bisher hat die Priorisierung ausgewählter OZG-Leistungen insgesamt noch nicht die gewünschte Wirkung entfaltet. Die meisten dieser OZG-Leistungen werden zwar noch in diesem Jahr EfA-fähig verfügbar sein, jedoch wird in vielen Fällen ein flächendeckender Roll-out nicht bzw. nur teilweise erreicht werden. Bund und Länder arbeiten weiter gemeinsam mit Hochdruck daran, insbesondere die priorisierten Leistungen zügig umzusetzen und in die Fläche zu bringen. Das BMI unterstützt die Länder im Rahmen der OZG-Programmsteuerung dabei mit aller Kraft. In ihrer Sondersitzung im August hat die Abteilungsleiterrunde zudem ein gemeinsames Kosten- und Preismodell für die Nachnutzung von EfA-Onlinediensten beschlossen, um den dauerhaften Betrieb von EfA-Lösungen zu ermöglichen.

Für die gesamte öffentliche Verwaltung

Ein entscheidender neuer Ansatz, auf den wir uns im IT-Planungsrat geeinigt haben, ist der Aufbau eines elektronischen Marktplatzes durch govdigital eG, eine Genossenschaft von IT-Dienstleistern aus Bund und Ländern. Die Marktplatzinfrastruktur soll als Produkt des IT-Planungsrats zukünftig anbieteroffen, nachhaltig und unter Verwendung von Standards einen ebenenübergreifenden Austausch von IT-Leistungen ermöglichen, auch für Kommunen. Flankierend werden künftig in dem von der FITKO betreuten FIT-Store Onlinedienste zu standardisierten Vertragsbedingungen zur Nachnutzung angeboten. Perspektivisch sollen Marktplatz und FIT-Store der gesamten öffentlichen Verwaltung zur Verfügung stehen. Dafür haben wir den Marktplatz govdigital ab 2024 zum Produkt des IT-Planungsrats erklärt und verlängern das Projekt bis dahin.

Reifegradmodell für Nachweisabrufe

Damit Verwaltungskunden digitale Verwaltungsleistungen einfach und schnell beantragen können, muss die Verwaltung ihre Registerlandschaft modernisieren und eine Architektur zur Nachweisübermittlung bereitstellen. Die Bund-Länder-Gesamtsteuerung Registermodernisierung hat deshalb 2022 eine Architektur eines Nationalen Once-Only-Technical-Systems (NOOTS) entworfen. Dieses soll Fachverfahren und Registern auch den Anschluss an das europäische Once-Only-Technical-System ermöglichen (Umsetzung der Single-Digital-Gateway-Verordnung). Zudem hat die Gesamtsteuerung ein Reifegradmodell für Nachweisabrufe veröffentlicht. Ziel der Registermodernisierung ist es, mindestens elektronisch auswertbare Nachweise (Reifegrad C) und perspektivisch bedarfsgerecht übermittelte Informationen (Reifegrad D) zu erreichen. Darüber hinaus stand die Weiterentwicklung einer leistungsfähigen OZG-Infrastruktur im Fokus unserer Bemühungen.

Ausweitung von 115

Der Beschluss von März 2022 zur Umsetzung des zentralen Bürgerpostfachs war wichtig und richtig als Startschuss zu einer verstärkten Bündelung zentraler Komponenten, insbesondere den Nutzerkonten von Bund und Ländern. Aktuell wollen viele Länder die BundID, das Nutzerkonto des Bundes,

mitnutzen und dafür künftig auf eigene Konten und Postfächer verzichten. Perspektivisch würde ich mir wünschen, dass Bund und Länder noch einen mutigen Schritt im Sinne der Bürgerinnen und Bürger weitergehen und sich auf ein einziges Konto und Postfach verständigen.

Bei der OZG-Umsetzung sieht der IT-Planungsrat die Behördennummer 115 als eine wichtige Säule im Hinblick auf die voranschreitende Digitalisierung in Staat, Wirtschaft und Gesellschaft. Dies haben wir durch den Beschluss 2022/05 erneut bekräftigt. Das Team der 115 wurde gebeten, im Hinblick auf die Anforderungen aus der gemeinsamen OZG-Umsetzung insbesondere die Leistungen nach dem EfA-Prinzip bei dem weiteren Ausbau der Supportfunktion der 115 bevorzugt zu berücksichtigen.

Endspurt der OZG-Umsetzung

Wir haben im IT-Planungsrat in diesem Jahr viel erreicht und kürzlich in einer Klausurtagung einen wichtigen Reformprozess zu unseren Strukturen und unserem Selbstverständnis angestoßen. Das war uns als Bundesvorsitz ein wichtiges Anliegen. Der Endspurt bei der OZG-Umsetzung 2022 hat gezeigt, dass wir noch enger kooperieren und Partikularinteressen überwinden müssen, um noch einen Zahn zuzulegen. Denn zu einer flächendeckenden Digitalisierung der Verwaltung gibt es keine Alternative. Das gilt auch für die Weiterentwicklung des OZG, an dem wir mit vereinten Kräften arbeiten und bei dem die Lessons Learned aus dem OZG berücksichtigt werden.

Im vergangenen Jahr haben wir es geschafft, von der Entwicklungsphase ins Ausrollen zu kommen. Dem neuen Vorsitzland Hessen wünsche ich viel Erfolg bei der Leitung des IT-Planungsrates im Jahr 2023.

Dr. Markus Richter ist Staatssekretär im Bundesministerium des Innern, für Bau und Heimat (BMI) und Beauftragter der Bundesregierung für Informationstechnik (CIO). Foto: BS/Henning Schacht

// SAVE THE DATE

Die Vorbereitungen für den nächten „Digitalen Staat" laufen bereits. Das Event findet vom 25.–26. April in Berlin statt.

Künstliche Intelligenz massenhaft

Der Weg vorwärts für die öffentliche Verwaltung

⟩⟩⟩ von **Benjamin Hilbricht,** Behörden Spiegel

Im Auswärtigen Amt (AA) arbeitet eine Künstliche Intelligenz (KI). Sie durchforstet ein Meer von Daten nach Mustern und errechnet die Wahrscheinlichkeit, dass bestimmte Ereignisse eintreten. Das ist nur ein Beispiel, wo der Öffentliche Dienst KI einsetzt. In der breiten Fläche der Verwaltung kommen die selbstlernenden Algorithmen jedoch kaum zum Einsatz. Dem stehen viele Sorgen entgegen. Doch es gibt Wege, KI in die Breite zu tragen.

„Wenn man sich so in den Behörden umhört, sagen 44 Prozent, dass sie nicht wissen, ob sie KI einsetzen wollen. Jeder Zweite!", ruft Nikolaus Hagl von SAP Deutschland frustriert aus. Woran liegt dieses Zögern? Nach wie vor sähen viele Verwaltungsangestellte in KI zunächst eine Gefahr für ihren Arbeitsplatz.

Ist mein Arbeitsplatz in Gefahr?

Dabei müsse allerdings zwischen zwei Arten von Tätigkeiten unterschieden werden, erklärt Dr. Sven Egyedy, Beauftragter für die Digitalisierung und die Auslands-IT sowie CIO beim Auswärtigen Amt. Auf der einen Seite stünden hochkomplexe Tätigkeiten und Entscheidungen. Als Beispiel dafür nennt Egyedy einen Polizeieinsatz. Aber auch die Entscheidung darüber, ob Deutschland Waffen an die Ukraine liefern soll, wird so bald keine Maschine für uns treffen.

Auf der anderen Seite stehen die verwaltungstypischen Routinetätigkeiten. Einen Brief öffnen, die Antworten in eine Tabelle eintragen, das Ganze ins nächste System kopieren, einen Bescheid erstellen. Alle diese Tätigkeiten könne eine Maschine übernehmen, sagt Raymond Klotz, Manager Public Sector Germany bei UiPath. „Wiederkehrende, einfache Tätigkeiten werden ersetzt." Damit würden die Menschen frei, sich mit komplexeren Themen zu befassen. In Anbetracht dessen, wieviel Zeit in der Verwaltung auf solche Tätigkeiten verwendet werde, würde sich da auch ein schlagkräftigeres System entwickeln.

Der Bereichsvorstand für den Public Sector bei Bechtle, Steven Handgrätinger, sagt: „Es gilt, digitale Resilienz zu erzeugen."

Foto: BS/Trenkel

„Wir sprechen von volldigitalen Workflows", sagt Steven Handgrätinger, Bereichsvorstand Public Sector bei Bechtle.

Allerdings gibt es hier auch kritische Stimmen. „Wenn ich sechs Stunden hochkomplexe Tätigkeiten habe und zwei Stunden Routinearbeiten, dann schiebe ich Letztere gerne mal dazwischen, um mich zu erholen", erklärt Moritz Heuberger von der Universität Potsdam. Anstelle dessen könne eine Sachbearbeiterin nicht acht Stunden hochkomplexen Tätigkeiten nachgehen, führt er weiter aus. Zwar sei das Feedback zur Prozessautomatisierung aus der Verwaltung generell sehr positiv. Die Mitarbeiterinnen und Mitarbeiter freuten sich, wenn ihnen Routinearbeiten abgenommen würden.

Deshalb will die öffentliche Verwaltung KI für sich erschließen. Breit und flächendeckend. Bisher sind die meisten KI in der Verwaltung allerdings sogenannte „Leuchtturmprojekte". Das sei zwar ein erster Schritt hin zu mehr KI im Öffentlichen Dienst: „Ich freue mich über jeden Leuchtturm, der aufgebaut wird", erklärt Marc Schlingheider, Leiter des Geschäftsbereichs Öffentlicher Sektor bei IBM. Dennoch sei da das Problem, dass Leuchttürme Manufaktur-Produkte seien. Das heiße, die Hersteller schneiderten sie individuell auf die Erfordernisse eines Kunden zu.

Stattdessen benötige die Verwaltung ein Massenprodukt. „Wir brauchen einen Standard, den wir individualisieren und in die Breite tragen können", sagt Gerald Jenner, Geschäftsfeldentwickler bei Dataport. Seine Idee ist, statt spezieller Künstlicher Intelligenzen eine Art Muster-KI zu entwickeln, die sein Team dann nur noch an die Bedürfnisse des Kunden anpassen müsse. Etwa wie ein Anzug von der Stange, bei dem der Hausschneider noch einmal die Ärmel kürze oder die Hose auslässe, je nach Bedarf.

Ängste überwinden

Sören Bergner, Unterabteilungsleiter beim Bundesministerium des Innern und für Heimat (BMI), fügt hinzu, dass KI-Technologie auch Akzeptanz brauche. Denn sowohl Bürgerinnen und Bürger als auch die Anwenderinnen und Anwender in den Ämtern hätten Ängste. „Ich verstehe die Sorge der Bürger, gerade wenn KI im Bereich der Sicherheit angewendet wird", sagte er. Aber die öffentliche Verwaltung könne und müsse den Ängsten begegnen. „Wir müssen bei allem, was wir tun, Transparenz schaffen. Welche Daten sammelt die KI und was macht sie damit?", erläutert er seine Strategie. Für die Anwender in der Verwaltung hingegen müsse eher erklärt werden, wie KI-Anwendungen sich auf ihre Arbeitsprozesse auswirkten. Das Beratungs- und Kompetenzzentrum des BMI sei da ein gutes Unterstützungswerkzeug. Bergner fasst zusammen: „Wir brauchen Transparenz in der Gestaltung und in der Anwendung von KI-Systemen."

Alle mitnehmen

Digitalisierung selbst macht noch keine smarte Stadt

⟩⟩⟩ von **Malin Jacobson,** Behörden Spiegel

Den Ansatz, Städte (durch Digitalisierung) intelligenter zu machen, gibt es bereits seit gut zwei Jahrzehnten. In vielen Städten wurden seitdem Smart-City-Konzepte entwickelt, weiterentwickelt und zur Anwendung gebracht. Sowohl die digitalen Anwendungsmöglichkeiten als auch die Gesellschaft und deren Ansprüche an die moderne Verwaltung haben sich mit der Zeit gewandelt. Und damit auch das Verständnis von Smart City. Das Verständnis von Smart City hat sich geändert. Während Städte lange technologiegetrieben gewesen seien, verstehe man heutzutage unter Smart City eine nachhaltige und integrative Stadtentwicklung, erläuterte Frauke Janßen, Beauftragte für Digitalisierung des Deutschen Städtetags. „Digitalisierung selbst macht noch keine smarte Stadt", so ihr Statement. Stattdessen müsse man sich in den Kommunen fragen, wie man leben wolle, welche Herausforderungen es gebe und wie man diese Ziele erreichen könne – „erst dann kann Digitalisierung ansetzen und uns an unser Ziel bringen". Dem stimmte auch Sindy Würffel, EU-Projektmanagerin der Stadt Ulm, zu: „Smart City ist kein Etikett wie „Kurort", sondern steht bei uns für das Konzept der Stadt." In Ulm habe man sich – um die Frage zu klären, wie die Bürgerinnen und Bürger leben wollten und welche Herausforderungen es gebe – zwei Jahre Zeit genommen, erläutert die Projektmanagerin. Auf die Frage, ob zwei Jahre Bürgerbefragung in unserer heutigen Gesellschaft noch zeitgemäß seien, erklärte sie, es brauche Zeit, das ganze kommunale Ökosystem zu informieren und von nachhaltigen Veränderungen zu überzeugen. „Stadthistorie kann nicht von heute auf morgen auf Schnellspurmodus umgestellt werden. 3.200 Mitarbeitende müssen mitgenommen werden – es reicht nicht, wenn nur einzelne Abteilungen die Dringlichkeit sehen."

Wie lässt sich mit Best Practices die Kooperation im Bereich Smart City verbessern? Hierzu diskutierte ein Panel unter der Moderation von Frauke Janßen, Beauftragte für Digitalisierung beim Deutschen Städtetag.

Foto: BS/Trenkel

Auch in Köln habe man sich zwei Jahre Zeit für die Strategieplanung genommen, ergänzte Dirk Blauhut, Stabsstelle Digitalisierung der Stadt Köln. Allein um alle Gremien zu informieren, habe man ein halbes Jahr benötigt. Er plädierte zudem dafür, das Potenzial und die Kreativität der Bürgerinnen und Bürger in den Kommunen stärker in den Blick zu nehmen. Das funktioniere nur über zielgruppenorientiertes Werben, erklärte er auf die Frage, wie man die Menschen erreichen könne, um neue Konzepte für die Verwaltung zu diskutieren: „Direkt auf Veranstaltungen und durch Tür-zu-Tür-Geschäft, nur eine Maßnahme wird nicht helfen." Beispielsweise durch Hackathons, Boys' and Girls' Day oder ein Seniorencafé könne man Gruppen zusammenbringen und den gesamtgesellschaftlichen Austausch fördern. In Ulm habe man die Menschen zum einen über die Vereinsebene erreicht, ergänzte Würffel, zum anderen habe man Workshops veranstaltet und die Bürgerinnen und Bürger nicht nach Problemfeldern, sondern nach Lösungen gefragt. Dadurch habe sich der Einzelne wertgeschätzt gefühlt und man habe das kommunal vorhandene Potenzial nutzen können, erklärte die Projektmanagerin.

Umgang mit den Endgeräten

Neben der Kommunikation sei auch der geschulte Umgang mit internetfähigen Endgeräten entscheidend für das Gelingen der Verwaltungsdigitalisierung, so Würffel. Daher habe die Stadt Ulm während der Pandemie mit der dortigen Universität Informationen darüber zusammengetragen, was die Menschen an Know-how bräuchten, um mit ihren Endgeräten umgehen und so die digitalen Angebote der Verwaltung nutzen zu können. Als Konsequenz habe man Digitallotsen ausgebildet, die den Bürgerinnen und Bürgern Hilfestellung bieten könnten. Auch einen Kreativraum für die Verwaltungsmitarbeitenden, in dem sie sich beispielsweise mit Open Source auseinandersetzen könnten, gebe es, eräuterte die Projektmanagerin. Würffel: „Denn nur wenn unsere Mitarbeitenden geschult sind, können sie es an die Bürger weitergeben."

Kommunikation und Austausch seien zudem wichtig, um Vertrauen aufzubauen, so Lars-Oliver Schröder, CMO & CSO von XignSys. Das gelinge nicht von heute auf morgen, sondern müsse kontinuierlich wachsen. Hierbei sei auch der Erfahrungsaustausch mit anderen Städten und Projekten entscheidend. Dass man mittlerweile einfach in anderen Städten anrufen und fragen könne, wie man dort Herausforderungen angehe, hob auch Blauhut positiv hervor. Während früher jede Stadt eher für sich selbst gesprochen habe, könne man nun kommunenübergreifend Lösungsansätze angehen. Die Zusammenarbeit sei jedoch noch ausbaufähig, meinte Janßen. Momentan gibt es ihrer Meinung nach noch viele Reibungsverluste, da vergleichbare Projekte oft nichts voneinander wüssten und sich daher nicht austauschen könnten. Außerdem müsse das Ziel sein, dass nicht nur vom BMI geförderte Modellkommunen ihre Smart-City-Konzepte ausbauen könnten, sondern deren Erkenntnisse auch in die Fläche getragen würden. „Wir bleiben noch im Networking hängen und schaffen den Sprung nach außen nicht."

Basis moderner Verwaltung

Welche Herausforderungen bietet die E-Akte?

⟩⟩⟩ von **Tim Rotthaus,** Behörden Spiegel

Die E-Akte wird schon in einigen Teilen der Bundesrepublik mit großem Erfolg eingesetzt. So sind bis 2022 in Baden-Württemberg allein knapp 19.300 Arbeitsplätze mit der E-Akte ausgestattet worden. Doch die Umsetzung auf eine komplett digitale Verwaltung sollte nicht auf die leichte Schulter genommen werden. Man könne an der E-Akte auch vorbeiarbeiten, so Prof. Dr. Robert Müller-Török, Professor für E-Government an der Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg.

Die Einführung der E-Akte in Deutschland bedarf weiterhin einiger Arbeit. Prof. Dr. Robert Müller-Török betont insbesondere organisatorische Herausforderungen. Foto: BS/Trenkel

Bis 2024 soll in Baden-Württemberg der Roll-out der E-Akte abgeschlossen sein. „Die E-Akte ist ein zentraler Baustein zur medienbruchfreien Kommunikation und Vorgangsbearbeitung in der Verwaltung“, erklärte Dr. Daniela Oellers, Gesamtprojektleiterin des Projektes „Landeseinheitliche E-Akte“ im Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg. Durch Dienstleistungsportale wie zum Beispiel „service-bw“ und das Angebot von Basisdiensten über digitale Schnittstellen ließe sich ein vollständig digitaler und medienbruchfreier Verwaltungsprozess darstellen. Weitere Dienste ließen sich ebenfalls ohne Probleme anbinden, so Oellers. Es gebe jedoch auch einige Herausforderungen und „Stolpersteine“ bei der breiten Einführung der E-Akte.

So bedeute eine Erweiterung der Schnittstellen einen erhöhten Entwicklungsaufwand. Unterschiedliche Systeme müssten fehlerfrei miteinander kommunizieren und auch Themen wie Sicherheit und Datenschutz dürften nicht vergessen werden, sagt Oellers.

An der E-Akte vorbeiarbeiten

Ein weiterer wichtiger Punkt ist auch die flächendeckende Einführung der E-Akte. „Es bringt nichts, nur den halben Markt zu haben“, erläuterte Müller-Török. Alle Dienststellen müssten an die E-Akte-Systeme angeschlossen werden, damit das Prinzip reibungslos funktioniere. Sonst werde an der E-Akte vorbeigearbeitet. In diesem Punkt sieht er in Deutschland noch einigen Nachholbedarf. So sei vor allem vergessen worden, die komplette diplomatische Vertretung Deutschlands in anderen Ländern an das E-Akte-System anzubinden. Dies zu ändern, bedürfe eines großen Aufwands, so Müller- Török. Die deutsche Verwaltung müsse sich im Klaren sein, dass die Einführung der E-Akte mit organisatorischen Veränderungen einhergehen werde.

Mehr Sicherheit

Marc Horstmann, Prokurist und Leiter der Geschäftsfelder Justiz und Europa bei Governikus, sieht große Probleme beim Thema Sicherheit. „Elektronische Daten und Dokumente weisen generell keinerlei Authentizität auf und haben keine Rechtsverbindlichkeit“, so Horstmann. In seinen Augen ist die E-Akte an sich zu kurz gedacht. Er erhofft sich ein erhöhtes Maß an Sicherheit durch den Einsatz von Kryptografie. Durch dieses Verfahren soll durch elektronische Siegel und Signaturen die Authentizität der Dokumente sichergestellt werden. Horstmann stimmte den anderen Referenten zu, dass ein flächendeckender Einsatz der E-Akte in der deutschen Verwaltung noch einiges an Arbeit benötige.

Die E-Akte ist die Grundlage einer elektrifizierten, digitalen, vernetzten Verwaltung.

Bild: BS/ItNeverEnds, pixabay.com

M365: Add-ins für nutzerfreundliche Sicherheit

⟩⟩⟩ Von **Andreas Liefeith,** Leiter Unternehmenskommunikation der procilon GmbH

Um zu vermeiden, dass sensible Daten beim Versand via E-Mail von unberechtigten Personen oder Systemen mitgelesen werden, kann man auf gebräuchliche Verschlüsselungs-Technologie nach S/MIME- oder PGP-Standard zurückgreifen. Höhere Security-Anforderungen bestehen aber z. B. beim elektronischen Rechtsverkehr (ERV). Zu diesem zählt auch das besondere elektronische Bürger- und Organisationen-Postfach (eBO), mit welchem natürliche und juristische Personen Dokumente an Gerichte und Behörden auf einem sicheren Übertragungsweg übermitteln können.

Als Experte für Kryptographie im Allgemeinen und den ERV im Speziellen hat procilon zwei Add-ins für O/365 auf den Markt gebracht, die Nutzerinnen und Nutzern eine einfache und sichere elektronische Kommunikation ermöglicht.

So können z. B. mit der Erweiterung des MS/Outlook-Clients durch proTECTr Mail Connect Dateianhänge mit nur einem Klick für die Empfänger einer E-Mail stark verschlüsselt und von diesen direkt aus dem Outlook heraus wieder entschlüsselt werden.

Ähnlich konzipiert ist die procilon MS/Outlook-Erweiterung für den elektronischen Rechtsverkehr. Das Add-in wird hier um

eine Komponente ergänzt, die eine Suche von adressierbaren Gerichten und Verwaltungen im Teilnehmerverzeichnis des ERV sowie die Erzeugung von XJustiz-Datensätzen ermöglicht.

Um diese Innovation effizient nutzen zu können, hat procilon ein Komplettpaket für den Einstieg und die Nutzung vom eBO zusammengestellt, um Anwender bestmöglich zu unterstützen.

IntechCORE

Softwareentwicklung & IT-Beratung

» Java-Softwareentwicklung mit Profis vor Ort
» Seit 2008 Dienstleister für die Justiz
» B2B Projekte mit ausgewählten Referenzkunden
» Partnernetzwerk mit Expertise in den Bereichen JavaScript und .NET

SCell based on Java ™

Eigene Produktentwicklung unserer skalierbaren Tabellenkalkulation
www.scalable-components.com

Es kommt auf die Standards an

Wie der Staat leistungsfähiger und intelligenter werden kann

⟩⟩⟩ von **Jörn Fieseler,** Behörden Spiegel

Die Staatsorganisation und der Föderalismus stehen seit Beginn der Corona-Pandemie und vor allem im Zuge der Umsetzung des Onlinezugangsgesetzes (OZG) in der Kritik. Kritik zu üben, ist das eine – es besser zu machen, das andere. Doch wie können ein intelligenter Föderalismus und eine leistungsfähige Staatsorganisation aussehen?

Digitale Kleinstaaterei beenden

„Trotz aller Kritik hat sich der Föderalismus über lange Zeit bewährt", unterstrich Dr. Christoph Baron. Seit der Pandemie bleibe jedoch der Eindruck, „da geht noch was", so der Direktor Öffentlicher Sektor bei KPMG. Drei Aufgaben müssten angegangen werden: Erstens seien die Strukturen zu überprüfen und das föderale System weiterzuentwickeln. In dem Zusammenhang müsse zweitens über ein „Mehr" auf Bundesebene nachgedacht werden. Allerdings sei ein Zentralstaat nicht für alles geeignet, zeigte Baron im selben Atemzug die Grenze dieser Aufgabe auf. Und schließlich gehört für den Direktor Öffentlicher Sektor dringend eine Reduzierung der Zuständigkeitsebenen zu einer leistungsfähigen Staatsorganisation. „Wir müssen die digitale Kleinstaaterei endlich beenden und länderübergreifend einheitliche Standards bei der Digitalisierung setzen", so die Forderung Barons. In diesem Kontext müsse der Staat als Regulierer auftreten, wie es bei der Breitbandversorgung im ländlichen Raum schon geschehe. Dafür müssten letztlich genügend Haushaltsmittel bereitstehen.

Diskutierten eifrig über die Notwendigkeit von Standards vorgegeben durch den Bund (v. l. n. r.): Dr. Ralf Kleindiek, CDO des Landes Berlin und Staatssekretär für Digitales und Verwaltungsmodernisierung, Dr. Ariane Berger, Leiterin Digitalisierung beim Deutschen Landkreistag, und Dr. Christoph Baron, Direktor Öffentlicher Sektor bei KPMG. Fotos: BS/Trenkel

Novellierung der Finanzierungsausgleichsgesetze nötig

Dem konnte Dr. Ariane Berger, Leiterin Digitalisierung beim Deutschen Landkreistag (DLR), nur zustimmen. „Wir haben eine Intelligenzreserve!" sagte sie. Das seien Kooperationen. Dazu müsse klar über verfassungsrechtliche Ebenen hinweg gedacht werden. Doch dafür brauche es einen Informationsverbund. Dieser sei bei der Umsetzung des OZG bereits geübt worden. Allerdings stecke der sprichwörtliche Teufel im Detail, nämlich in den Verwaltungsvereinbarungen und den Finanzierungsfragen. Für die Digitalisierungsexpertin stehe damit der Bund in der Pflicht, langfristig für eine schlagfertige Finanzierung zu sorgen. Zugleich müssten jedoch die Finanzierungsausgleichsgesetze der Länder novelliert werden, forderte Berger: „Das geht ohne eine Verfassungsänderung."

Kommunen erbringen 80 Prozent der Leistungen

„Wenn wir den Staat digitalisieren wollen, müssen wir uns die Frage stellen, wie viel Föderalismus wir brauchen und wo wir darauf verzichten können", sagte Stefan Krebs, Beauftragter der Landesregierung für Informationstechnologie des Landes Baden-Württemberg. Beim Thema Standards sind für ihn zwei Faktoren von Bedeutung. Zum einen werde die Föderale IT-Kooperation (FITKO) für die Umsetzung von Standards immer wichtiger. Zum anderen seien die Kommunen stärker einzubinden. Schließlich würden Letztere 80 Prozent der Leistungen erbringen, seien aber im Staatsgefüge als Teil der Länder verfassungsrechtlich nicht vertreten.

Vertrauen in den Staat erhalten

Es sei jedoch der falsche Weg, wenn der IT-Planungsrat Fachverfahren einheitlich vorschreiben wolle. „Das kann nur schiefgehen" , so der bekennende Föderalismusfreund aus Baden-Württemberg. Stattdessen brauche es ein agiles, eigenverantwortliches Handeln aller Akteure. Und: „Wir müssen mal wirklich kleine Lösungen bauen, die dann auch funktionieren."

Dr. Ralf Kleindiek, CDO des Landes Berlin und Staatssekretär für Digitales und Verwaltungsmodernisierung in der Hauptstadt, konnte dem nicht widersprechen. Ganz im Gegenteil. Es gehe um nicht weniger, als das Vertrauen der Bürgerinnen und Bürger in den Staat zu erhalten und zu stärken. „Dazu ist der Erfolg der Digitalisierung unabdingbar."

Intelligenter Föderalismus und leistungsfähige Staatsorganisation

Deutschland ist ein föderaler Staat – eine Struktur, die sich trotz aller Kritik bewährt hat, im Zeitalter der Digitalisierung und erst recht nach den Erfahrungen, die wir alle als Bürgerinnen und Bürger, aber vor allem auch die Unternehmen in der Corona-Pandemie machen mussten, „geht bei der Digitalisierung noch was". Wir sind schon besser geworden, aber in vielen Bereichen sind wir noch nicht wirklich gut. Welche Schulaufgaben müssen wir erledigen, um im internationalen Ranking wie dem „EU e-Government Benchmarking" einen besseren Platz zu erreichen?

Erste Aufgabe

Strukturen überprüfen und das föderale System weiterentwickeln!

Mit Bund, Ländern, häufig Bezirksregierungen, Landkreisen und Gemeinden haben wir bis zu fünf Verwaltungsebenen, die Zuständigkeiten besitzen. Der Zentralstaat könnte hier zwar manches, aber nicht alles besser machen. Es muss daher immer wieder geschaut werden, wo doppelte und konkurrierende Zuständigkeiten abgebaut und Entscheidungsketten verkürzt werden können. Und das muss dann ernst genommen werden, denn es spart Zeit und Ressourcen und führt obendrein zu einer höheren Zufriedenheit der Kunden, die öffentliche Dienstleistungen empfangen.

Bei der drängenden Zukunftsaufgabe Digitalisierung sind dann Zentralität digitaler Lösungen als operatives EfA-Prinzip und die Zuständigkeiten im Föderalismus auch kein Widerspruch, denn hier kommt es vor allem darauf an, einheitliche Standards zu setzen. Die Zulassung eines PKW beispielsweise ist immer der gleiche Vorgang, egal, ob in Flensburg, Berchtesgaden, Köln oder in Berlin. Hier sollte das gleiche System, bundesweit vernetzt, zum Einsatz kommen.

Zweite Aufgabe

Digitale Kleinstaaterei beenden und länderübergreifend einheitliche Standards bei Digitalisierung setzen!

Am Anfang stehen hier die Selbsterkenntnis und ein altes Sprichwort: Zu viele Köche verderben den Brei. Wir müssen immer wieder das gleiche Muster erkennen: „cuius regio eius religio". Jeder macht seines und zu viele arbeiten an – im Ergebnis oft auch noch mit unterschiedlichen – Lösungen für die gleichen Aufgaben.

Bei der Digitalisierung muss grundsätzlich gelten: Der Staat setzt den rechtlichen und planerischen Rahmen. Er ist überall dort Dienstleister, wo es wirtschaftlicher für den Nutzer oder im Sinne der Diskriminierungsfreiheit notwendig ist, oder wenn es bei wichtigen Versorgungsfragen zu einem Marktversagen kommt – beispielsweise bei der Breitbandversorgung in dünn besiedelten Räumen.

Thorsten Kaiser ist Bereichsvorstand Öffentlicher Sektor bei KPMG. Foto: BS/KPMG

Im Setzen von Standards liegt die wahre Gestaltungsmacht, aber auch -pflicht, des Staates.

Dritte Aufgabe

Schneller werden, damit uns der Rest Europas nicht überholt und unsere wirtschaftliche und politische Stärke in einer digitalisierten Welt verloren geht.

Das Onlinezugangsgesetz (OZG) verpflichtete Bund, Länder und Gemeinden bis Ende 2022 knapp 600 Verwaltungsleistungen digital über Verwaltungsportale anzubieten. Das OZG ist zwar auch weiterhin gültig, hat sich aber als nicht ausreichend erwiesen, die Umsetzungsproblematik bei der Digitalisierung von Verwaltungsleistungen vollständig zu lösen. Es müssen deshalb jetzt – und zwar parallel zum letztlich nur den Aufschub legitimierenden „OZG 2.0" – die konkreten Schritte und ein Zeitplan festgelegt werden, um die Rahmenbedingungen für eine umfassende Verwaltungsdigitalisierung zu schaffen.

Zentrale Leistungen müssen endlich priorisiert und der Rollout bereits entwickelter Leistungen beschleunigt erfolgen. Wenn festgestellt wird, dass 80 % der Verwaltungsleistungen bereits digital zur Verfügung stehen (EU E-Government Benchmark 2021), dann sind dies offensichtlich nicht diejenigen, die vorrangig benötigt werden. Anders ist der allgemein wahrgenommene Mangel an Digitalisierung nicht zu erklären.

Der Fokus bei der Priorisierung muss deshalb auf die Anzahl der tatsächlich erreichten Nutzerinnen und Nutzer gelegt werden. Und wenn der Staat es allein nicht schafft, zum Beispiel eine digitale ID bereit zu stellen, so steht ihm die leistungsfähige digitale Wirtschaft für die temporäre Aufgabe des Übergangs in die digitale Welt bei der OZG-Umsetzung zur Seite.

Lassen Sie uns zusammen die Digitalisierung im föderalen Deutschland voranbringen!

HEssenDIGITAL

DIGITALE VERWALTUNG IN HESSEN
VISION | AGENDA | UMSETZUNG

08. Juni 2022 | Bad Homburg

www.hedigital.de

HESSEN DIGITAL

Kulturwandel dringend benötigt

Hilft der Generationenwechsel?

⟩⟩⟩ von **Matthias Lorenz,** Behörden Spiegel

Das Wort Revolution bezeichnet eine schnelle, radikale Veränderung der gegebenen (politischen, sozialen, ökonomischen) Bedingungen. So lautet die Definition des Wortes im Politiklexikon von Klaus Schubert und Martina Klein. Außer Acht gelassen wird in dieser Definition die kulturelle Revolution. Auch auf dem Kongress HEssenDIGITAL 2022 nahm kein Experte das Wort „Revolution" in den Mund. Trotzdem kristallisierte sich folgende Kernbotschaft heraus: Damit die Digitalisierung des Staates und der öffentlichen Hand gelingt, braucht es in der Verwaltung nun eine kulturelle Revolution. Diese muss im Kopf der Mitarbeitenden stattfinden – aber längst nicht nur.

Vertrauen in den Staat erhalten

Der Revolution versucht die Strategie Digitale Verwaltung Hessen 4.0 (DVH 4.0) einen Rahmen zu geben. Auf das Papier, das ein Jahr zuvor veröffentlicht wurde, ist man zwischen Wiesbaden, Fulda und Kassel besonders stolz. Patrick Burghard, Staatssekretär für Digitale Strategie und Entwicklung sowie CIO des Landes, betont, dass man schon in der Entwicklung der Strategie einen radikalen Perspektivwechsel vorgenommen habe: „Wir sind sehr nutzerzentriert an das Thema herangegangen." Im Mittelpunkt habe die Frage gestanden, wie man den Bürger und die Unternehmen in die Position bringen könne, deutlich positiver mit der Verwaltung in Kontakt zu treten. Darüber hinaus habe man sich auch nicht gescheut, einige Visionen zu formulieren, die kurz- und mittelfristig noch nicht umsetzbar seien.

Mitarbeitende mitnehmen

Daneben kommt der CDU-Politiker auch auf das Thema der Mitarbeitenden zu sprechen. Die DVH 4.0 solle ein „Wir-Gefühl" bei den Mitarbeitenden auslösen, denn: Bei der Digitalisierung müssten diese auf allen Ebenen der Verwaltung mitmachen. Selbiges hebt auch Holger Klötzner, Dezernent für Digitalisierung und Schule der Wissenschaftsstadt Darmstadt,

hervor. Die Stadt sieht sich als Vorreiter im Bereich Smart City. Vorhaben in diesem Bereich hingen jedoch zumindest teilweise von der Digitalisierung der Verwaltung ab, erklärt Klötzner. Dies sei jedoch nicht einfach: „Es ist auch ein Kulturwandel“, sagt er und nennt als Beispiel das noch oft vorgeschriebene Schriftformerfordernis. Die Mitarbeitenden auf diesem Weg mitzunehmen, sei ein Prozess: „Wir sind an dieser Stelle auch in Darmstadt noch nicht bei 100 Prozent, aber wir müssen uns dem Ziel langsam annähern. Man darf nicht von vorneherein sagen, man hat in seiner Verwaltung nicht das richtige Mindset dafür“, warnt Klötzner.

Wertebasierte und offene Kultur

Die Mitarbeitenden müssen jedoch auch in die Position gebracht werden, ihren Teil zur Verwaltungsdigitalisierung beitragen zu können. Hier kommt ein nächster Aspekt der nötigen Revolution ins Spiel, den die Präsidentin der Föderalen IT-Kooperation (FITKO), Dr. Annette Schmidt, folgendermaßen formuliert: „Wir brauchen eine andere Kultur im Umgang miteinander. Wir müssen es zulassen, dass Fehler gemacht werden.“ In der FITKO selbst sei es sehr gut gelungen, eine wertebasierte und offene Kultur zu ermöglichen. Die Organisation steht jedoch viel im Austausch mit anderen Behörden. „Dort treffen wir oft auf ein immenses Beharrungsvermögen an bisherigen Vorstellungen, Vorgehensweisen und Strukturen“, berichtet Schmidt. Hier sei noch eine Menge zu tun. Es gelte unter anderem, die neuen Werte schon früh vorzuleben, zum Beispiel in der Ausbildung und in den Hochschulen.

Genau an dieser Stelle setzt die Hessische Hochschule für öffentliches Management und Sicherheit an. „Wir fangen schon bei den Studierenden an, das digitale Mindset zu verankern“, erläutert Prof. Dr. Beate Eibelshäuser, die kommissarische Dekanin des Fachbereichs Verwaltung. Auch sie sieht es als Problem, dass man in Deutschland immer alles perfekt machen wolle. Deswegen sei es wichtig, dass auch an Hochschulen Experimentierräume geschaffen würden, wo sich die Studierenden ausprobieren könnten. „Um Innovationen zu treiben, braucht man eine Fehlerkultur, damit man beispielsweise herausfinden kann, welche Verfahrensweisen funktionieren und welche nicht“, so Eibelshäuser.

„Um Innovationen zu treiben, braucht man eine Fehlerkultur“, erklärt Prof. Dr. Beate Eibelshäuser.
Foto: BS/Patrick Schmetzer

Wo ist unser Wagniskapital?

Selbst im hessischen Rechnungshof ist man der Ansicht, dass eine Fehlerkultur erlaubt sein müsse. Das Klischee über den Rechnungshof stimme nicht mehr: „Wir sehen, dass sich die Zeiten verändert haben, sowohl bei uns intern als auch bei den Behörden“, sagt Dr. Walter Wallmann, der Rechnungshof-Präsident. Natürlich müsse weiterhin auf Effizienz und Effektivität geachtet werden. Aber man brauche Menschen, die den Mut hätten, Verantwortung zu übernehmen. „Es darf nicht so weit kommen, dass man aus Angst gewisse Sachen nicht mehr vorantreibt.“ Zudem merkt Wallmann an, dass jährliche Haushalte alles andere als agil seien. Beim Stichwort Fehlerkultur müsse auch die Frage gestellt werden: „Wo ist unser Wagniskapital?“

Die kulturelle Revolution muss sich jedoch nicht nur im Kopf der Mitarbeitenden vollziehen. Es geht auch um Organisationen an sich, die sich ändern müssen. Dem Co-CIO des Landes Hessen, Roland Jabkowski, fällt an dieser Stelle sofort das Einer-für-Alle-Prinzip (EfA-Prinzip) ein, welches im Rahmen der Umsetzung des Onlinezugangsgesetzes (OZG) von den Bundesländern angewandt werden soll. „Überall herrscht noch die Kultur eines ‚Mia san mia‘“, kritisiert Jabkowski. Dies führe in der Praxis dazu, dass zwar alle die Vorteile von EfA im Gespräch nennen könnten, die Umsetzung bröckele jedoch.

Die Zeit gibt Hoffnung

Auch auf der kommunalen Ebene müssen gerade in Bezug auf die Zusammenarbeit grundlegende Veränderungen stattfinden. Dieser Ansicht ist zumindest Bertram Huke, Direktor des kommunalen IT-Dienstleisters ekom21. Wenn man hinter die Kulissen schaue, sehe man: Die Rechtslage in den Kommunen sei gleich oder sehr ähnlich, trotzdem werde zu 80 Prozent unterschiedlich gearbeitet. „Das führt zu wahnsinnigen Ineffizienzen“, bekräftigt Huke. Nun müsse man sie motivieren, zusammenzuarbeiten und beispielsweise auf Standardlösungen zu setzen. Es könnten bereits ungeahnte Gewinne entstehen, wenn drei bis fünf Kommunen einen Prozess gleich bearbeiten würden.

Damit die Digitalisierung der Verwaltung ein Erfolg wird, muss die kulturelle Revolution also auf mehreren Ebenen vorangetrieben werden: bei den Mitarbeitenden, aber auch bei den Behörden und Organisationen an sich. Bei diesem Prozess, so der Eindruck, steht die Verwaltung noch ziemlich am Anfang. Ein Aspekt, der Hoffnung macht, ist die Zeit. So gibt es laut Huke gerade einen Generationenwechsel bei Bürgermeistern und Landräten. Und mit den frisch ausgebildeten Mitarbeitern oder Absolventen könnten auch andere Denkmuster in die Behörden einziehen. Die damit einhergehende Hoffnung spricht Prof. Eibelshäuser aus: „Die Dinge, welche wir heute angesprochen haben, werden sich also ein Stück weit herauswachsen.“

Mehr Mut zur Veränderung

Gießkannen-Förderung wird kritisiert

⟩⟩⟩ von **Sven Rudolf,** Behörden Spiegel

„Was wird für die Umsetzung des Onlinezugangsgesetzes (OZG) gebraucht?“ fragte Steven Janiec, Director von Deloitte Consulting, zum Auftakt eines schnellen Diskussionsformats auf dem Kongress HEssenDIGITAL. Das Thema OZG war aufgrund der nahen Deadline Ende 2022 allgegenwärtig. Janiec pitchte zu diesem Thema drei Thesen. Deren Erfüllung sei nötig, um OZG und Digitalisierung voranzubringen. Er forderte mehr Ende-zu-Ende-Digitalisierung, mehr Agilität in der Verwaltung und mehr Mut zur Veränderung.

Agilität und Fachwissen

Volker Mosler, Co-Leiter der Koordinierungsstelle OZG-Kommunal aus dem Hessischen Ministerium des Innern und für Sport, stimmte den Thesen größtenteils zu, ergänzte jedoch, dass ein stetiger Dialog mit den Kommunen und das Finden von Fachansprechpartnern für mehr Akzeptanz des OZG sorgen würde. Martin Woitschell, Referatsleiter Projektreferat OZG beim Hessischen Ministerium des Innern und für Sport, war hingegen der Meinung, man solle sich zunächst auf die Umsetzung des OZG konzentrieren. Dazu merkte er an, dass man kleinere Kommunen für die Zusammenarbeit zusammenlegen solle, um ihnen die Umsetzung zu erleichtern. Thomas Wieland, Leiter Digitalisierung und E-Government bei der Metropolregion Rhein-Neckar, kritisierte dagegen die Fokussierung auf das OZG. Er sagte, es müsse nicht nur digitalisiert, sondern auch automatisiert werden. Außerdem brauche es in der Verwaltung mehr Agilität. Hierfür müsse mehr Fachwissen geschaffen werden. Diskutiert wurde abgesehen von der OZG-Umsetzung auch der Weg der Städte und Landkreise hin zum Zielbild der digitalen Kommune. Jürgen Vogler, Geschäftsführung von procilon, fragte, was eigentlich eine digitale Kommune sei. Seine Gesprächspartnerin Sabine Bachmann, Leiterin der Stabstelle Digitale Verwaltung aus dem Landkreis Groß-Gerau, berichtete über den aktuellen Stand der Umsetzung von digitalen Kommunen. Beim Thema Förderung kritisierte sie, dass es sich bei den aktuellen Förderungen eher um Maßnahmen mit Gießkannen-Effekt handele, die mit einem großen Arbeitsaufwand verbunden seien. Ihrer Meinung nach wäre eine Art Meilenstein-System sehr viel nützlicher.

Vermittlung digitaler Kompetenzen

Wieder etwas allgemeiner wurde es dann bei der Diskussion des Themas der „digitalen Transformation“. Christian Rupp, CDO von PROSOZ Herten, pitchte dazu drei Thesen, die in erster Linie auf die geistige Bereitschaft zur Umsetzung der Digitalisierung abzielten. Dr. Markus Unverzagt, Referatsleiter Digitale Transformation im hessischen Ministerium für Digitale Strategie und Entwicklung, stimmte hiermit insoweit überein, als dass es gesunden Menschenverstand brauche, um die Digitalisierung umzusetzen. Unverzagt sprach auch die Tatsache an, dass Kompetenz nur ein Baustein von vielen beim Thema der Digitalisierung sei. Prof. Dr. Beate Eibelshäuser, Dekanin (komm.) vom Fachbereich Verwaltung der Hessischen Hochschule für öffentliches Management und Sicherheit, fokussierte sich bei ihrem Kommentar im Gegensatz zu Unverzagt auf den Punkt der Kompetenz und sprach sich dafür aus, Studierende als Digital Scouts zur Vermittlung zu verwenden, um alle bei der Digitalisierung mitzunehmen.

Sabine Bachmann, Leiterin der Stabstelle Digitale Verwaltung aus dem Landkreis Groß-Gerau, und Jürgen Vogler, Geschäftsführung von procilon, diskutierten zum Thema digitale Kommune. Foto: BS/Patrick Schmetzer.

Die SINA Workstation erfüllt als einzige Lösung standardmäßig alle BSI-Anforderungsprofile an einen sicheren Arbeitsplatz. VPN-Client, 2-Faktor-Authentisierung, Festplattenverschlüsselung und Schnittstellenkontrolle in einem Gerät.

secunet.com protecting digital infrastructures

secunet

Schwerpunkte für das Vorsitzjahr 2023

Handlungsfähigkeit sicherstellen

⟩⟩⟩ Gastbeitrag von **Patrick Burghardt,** CIO des Landes Hessen

Es könnte kaum einen spannenderen Zeitpunkt geben als 2023, um den Vorsitz des IT-Planungsrats zu übernehmen. Denn es stehen inhaltlich viele große Themen an. Aber auch organisatorisch und strategisch steht der IT-Planungsrat – und mit ihm zusammen die Föderale IT-Kooperation (FITKO) – vor deutlichen Veränderungen. Denn eine Verwaltung, die agiler und digitaler werden muss und will, muss regelmäßig überprüfen, ob die bestehenden Organisationsstrukturen den Anforderungen noch gerecht werden. Dies ist bei der erstmals durchgeführten Klausurtagung des IT-Planungsrats im November 2022 geschehen. Das Vorsitzjahr wird also stark geprägt sein von Maßnahmen zur Stärkung der Handlungsfähigkeit des IT-Planungsrats und der FITKO.

Registermodernisierung und Once Only

Ein wichtiger Fokus meiner Arbeit als Vorsitzender werden die erstmals gemeinsam formulierten mehrjährigen Schwerpunktthemen sein. Mittels der großen Leitplanken sollen der Blick fokussiert und die Kräfte gebündelt werden, sodass wir schnellere Entscheidungen treffen, effektiver arbeiten und mehr Wirksamkeit erzeugen können. Die fünf gewählten Schwerpunkte sind zum einen die digitale Infrastruktur mit Fokus auf der Cloud-Transformation und zum anderen die digitale Transformation, hier vor allem der Ausbau der digitalen Kompetenzen des eigenen Personals und die Standardisierung und Harmonisierung sowie der Abbau gesetzlicher Hemmnisse. Dritter Schwerpunkt sind digitale Anwendungen wie die Weiterentwicklung des OZG, die Stärkung der Nachnutzungen sowie die Umsetzung der Single-Digital-Gateway-Verordnung und die föderale IT-Architektur. Beim Schwerpunkt Datennutzung und Datenschutz stehen Registermodernisierung und Once Only im Mittelpunkt. Fünfter Punkt ist die Informationssicherheit.

Patrick Burghardt ist seit 2019 Staatssekretär für Digitale Strategie und Entwicklung sowie CIO und Bevollmächtigter der hessischen Landesregierung für E-Government und Informationstechnologie.
Foto: BS/HMinD

Übergreifendes Zielbild und politischer Wille

Hessen legt 2023 sein Augenmerk auf Cloud, digitale Kompetenzen und OZG 2.0. Das Potenzial der Cloud-Transformation ist bezüglich der Steigerung von Effizienz und Arbeitgeberattraktivität enorm. Noch fehlt es jedoch an einem abgestimmten Vorgehen, um dieses auch vollständig zu heben. Ziel Hessens ist es, gemeinsam mit Bund und Ländern im IT-Planungsrat die politischen und organisatorischen Rahmenbedingungen für eine erfolgreiche Cloud-Transformation der Verwaltung zu definieren und zu initiieren. Dazu ist es notwendig, ein übergreifendes Zielbild zu definieren und den politischen Willen zu formulieren. Weiterhin müssen wir die dafür erforderlichen organisatorischen Rahmenbedingungen analysieren und prüfen sowie die betriebswirtschaftlichen Rahmenbedingungen für die Etablierung eines sicheren und zuverlässigen Cloud-Marktes schaffen. Dazu müssen wir unter anderem über die Rolle und Aufgabe der öffentlichen IT-Dienstleister im „Spielfeld Cloud" und Möglichkeiten der Konsolidierung von Angebot und Nachfrage nachdenken. Zudem müssen wir Projekte voranbringen, die schnell und in der erforderlichen Entschiedenheit die Cloud-Transformation ermöglichen.

Auf Bedürfnisse zugeschnitten

Erste Schritte auf dem Weg zur Stärkung der Digitalkompetenzen in der öffentlichen Verwaltung wurden bereits erfolgreich getätigt. So haben wir seit 2022 die Weiterbildungsplattform eGovCampus, um zugeschnitten auf die Bedürfnisse der Verwaltungsbeschäftigten die Kompetenzen bei E-Government und Verwaltungsinformatik zu steigern. Hessen möchte – gerne gemeinsam mit weiteren Bundesländern – die Gestaltung und Pilotierung von Fortbildungsmaßnahmen auf Basis der Lernmodule aus dem eGov-Campus angehen.

Die OZG-Umsetzung hat viele Entwicklungsfelder auf dem Weg zu einer digitalen Verwaltung aufgezeigt. Auf Grundlage dieser Erkenntnisse stehen im dritten Schwerpunkt „OZG 2.0" die Mitgestaltung des OZG-Nachfolgegesetzes sowie die Weiterentwicklung der interföderalen Zusammenarbeit im

Mittelpunkt. Konkret wird sich Hessen als Vorsitz dafür einsetzen, Hürden in der Verwaltungsdigitalisierung abzubauen, die Ende-zu-Ende-Digitalisierung von Verwaltungsprozessen voranzutreiben und neue Dialogformate zwischen Bund, Ländern und Kommunen zu etablieren.

Dialog intensivieren

Begleitet wird die thematische Arbeit von der Weiterentwicklung der Governance im IT-Planungsrat, um eine noch höhere Wirksamkeit des Gremiums zu erreichen. Neben den mehrjährigen Schwerpunktthemen soll durch die Einrichtung fachpolitischer Sprecher als Schnittstelle zu den Fachministerkonferenzen die Verzahnung der Gremienarbeit verbessert werden. Zudem sollen die föderalen Arbeitsstrukturen unterhalb des IT-Planungsrats gestrafft und in den Sitzungen selbst mehr Raum für den strategischen Austausch und weichenstellende Entscheidungen für die digitale Transformation etabliert werden. Ein besonderes Augenmerk wird Hessen auf das Kommunalgremium des IT-Planungsrats legen. Mir ist es wichtig, diesen Dialog zu intensivieren, um die Umsetzung der Verwaltungsdigitalisierung im Gefüge von Bund, Ländern und Kommunen zu optimieren.

Wirksamer werden

Ebenso muss die FITKO als „Umsetzungsmuskel“ des IT-Planungsrats weiter ertüchtigt und strategisch passgenau ausgerichtet werden. Wir haben daher die vor drei Jahren bei der Gründung der FITKO getroffenen Annahmen bewertet und an die aktuellen Rahmenbedingungen angepasst. Denn wir wollen, dass die FITKO in der länder- und ebenenübergreifenden Verwaltungsdigitalisierung noch wirksamer wird. Nur so können wir das gemeinsame Ziel einer umfassenden Digitalisierung der Verwaltung schnell und effektiv erreichen.

// SAVE THE DATE

Die Vorbereitungen für den nächten Kongress HEssen DIGITAL laufen bereits. Das Event findet am 8. März in Bad Homburg statt.

IT-Sicherheitstag Sachsen

Der menschliche Faktor in der Informationssicherheit

16. Juni 2022 | Dresden

Deutsches Hygienemuseum

www.sicherheitstag-sachsen.de

IT-SICHERHEITSTAG SACHSEN

Gemeingefährliche IT-Sicherheitsmuffel

Der menschliche Faktor

〉〉〉 von **Benjamin Hilbricht,** Behörden Spiegel

Die Hälfte aller Cyber-Angriffe gelingt nur, weil ein Mensch einen Fehler macht. Also fordern manche IT-Sicherheitsverantwortliche Lösungen, bei denen Nutzerinnen und Nutzer möglichst wenig selbst machen. Andere wollen sie durch Aus- und Fortbildung zu Sicherheits-Assets machen. Der richtige Weg wurde auf dem IT-Sicherheitstag Sachsen 2022 kontrovers diskutiert.

„Ich kenne einen hochkarätigen Juristen, der ein Tool im Gebrauch hatte, das Mausbewegungen simuliert, damit der Bildschirmschoner nicht angeht", erzählt Katja Thalheim-Heinecke von der Hochschule Meißen (FH) und Fortbildungszentrum. Der Mann habe aus Bequemlichkeit seine sämtlichen Daten ungeschützt gelassen. Jeder habe ohne Passwortabfrage auf seinen PC zugreifen können.

Zu kompliziert, zu teuer?

Wie sollen Dienstherren mit Mitarbeitern umgehen, die quasi die Maskenmuffel der IT-Security sind? Ähnlich wie bei der Corona-Impfung schöben die Menschen die angeblichen Nebenwirkungen vor, um sich nicht mit IT-Sicherheit befassen zu müssen, sagt Jörg Steinig. Der Beauftragte für Informationssicherheit des Landes (CISO) Freistaat Sachsen listet auf: „Zu kompliziert, zu teuer …"

Uwe Hoppenz, Fachbereichsleiter Cyber-Sicherheit in mobilen Infrastrukturen und Chiptechnologie, Bundesamt für Sicherheit in der Informationstechnik (BSI) Freital, stimmt ihm zu. Aber er sagt auch: „Wenn wir immer auf den Nutzer einschlagen, werden wir keinen Gewinn haben." Deswegen bemühe sich das BSI beim Aufbau des 5G- und 6G-Netzes, den User in den Mittelpunkt zu stellen. „Wir müssen es einfach handhabbar machen", betont er. „Sicherheit muss für den Nutzer lebbar sein."

„Wenn ich nicht verstehe, warum ich etwas tue, mache ich es nicht", erklärt Sandra Balz. Balz leitet die Geschäfte der Transferstelle IT-Sicherheit im Mittelstand (TISiM) des Vereins Deutschland sicher im Netz e.V. (DsiN). Aufgrund

ihrer Arbeit hat Balz viel Erfahrung mit den Opfern von Cyber-Attacken. Sie sagt, mit der IT-Sicherheit sei es wie mit Pillen, die ein Arzt verschreibe. Wenn die Patienten nicht einsähen, warum sie die Medikamente bräuchten, dann nähmen sie sie nicht. Wie soll eine Behörde mit Mitarbeitern – teilweise auch Führungskräften – umgehen, die ein IT-Sicherheitsrisiko sind? Es gibt technische Lösungen. „Die Sensorik, die uns durch Technik verloren gegangen ist, müssen wir durch Technik ersetzen", stellt Steinig fest. So könne ein Programm herausfinden, ob ein Administrator sich dreimal falsch angemeldet habe. Oder dann automatisch Alarm schlagen, wenn sich jemand um drei Uhr nachts von einem amerikanischen Server aus anmelde. Das ist aber nur die Ebene der Detektion. Innerhalb eines gesicherten Netzwerks müssen andere Vorkehrungen ergriffen werden. Nach dem Zero-Trust-Prinzip bekommen Mitarbeitende nur diejenigen Berechtigungen, die sie absolut brauchen, um in einem System zu arbeiten. Das ist eine Entmündigung. Aber mit so einem Ansatz kann zumindest nicht der Praktikant Firmengeheimnisse ins Internet stellen.

Andererseits kann man die Mitarbeiter besser ausbilden. Sie müssen wissen, wie Passwörter sicher gesetzt und verwahrt werden, dass und warum man Updates machen muss. Aber: „Ein IT-Mensch spricht sein Fachchinesisch und denkt, alle verstehen ihn, weil alle nicken. Dabei wollen sie nur nicht zugeben, dass sie keine Ahnung haben", sagt Roland Schreckenberger, jetzt Leiter bei ML Cyber Sec bei der ML Gruppe. Früher war er Informationssicherheitsbeauftragter der Stadt Troisdorf. Aus diesen Erfahrungen hat er zwei Erkenntnisse destilliert. Erstens sollten IT-Beauftragte eine Liste mit verbotenen Worten bekommen: kein „Script", „Ransomware", „Malware"… Die würden Laien nur verunsichern. Zweitens müsse einer sich quälen: die User oder die IT-Abteilung. Es sei die Aufgabe der Letzteren, den Usern ihre Aufgaben so leicht wie möglich zu machen.

Was passiert, wenn alles schiefgeht

Aber manchmal läuft alles schief, so wie 2021 in der Kommune Anhalt-Bitterfeld. Die meisten wissen, wie sie sich bei Verkehrsunfällen oder bei Einbrüchen verhalten müssen. Doch bei Cyber-Angriffen auf ihr Unternehmen zahlen viele das Lösegeld und halten die Polizei aus dem Spiel.

„Informieren Sie die Polizei! Wir müssen wissen, dass etwas passiert", sagt Henrik Hohenlohe in Richtung der Opfer von Cyber-Angriffen. „Sicher nicht, weil ich Ihnen verspreche, dass wir das Verbrechen aufklären", fährt der Leiter des Cybercrime Competence Centers Sachsen (SN4C) dann fort. Nur jeder dritte Vorfall werde aufgeklärt. Aber die Sächsische Polizei sei gut vernetzt. Neben rund 90 Kräften im SN4C sei sie angebunden an das Bundeskriminalamt (BKA) und die anderen Landespolizeien. Zudem unterhalte das SN4C gute Beziehungen zum Bitkom e.V. und großen IT-Unternehmen. Wenn man bei einem Fall nicht weiterkomme, hole sich das SN4C Unterstützung aus der Wirtschaft. „Das Ganze ist auch kostenfrei." Hohenlohe lächelt verschmitzt. „Wir haben kein Geschäftsmodell, das dahintersteht."

Welchen Stellenwert hat der User für sichere IT? Dies diskutierten (v.l.n.r.:) Uwe Hoppenz (BSI Freital), Jörg Steinig (CISO Freistaat Sachsen), Moderator Uwe Proll, Sandra Balz (TISiM-Geschäftsstellenleiterin, DSiM) und Henrik Hohenlohe (Leiter des SN4C, LKA Sachsen). Foto: BS/Hilbricht

Eine Lücke geschlossen …

… tausend neue geöffnet

⟩⟩⟩ von **Paul Schubert,** Behörden Spiegel

Der Nachrichtenwert der Cyber-Sicherheit steigt täglich. Leider sind das keine guten Nachrichten, handelt es sich dabei meist um Berichterstattung über erfolgreiche Cyber-Angriffe. Mittlerweile stehen für Firmen Cyber-Attacken auf Platz eins der Geschäftsrisiken, erläuterte Thomas Popp, Mitglied der Staatsregierung und CIO der sächsischen Staatskanzlei, auf dem IT-Sicherheitstag Sachsen 2022 des Behörden Spiegel. Das Nachbarland von Sachsen, Sachsen-Anhalt, hat in dieser Thematik seine besonders bitteren Erfahrungen gemacht.

Die Rede ist vom medienwirksamen Angriff auf die Kommunalverwaltung Anhalt-Bitterfeld im vorletzten Jahr. Solche erfolgreichen Hacker-Angriffe gefährdeten die Versorgungssicherheit für Bürgerinnen und Bürger, seien aber nur die „Spitze des Eisbergs", sagte Popp. In Anhalt-Bitterfeld waren mehr als 1.000 Computer und 159 Programme von der Cyber-Attacke betroffen.

Thomas Popp (vorne re.), Mitglied der Staatsregierung und CIO der sächsischen Staatskanzlei, im Gespräch mit einem Cyber Security-Unternehmen auf dem IT-Sicherheitstag Sachsen. Foto: BS/Schubert

Cyber Crime als Dienstleistung

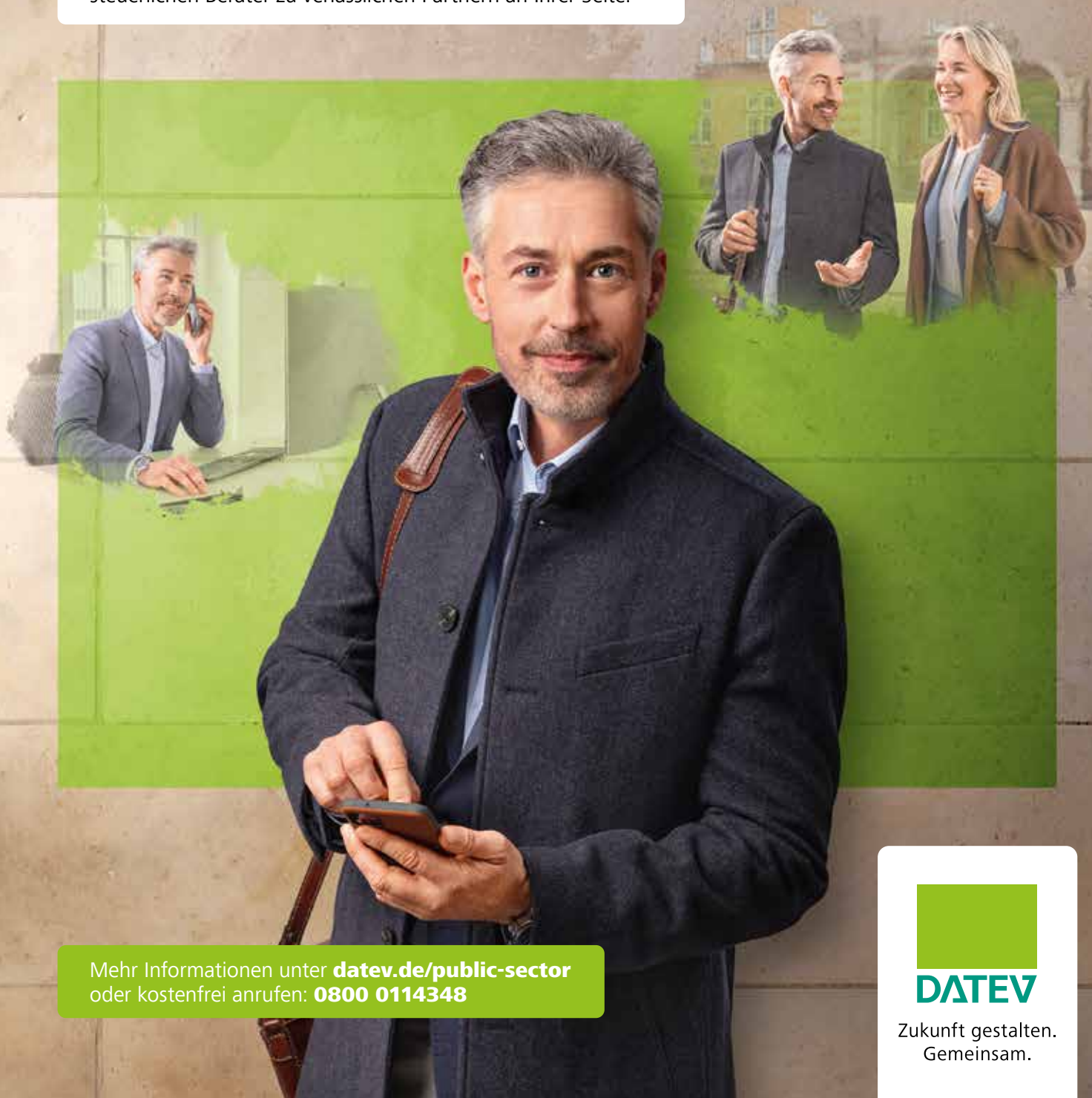
Des Weiteren sei die Arbeit von Rechnungswesen und Führerscheinstelle extrem eingeschränkt oder gar nicht verfügbar gewesen, erklärte Henrik Hohenlohe, Leiter der zentralen Ansprechstelle Cybercrime im Landeskriminalamt Sachsen. Auch er beobachtet, dass Wirtschaft und Verwaltung immer mehr von Cyber-Attacken betroffen sind: „Cyber-Angriffe betreffen mittlerweile neun von zehn Unternehmen." Ein besonders großes Problem entstehe durch Cyber Crime as a Service, erläuterte Hohenlohe: „Dabei handelt es sich um illegale Marktplätze mit Kaufhaus-Charakter. Die Nutzenden haben einen leichten Zugang zu den Angeboten und brauchen keine Expertise, um eine "Dienstleistung" zu erwerben. Er forderte einen Dreiklang aus IT-Sicherheit, Strafverfolgung und Awareness bei den Nutzenden. Nur so könne man der Entwicklung der steigenden Cyber-Gefahr entschlossen entgegentreten.

Awareness steigern

Durch das sächsische Informationssicherheitsgesetz werden die sächsische Staatsverwaltung und die sächischen Kommunen zu Aufbau und Unterhaltung einer angemessenen Informationssicherheit verpflichtet. Dennoch gestaltet sich die Bekämpfung im Freistaat schwierig: „Wenn wir eine Sicherheitslücke schließen, schaffen Kriminelle tausend neue", sagte Staatssekretär Popp. Er forderte dazu auf, die Awareness vor allem bei den Kleinunternehmern zu steigern. Diese sähen sich oft nicht als Angriffsziel: „Auch wenn sie ‚nur' Opfer von Kollateralschäden werden, können sie nicht mehr arbeiten", so Popp. Der CIO der sächsischen Staatskanzlei rief weiterhin dazu auf, die IT-Infrastrukturen resilienter zu gestalten. Doch sei das nicht das Hauptproblem: „Am Ende müssen wir die Mitarbeitenden mitnehmen. Das wichtigste sind sensibilisierte Bedienstete und Führungskräfte." Der Faktor Mensch sei leider immer noch der anfälligste Punkt bei der Cyber-Sicherheit, resümierte Popp.

SIE SORGEN DAFÜR, DASS DAS ÖFFENTLICHE LEBEN FUNKTIONIERT. WIR BEGLEITEN SIE DABEI MIT SMARTEN LÖSUNGEN IN DIE DIGITALE ZUKUNFT.

In der Verwaltung sind digitale Lösungen der Weg, um den öffentlichen Auftrag optimal zu erfüllen. DATEV bietet dafür leistungsstarke und rechtssichere Software für Finanz-, Personalwesen und Verwaltungsprozesse. Das macht DATEV und die steuerlichen Berater zu verlässlichen Partnern an Ihrer Seite.



Mehr Informationen unter **datev.de/public-sector**
oder kostenfrei anrufen: **0800 0114348**

DATEV

Zukunft gestalten.
Gemeinsam.

Live-Hackings für Schülerinnen und Schüler

Sächsische Staatsregierung sensibilisiert für IT-Sicherheit

Sensibilisierungsaktionen gegen Cyber-Attacken sind in der heutigen Zeit notwendiger denn je. In Sachsen werden sogar schon Schülerinnen und Schüler auf die Thematik aufmerksam gemacht. Ein Interview mit dem Staatssekretär für Digitale Verwaltung und Verwaltungsmodernisierung der sächsischen Staatsregierung Thomas Popp über Aufklärung über Cyber-Sicherheit und die Cyber-Bedrohungslage im Freistaat.

***Behörden Spiegel:** Jeden Tag sind Meldungen über Sicherheitslücken, Angriffsversuche und Systemausfälle zu verzeichnen. Wie bewerten Sie die aktuelle Bedrohungslage für die sächsische Verwaltung? Wie gut ist sie aufgestellt?*

Popp: Die Gewährleistung der IT-Sicherheit stellt für die sächsischen Behörden eine besondere Herausforderung dar. Bereits im Vorfeld des russischen Angriffskriegs in der Ukraine bestand eine hohe Gefährdungslage aufgrund von Schwachstellen in Softwarekomponenten, die Cyberattacken erst ermöglichen, denken Sie nur an die Exchange- Lücke oder die Log4Shell Schwachstelle – beides vom BSI mit der höchsten Warnstufe Rot versehen. Daneben gibt es ein permanent hohes Grundrauschen bei Cyber-Angriffen. Die gemeinsamen Schutzsysteme von kommunalem und Landesverwaltungsnetz wehren täglich eine Vielzahl von Angriffen verschiedenster Angriffsvektoren erfolgreich ab. Im Kontext des Krieges haben wir weitere technische Maßnahmen veranlasst, um insbesondere die Übergänge von Diensten in das Internet abzusichern. Insgesamt bewerte ich die Lage als angespannt, aber wir haben Mittel und Wege, uns zu schützen.

Thomas Popp ist Staatssekretär für Digitale Verwaltung und Verwaltungsmodernisierung, Mitglied der Staatsregierung und CIO sowie Beauftragter der Sächsischen Staatsregierung für die Kulturhauptstadt Europas 2025.

Foto: BS/Matthias Rietschel

Wie versucht die sächsische Staatsregierung, Bürgerinnen und Bürger für Cyber-Attacken zu sensibilisieren?

Popp: Vor der Corona-Pandemie gab es zusammen mit den sächsischen Volkshochschulen und der Verbraucherzentrale regelmäßig Sensibilisierungsveranstaltungen für Bürgerinnen und Bürger, sogenannte Live-Hackings. An den gut 50 Veranstaltungen nahmen über 5.000 Teilnehmer teil. Wir prüfen derzeit, dieses Format wieder aufleben zu lassen. Zudem möchte ich auf die Präventionsangebote der Polizei und auf die Aktivitäten zum Verbraucherschutz verweisen, die das BSI forciert. Wie bei allen anderen Bereichen im Leben gilt jedoch auch bei der Cyber-Sicherheit: Jeder ist zunächst selbst verpflichtet, sich über Risiken und Nebenwirkungen zu informieren und entsprechend zu handeln. Angebote dafür findet man leicht. Im Familien- und Freundeskreis ist immer jemand, den man fragen kann. Es sollte eben nicht so sein, dass viele über Bildschirmgröße, Prozessorkapazitäten und Speichergeschwindigkeit diskutieren können, aber nur wenige die Einstellungen und Verhaltensweisen für die datensparsame, sichere Nutzung des Endgeräts kennen. Cyber-Gefahren und Cyber-Vorkehrungen gehören zur Kompetenz-Grundausstattung in diesen Zeiten.

Werden Schülerinnen und Schüler in Sachsen in dieser Thematik besonders unterstützt?

Popp: Im Rahmen der bereits genannten Live-Hackings gab es mehrfach Veranstaltungen, die sich speziell an Schülerinnen und Schüler richteten. Zudem unterstützen wir das Sächsische Landesamt für Schule und Bildung am „Safer Internet Day". Zu diesem jährlichen Aktionstag richten wir Sensibilisierungsformate speziell für Schulen aus. Während der Corona-Pandemie geschah dies online. 2022 haben ungefähr 2.100 Schülerinnen und Schüler aus 39 Schulen an den Angeboten teilgenommen. Das pädagogische Personal wird in separaten Veranstaltungen ebenfalls fortgebildet. So wird ihm das Rüstzeug an die Hand gegeben, das Thema Cyber-Sicherheit an geeigneter Stelle in den Unterricht einzubinden.

Die Gesetze zur Informations- und Cyber-Sicherheit werden immer schärfer und enthalten immer mehr Anforderungen. Was kommt auf die deutsche Verwaltung in den nächsten Monaten und Jahren zu? Ist das angemessen?

Popp: Die bestehenden Gesetze zur Erhöhung der Informationssicherheit sind unbedingt notwendig und keinen Deut zu scharf. Eine unsichere Digitalisierung können wir uns nicht erlauben: nicht als Wirtschaft, nicht als Gesellschaft und erst recht nicht als Staat. Wir in Sachsen haben mit dem Sächsischen Informationssicherheitsgesetz eine starke rechtliche Grundlage geschaffen, um die Wehrhaftigkeit gegen Cyber-Angriffe zu erhöhen und fortlaufend an die jeweiligen Lagebedingungen anpas-

sen zu können. Dieses Gesetz stellt die Geschäftsgrundlage für unser Handeln dar. Andere rechtliche Rahmen wie das IT-Sicherheitsgesetz des Bundes, die neue NIS2-Richtlinie oder auch zuletzt die Sicherheitsverordnung zum OZG-Portalverbund sehe ich grundsätzlich positiv. Sie ergänzen, wofür wir mit unserem Landesgesetz den Boden bereitet haben: Informationssicherheit ist ein Grundpfeiler der Digitalisierung! Wir müssen das bei allen Digitalisierungsmaßnahmen von Anfang an mitdenken und das muss bei den Führungskräften anfangen.

Mit zunehmenden fachlichen Anforderungen benötigt die Verwaltung vermutlich auch mehr Personal mit den entsprechenden Kompetenzen. Wie will der Freistaat Sachsen dem Problem des Fachkräftemangels im IT-Bereich bzw. IT-Sicherheitsbereich in der Verwaltung entgegenwirken?

Popp: Wichtig ist zunächst, ein möglichst genaues Bild über die Entwicklung vorliegen zu haben. Dafür hat die Sächsische Staatsregierung eine Strategiekommission „Organisation/Personal" unter meiner Leitung eingesetzt. Die Kommission erarbeitet verlässliche Informationen darüber, welche staatlichen Aufgaben mit welchem Personaleinsatz zu bewältigen sind. Die Ergebnisse der Kommission werden eine verlässliche Basis für die künftige Aufgaben- und Personalpolitik im Freistaat Sachsen sein. Schon jetzt wissen wir, dass uns der Fachkräftemangel im IT-Bereich große Probleme bereiten wird. Für Spezialisten im IT-Bereich bzw. IT-Sicherheitsbereich ist der Konkurrenzkampf mit der Wirtschaft in vollem Gange. Das gilt auch für andere Fachbereiche. Die demografische Entwicklung setzt den gesamten Arbeitsmarkt unter Druck. Wir setzen auf eigene Ausbildungs- und Fortbildungsangebote, um dies wenigstens teilweise abzufedern. Wir versuchen, die Verwaltung als den attraktiven Arbeitgeber bekannt zu machen, der er ist. Dazu gehören die Vereinbarkeit von Familie und Beruf, eine sinnstiftende Tätigkeit für das Gemeinwesen und zeitgemäße Arbeitsplatzausstattung sowie flexible Arbeitszeitmodelle. Dieses Bündel an Vorteilen lässt den Umstand einer teilweise geringeren Vergütung im Staatsdienst für viele Jobsuchende in den Hintergrund treten.

// SAVE THE DATE

Die Vorbereitungen für den nächten IT-Sicherheitstag Sachsen laufen bereits. Das Event findet am 28. Juni in Dresden statt.

OZG, SDG, RegMoG, eIDAS, ERV, Peppol ...

An Ihrer Seite zur Umsetzung der „Akronymen-Vorhaben": Governikus

Die Digitalisierungsvorhaben nehmen jenseits der erlaubten Höchstgeschwindigkeit Fahrt auf, die Akronyme auf den Schildern am Straßenrand nehmen deutlich zu. Und doch müssen alle berücksichtigt bzw. eingehalten werden, damit das große und keineswegs ausschließlich nationale Ziel auch erreicht werden kann: Verwaltungsvorgänge zum Nutzen von Bürgerinnen und Bürgern UND Verwaltungsmitarbeitenden zu digitalisieren.

Sichere Identitäten, sichere Kommunikation, sichere Daten.

Überall dort, wo Personen und Organisationen sicher identifiziert, Daten sicher und vertraulich übermittelt oder Datenunverfälschtheiten sicher nachgewiesen werden müssen, können Sie sich auf die Basisdienste und -funktionsbausteine verlassen, die Governikus im Auftrag von Bund und Ländern entwickelt.

Im Fokus stehen hierbei aktuell die verschiedenen Akronyme für das Onlinezugangsgesetz (2.0), Nutzer- und Unternehmenskonto bzw. Unternehmenspostfach, die Single-Digital-Getaway-Verordnung, das Registermodernisierungsgesetz, die Überarbeitung der eIDAS-Verordnung, Infrastrukturen im Kontext eRechnung, der elektronische Rechtsverkehr mit seinen besonderen Postfächern etc. und natürlich auch die Umsetzung der Smart-eID. Technische Richtlinien des BSI, europäische ETSI- und nationale KoSIT-Standards sind dabei unsere Leitplanken.

Mit der Anwendung Governikus, der Anwendung GMM, DVDV sowie EGVP und SAFE (um noch ein paar weitere Akronyme ins Spiel zu bringen) entwickeln und pflegen wir Produkte des IT-Planungsrats sowie der Justiz. Die Weiterentwicklungen der damit bei Bund und Ländern zur Verfügung stehenden Basisdienste und Standardbausteine sind darauf ausgerichtet, die vielen Vorhaben zu unterstützen: mit Lösungen zur Nutzung des Online-Ausweises, für interoperable Nutzerkonten, zur Zustimmung für Registerabfragen, zur Erstellung von eIDAS-Signaturen und deren Validierung, zur Beweiswerterhaltung, für sichere Transportinfrastrukturen, wie OSCI, Peppol etc. – um nur ein paar zu nennen.

Daran und an vielen anderen Themen arbeiten über 200 Governikus-Mitarbeitende gemeinsam in engem Dialog mit Kunden, Partnern und in unterschiedlichen Gremien für eine optimale Vernetzung. Denn unser Zielbild ist die digitale Souveränität in einer komplex vernetzten Welt.

www.bw-4-0.de #bw40

BADEN-WÜRTTEMBERG 4.0

Es brodelt im Kessel

Nur punktuelle Einigkeit zwischen Land und Kommunen

⟩⟩⟩ von **Matthias Lorenz,** Behörden Spiegel

In Baden-Württemberg ist man der Überzeugung: „Kein Blatt Papier passt bei der Digitalisierung der Verwaltung zwischen Land und Kommunen." Dies wird zumindest von Landesseite immer wieder betont. Betrachtet man jedoch die Umsetzung des Onlinezugangsgesetzes (OZG), kommen Zweifel an dieser Aussage. Zwar bietet beispielsweise die Plattform „ServiceBW" den Kommunen eine echte Unterstützung, trotzdem ist die Stimmung auf der kommunalen Ebene vielerorts alles andere als gut.

Die Rolle der Plattform „ServiceBW" betonte beispielsweise Marius Herr, der OZG-Koordinator des Landes Baden-Württemberg, auf dem Kongress Baden-Württemberg 4.0 2022: „Diese Plattform ist der zentrale Dreh- und Angelpunkt, an dem wir Verwaltungsleistungen digitalisieren wollen." Sie sei aufgrund ihrer modularen Aufbauweise in dieser Form einzigartig in Deutschland. Auch stelle man auf ihr den sogenannten Universalprozess bereit, mit dessen Hilfe Kommunen relativ einfach digitalisieren könnten.

Intensiv genutzt wird „ServiceBW" beispielsweise von der Stadt Mannheim. Deren Abteilungsleiterin IT-Qualitätsmanagement und digitale Strategie, Judith Geiser, erzählte von der Doppelstrategie der Stadt bei der OZG-Umsetzung. Zum einen schließe man sich komplett an „ServiceBW" an, zum anderen setze man jedoch auch auf ein weiteres Serviceportal. Dadurch könne man auch Prozesse aus eigener Motivation heraus digitalisieren. Bis zum Ablaufen der OZG-Umsetzungsfrist Ende 2022 wolle man hauptsächlich den Universalprozess nutzen, kündigte Geiser an. „Wir sind jetzt aber schon an den weniger genutzten Leistungen dran, für die es im Jahr vielleicht 100 Anträge gibt."

Düsteres Bild

Bat man die kommunalen Vertreter auf dem Kongress nach einer Einschätzung des Stands der OZG-Umsetzung, zeichnete sich jedoch ein deutlich düstereres Bild. Die Allermeisten wähnten sich noch am Start der Umsetzung, gerade im

Grafik: BS/Hofmann unter Verwendung von CoreDESIGN, stock.adobe.com

digital@bw

Backend-Bereich schien noch nicht viel passiert zu sein. Gründe für dieses ernüchternde Ergebnis gab es viele. Ein Problem sind die Einer-für-Alle-Leistungen (EfA-Leistungen), welche oft noch nicht zur Verfügung standen und stehen. Das Problem brachte ein Kongressteilnehmer folgendermaßen auf den Punkt: „Wie soll die Bürgermeisterin einer 6.000-Einwohner-Gemeinde allein entscheiden, ob sie jetzt noch auf eine EfA-Leistung warten soll?“ Es brauche also gerade für kleinere Kommunen Hilfe bei der Entscheidungsfindung.

Kostendruck für mehr Einheitlichkeit

Auf Landesebene ist man sich bewusst, dass das EfA-Prinzip auch Schwierigkeiten mit sich bringt. Bei länderspezifischen Verfahren, die man in bundesweite Nutzung bringen wolle, bestehe nun einmal die Möglichkeit, dass andere Bundesländer andere Verfahren einsetzten, erklärte Stefan Krebs, der CDO/CIO der baden-württembergischen Landesregierung. Deswegen habe man sich beim im Frühling 2022 beschlossenen OZG-Booster auf die Digitalisierung von 35 bundeseinheitlichen Lösungen fokussiert. Krebs warnte jedoch vor weiteren Zeitverlusten: „Selbst wenn eine Lösung technisch funktioniert, gibt es manchmal rechtliche Hindernisse, die auf Bundesebene beseitigt werden müssen.“ Ein weiteres Hindernis für viele Kommunen ist die Kostenfrage der OZG-Umsetzung. Wer finanziert die Digitalisierung und den Betrieb der Verwaltungsleistungen? Hier ist noch ein weiter Weg zu gehen: So lehnt es OZG-Koordinator Herr in Bezug auf EfA-Leistungen ab, dass die nachnutzenden Länder die Finanzierung komplett übernehmen. Hier seien Lösungen zu finden. Von kommunaler Seite war folgender Vorschlag zu hören, der für mehr Einheitlichkeit sorgen soll: Das Land oder der Bund bietet den Kommunen für einen einheitlichen Prozess eine Lösung kostenfrei an. Falls eine Kommune diesen Prozess anders umsetzen wolle, müsse sie es selbst zahlen. Durch den Kostendruck werde also für mehr Einheitlichkeit gesorgt. Auch stellt sich nach wie vor für viele Kommunen die Frage nach der richtigen Vorgehensweise. Schließlich schreibt das OZG nur die Digitalisierung des Frontends vor. Thomas Wieland ist der Meinung, beim OZG habe man sich dafür entschieden, zuerst die Fassaden zu bauen und für den Bürger einen Zugang zu schaffen, was sich politisch sehr gut verkaufen ließe. „Aber eigentlich muss man sich mit den Prozessen beschäftigen“, sagte der Leiter Digitalisierung und E-Government der Metropolregion Rhein-Neckar. Für Online-Verwaltungsleistungen müssten Verwaltungsprozesse neu gedacht werden, man könne analoge Vorgehensweisen nicht eins zu eins in die digitale Welt übertragen.

Wichtig sei darüber hinaus die Einbindung der Fachabteilungen, welche selbst für ihre Prozesse verantwortlich seien. Damit bei der Digitalisierung echte Fortschritte erzielt werden könnten, dürfe eins nicht vergessen werden: „Sie müssen Beteiligte zu Betroffenen machen“, stellte Wieland klar.

Prozesse streichen

Prozesse haben sich auch in der Landeshauptstadt Stuttgart geändert. Dort hat man für das neu geschaffene Amt für Digitalisierung, Organisation und IT einen berüchtigten Leiter aus der bayerischen Landeshauptstadt München abwerben können: Thomas Bönig, der in München die Funktion des CDO innehatte und ein harter Kritiker des Onlinezugangsgesetzes ist. Bönig lässt keinen Zweifel daran, dass er auch in Stuttgart keinen Stein unangetastet lassen wird. „Wir werden hier nicht alles so lassen, wie es ist. Mein erster Schritt wird es sein, zu überprüfen, welche Prozesse man streichen kann. Bei den übrig gebliebenen Prozessen wird dann geschaut, welche abgeflacht werden können.“ Das OZG sei nichts weiter als Bürokratie online, kritisiert Bönig. Stattdessen brauche es in der Verwaltung einen tiefgehenden Kulturwandel, an dessen Ende die Verwaltung sich zu einem modernen Dienstleister entwickelt habe. Man müsse beweglicher und agiler werden, brauche eine ehrliche Feedback- und Fehlerkultur. Auch müsse der Mut gefunden werden, echte Visionen zu entwickeln.

Die kommenden Aufgaben fest im Blick: Thomas Bönig hat sich als neuer Leiter des Stuttgarter Amts für Digitalisierung, Organisation und IT als erstes die Abschaffung von Prozessen vorgenommen.

Foto: BS/Mark Gross

Mit dieser Einstellung kann die Landesebene allerdings nicht viel anfangen. „Ich habe keine Vision“, antwortete Dr. Michael Zügel, Referatsleiter E-Government, Open Government, Verwaltungsmodernisierung im Ministerium des Innern, für Digitalisierung und Kommunen Baden-Württemberg, auf die Frage, wie seiner Meinung nach die digitale Verwaltung in fünf Jahren aussehen solle. Politik sei die Kunst des Möglichen. Stattdessen wünscht er sich mehr „Street Credibility“. Man müsse den Bürgern und Unternehmen beweisen, dass der Staat digitalisieren könne. Hier sei der OZG-Booster die Nagelprobe: Gelinge die Umsetzung, habe man die Kurve nochmal gekriegt.

Deutlich wird also: In Land und Kommunen existieren durchaus verschiedene Meinungen, wie die Verwaltungsdigitalisierung in Angriff genommen werden solle. Die gerade von Landesseite oft betonte Einigkeit ist zwar punktuell vorhanden, jedoch längst nicht so ausgeprägt, wie es die Landesregierung gerne hätte. Es brodelt im Kessel.

Smarte Infrastruktur im Ländle

Wie sie gelingt und was sie verhindert

⟩⟩⟩ von **Malin Jacobson,** Behörden Spiegel

Wie smart sind wir? Wie smart können wir werden? Und wie kommen wir dahin? Diesen Fragen stellten sich Vertreterinnen und Vertreter aus Kommunen, Verbänden und der Landesverwaltung Baden-Württembergs auf dem Regionalkongress Baden-Württemberg 4.0 in Stuttgart im Juni 2022.

Man sei auf einem guten Stand, aber es gebe noch Luft nach oben, waren sich die Vertreterinnen der kommunalen Spitzenverbände – Ariane Krüger, Leiterin der Stabsstelle Digitalisierung beim Landkreistag Baden-Württemberg, Leonie König, Referat Digitalisierung des Gemeindetags Baden-Württemberg, und Stella Grießmayer, Leiterin Stabsstelle Digitalisierung beim Städtetag Baden-Württemberg – einig. Diese Einschätzung bestätigte auch eine Studie der Hochschule Kehl, in welcher über 80 einzelne Fallstudien zum Digitalisierungsgrad der baden-württembergischen Kommunen ausgewertet wurden. Philipp Bauer, Wissenschaftlicher Mitarbeiter für Digitalisierung der öffentlichen Verwaltung an der Hochschule Kehl, beschrieb den oftmals zu sehenden Umstand, dass die Digitalisierung zwar immer mehr institutionalisiert werde, aber: „Je kleiner eine Kommune ist, desto größer sind der Ressourcenmangel und die Abhängigkeit von einzelnen Personen."

Gerade große Kreisstädte und Großstädte seien bezüglich Digitalisierungsstrategie, -beauftragten und interkommunaler Zusammenarbeit sehr gut aufgestellt. Bei den Gemeinden und kleineren Städten sowie Landkreisen hätten hingegen nur 20 Prozent eine Digitalisierungsstrategie. Und nur die Hälfte der Gemeinden und kleineren Städte habe einen Digitalisierungsbeauftragten und kooperiere mit anderen Kommunen bezüglich der Digitalisierung. „Auffällig war zudem", so Bauer, „dass fast alle Kommunen angegeben haben, beim Prozessmanagement und der Personalausstattung nicht gut aufgestellt zu sein, den größten Handlungsbedarf allerdings bei OZG, IT-Personal und IT-Kompetenzausbau sehen." Dabei sei vor allem ein gutes Prozessmanagement die Grundlage für eine erfolgreiche Digitalisierung. Laut Selbsteinschätzung der Kommunen lägen die größten Hindernisse in den Bereichen Personalausstattung und Finanzmittel für IT sowie Unterstützung durch die Politik, ergänzte Bauer abschließend.

Ausprobieren und scheitern

Für die Kommunen sei vor allem problematisch, so König, dass aktuell noch andere Herausforderungen außer der Verwaltungsdigitalisierung wichtige Ressourcen bänden. Um dem entgegenzuwirken, ist es ihrer Meinung nach wichtig, die digitalen Infrastrukturen so zu gestalten, dass sie einfach und damit von möglichst vielen Mitarbeitenden zu bedienen sind. Und Krüger forderte eine durchgehende Ende-zu-Ende-Digitalisierung, um einen echten Mehrwert für Kommunen vor Ort zu schaffen – die OZG-Maske für die Bevölkerung reiche da bei Weitem nicht aus. „Da haben gerade die kleinen und niederschwelligen Förderprogramme des Landes viel bewirkt, um in den Kommunen erste Ideen zur Umsetzung zu bringen und Lösungsideen ausprobieren zu können", berichtete Grießmayer. „Ausprobieren und scheitern", empfahl auch Dr. Michael Bauder, Leiter der Stabsstelle Data Science der Stadt Freiburg. Aus diesem Grund habe man in der Stadt

Im Thesen-Pitch „Digitale Kommunen" sprach Jürgen Vogler, Geschäftsführer von procilon, mit Ariane Krüger, Leonie König und Stella Grießmayer (v. l. n. r.) über den Digitalisierungsgrad der baden-württembergischen Kommunen.

Foto: BS/Mark Gross

im Breisgau erst mal mit einem Datenplattform-Prototyp begonnen, um „zu sehen, wo unsere Grenzen sind und wo es mehr Ressourcen braucht“. Zu Beginn habe man Anforderungen wie Echtzeitfähigkeit, Schnittstellendefinition und High-Perfomance-Computing sowie Rahmenbedingungen wie die Integration bestehender Systeme, Governance, OZG oder DIN SPECs definiert, um die Skalierung des Prototyps vornehmen zu können, berichtete der Stabsstellenleiter. Später erfolgten dann der Ausbau bewährter Beteiligungsinstrumente, ein Partizipationsmodell für die Entwicklung und Gestaltung einzelner Maßnahmen sowie der Wissenstransfer und die Ergebnisbewertung. „Das Projekt beruht auf Open Source sowie standardisierten Schnittstellen und Datenformaten,“ erklärte Bauder, „und hat zum Ziel, eine Datenplattform zu kreieren, die zukünftig an die Anforderungen Freiburgs anpassbar und kompatibel mit anderen Systemen ist.“ So wolle man beispielsweise mit den Datenräumen der Uniklinik Freiburg oder dem Fraunhofer EMI zusammenarbeiten können. In vorhandene Apps, beispielsweise von ÖPNV-Anbietern, flössen viele Daten der städtischen Datenerhebung bereits ein – daher werde man auch keine neue App kreieren, so der Freiburger. „Die 37ste Stadt-App lädt sich keiner runter.“

Best Practice

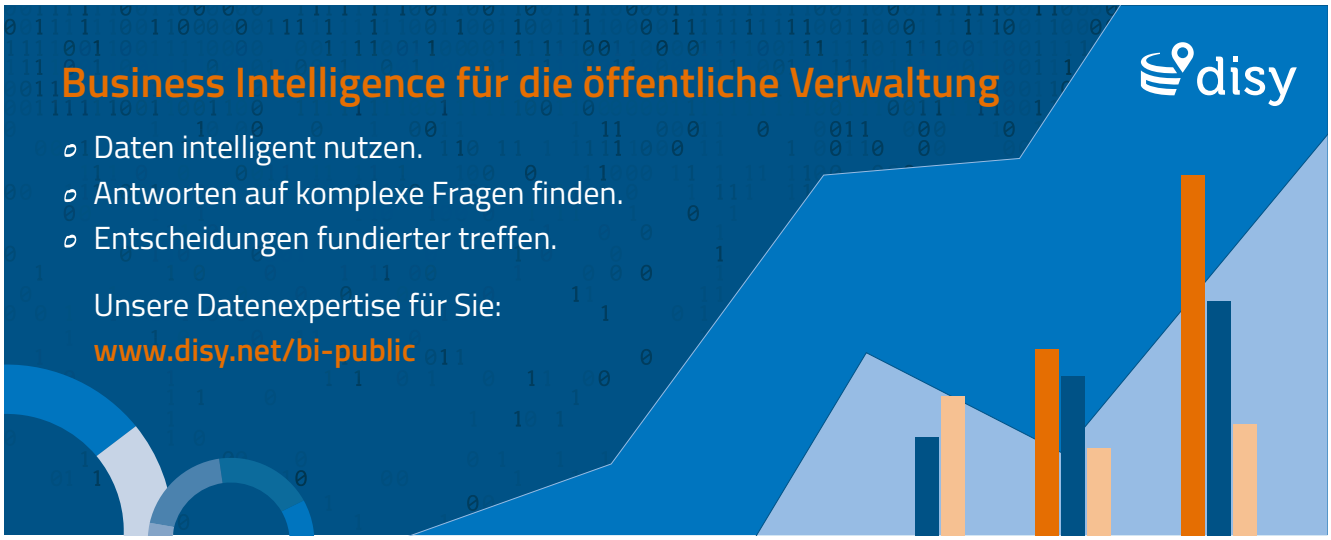
In Ulm kam man zu dem Schluss, dass Stadtentwicklung und Digitalisierung nur zusammen gedacht werden könnten, da die Digitalisierung die Stadt nachhaltig verändern werde, erläuterte Thomas Häufele, Senior Consultant der City & Bits GmbH, welche gemeinsam mit der Geschäftsstelle Digitale Agenda der Stadt Ulm das Projekt Ulm4CleverCity orchestrierte. Als wichtige Orientierungspunkte für eine smarte Stadtentwicklung wurden die Bevölkerungsentwicklung, Nachhaltigkeit und Klimaschutz, der wirtschaftliche Wandel und der Umgang mit Daten definiert. „Es ist wichtig, sich zu überlegen, wohin wir uns langfristig entwickeln, um die entsprechenden Weichen schon heute zu stellen“, meinte der Senior Consultant diesbezüglich. Dabei habe man sich in Ulm auf vier Aspekte fokussiert: Zum einen auf infrastrukturelle Grundlagen, welche sich damit befassten, wie Daten erfasst werden könnten, zum anderen auf die Dateninfrastruktur, die das Zusammenführen und Nutzbarmachen von Daten zum Ziel habe. Des Weiteren auf datenspezifische Ziele, sprich Standards und Schnittstellen, Maschinenlesbarkeit, offene Daten, Datenethik und -souveränität sowie Suffizienz. Und schließlich auf die Datenexzellenzorganisation, die sich mit digitalen Identitäten und der Frage, wer über welche Daten welche Berechtigungen habe, befasse.

Nichts ist statisch

Auf Grundlage der Erfahrungen aus diesem Projekt empfahl der Senior Consultant den anwesenden Kommunalvertreterinnen und -vertretern: „Fangen sie mit einer schon bestehenden Herausforderung an, für die sie eine Lösung suchen, nicht mit irgendeinem gut klingenden Projekt. Schaffen sie Nutzen für Bürgerinnen und Bürger und/oder die Verwaltungsmitarbeitenden. Und investieren sie in den Aufbau von Grundwissen und -kompetenzen ihrer Belegschaft, denn die Prozesse werden immer komplexer.“ Gerade im letzten Punkt sah auch Jens Leyh vom Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO die größte Herausforderung für die Kommunen: „Digitalisierung bedeutet, dass man immer neu dazulernen und sich anpassen muss.“ Für die Kommunen sei das eine große Herausforderung, weil nichts mehr statisch sei und man sich ständig selbst neu erfinden müsse.

// SAVE THE DATE

Die Vorbereitungen für den nächten Kongress BaWü 4.0 laufen bereits. Das Event findet am 29. Juni in Stuttgart statt.



Positive Bilanz von digital@bw

Prävention und Kooperation zentrale Bausteine der Cyber-Sicherheit

Im April 2022 veranstaltete die Landesregierung Baden-Württemberg das „CyberSicherheitsForum". Zudem wurde die Digitalstrategie „digital@bw" im letzten Sommer fünf Jahre alt. Der Behörden Spiegel nahm dies zum Anlass, um mit Thomas Strobl, dem stellvertretenden Ministerpräsidenten sowie Minister des Inneren, für Digitalisierung und Kommunen des Landes, über beide Themen zu sprechen. Das Interview führte Guido Gehrt im Sommer 2022.

***Behörden Spiegel:** Herr Minister Strobl, mit der „Cybersicherheitsagentur" Baden-Württemberg (CSBW) wurde im vergangenen Jahr „das Herzstück der neuen Cyber-Sicherheitsarchitektur des Landes" gegründet. Was zeichnet die CSBW aus?*

Strobl: Die Cybersicherheitsagentur ist unsere Antwort auf die wachsenden Gefahren von Cyber-Angriffen im digitalen Raum. Sie verbessert die Cyber- Sicherheit in Baden-Württemberg. Zum ersten Mal hat das Land damit eine zentrale Koordinierungs- und Meldestelle, die im ständigen Austausch mit allen relevanten Sicherheitsbehörden und Akteuren steht. Zum Beispiel, um Informationen über Schwachstellen und aktuell laufende Angriffsversuche in der Landesverwaltung zu dislozieren und so mögliche Lücken schnellstmöglich zu schließen. Durch die CSBW verhindern wir Doppelstrukturen und sorgen dafür, dass wichtige Informationen alle Beteiligten rasch erreichen, damit die Zusammenarbeit bestmöglich funktioniert. So macht die Cybersicherheitsagentur die Bekämpfung und Abwehr von Sicherheitsbedrohungen im digitalen Raum schlagkräftiger, effektiver und effizienter. Gerade in der aktuellen Lage im Zusammenhang mit dem Ukraine-Krieg stellt die CSBW unter Beweis, dass sie schnell auf akute Situationen reagiert. Sie hat etwa umgehend das Monitoring der IT-Systeme intensiviert und mögliche kurzfristige IT-technische Maßnahmen zum Schutz der Systeme umgesetzt. Die CSBW entwickelte etwa technische Lösungen zur Identifikation der in der Ukraine entdeckten Lösch-Malware und berät die IT-Bereiche des öffentlichen Sektors, um diese Maßnahmen umzusetzen. Der wichtigste Baustein ist freilich die Prävention. Denn bei der Cyber-Sicherheit spielt der Faktor Mensch eine ganz entscheidende Rolle. Es ist deshalb ganz entscheidend, dass die CSBW Verwaltungsmitarbeiter, Bürgerinnen und Bürger für die Gefahren im Cyber-Raum sensibilisiert. Bei der Sensibilisierung hilft uns auch unser „CyberSicherheitsForum". Es findet in diesem Jahr bereits zum vierten Mal statt. Hierzu lade Sie an dieser Stelle ganz herzlich ein. Im Fokus steht in diesem Jahr der Umgang mit unseren Daten und digitalen Anwendungen: Gemeinsam mit Expertinnen und Experten aus Staat, Wirtschaft, Forschung und Gesellschaft beschäftigen wir uns mit dem Thema „Digitale Souveränität".

Bereits seit Februar 2019 unterhält das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Verbindungsbüro in Stuttgart. Wie steht es Ihrer Ansicht nach grundsätzlich um die föderale Zusammenarbeit im Bereich der Cyber-Sicherheit?

Strobl: Das Thema Cyber-Sicherheit kann kein Land alleine lösen – Cyber-Angriffe sind grenzenlos. Nur gemeinsam können wir den aktuellen Gefahren im Netz wirksam begegnen. Eine leistungsfähige und nachhaltige Cyber-Sicherheitsarchitektur erfordert eine gemeinsame Anstrengung von Bund und Ländern und in viel stärkerem Maße künftig auch von Europa. Deshalb findet hier ein sehr guter Austausch mit dem Bund statt. In Baden-Württemberg legen wir großen Wert darauf, unseren verfassungsgemäßen Auftrag im Bereich der Abwehr von Cyber- Angriffen in eigener Verantwortung wahrzunehmen. Darum haben wir die CSBW als zentrale Ansprechpartnerin in Baden-Württemberg für Organisationen der Cyber-Sicherheit geschaffen, sowohl auf Bundes- wie auch Länderebene. Die Zusammenarbeit der föderalen Partner – aber auch innerhalb des Landes – ist ein elementarer Baustein für die Sicherheit im digitalen Raum. So hat sich beispielsweise ein guter und regelmäßiger Austausch zwischen der CSBW und dem CyberCompetenceCenter Hessen3C sowie dem bayerischen LSI etabliert.

Inwieweit verändert sich die Cyber-Bedrohungslage hierzulande durch den Krieg in der Ukraine?

Strobl: Die Bedrohungslage im Zusammenhang mit dem Ukraine-Krieg hat sich noch einmal verschärft. Es besteht zwar gegenwärtig keine akute Gefährdung. Diese Situation kann sich freilich jederzeit ändern. Uns liegen Informationen vor, dass es in Bälde zu einer konkreten Lageverschärfung mittels Cyber- Angriffen auf Hochwertziele kommen könnte. Dies ist übrigens auch die Einschätzung des BSI. Bislang kam es in Deutschland nur zu einigen wenigen Vorfällen, die in Zusammenhang mit dem Krieg in der Ukraine stehen. Allerdings sind beispielsweise auch erste Phishing-Mails mit Bezug zum Ukraine-Krieg auf Deutsch im Umlauf. Hier ist jeder Einzelne zur Vorsicht und Wachsamkeit aufgerufen.

Im Sommer 2017 wurde die Digitalstrategie „digital@bw" verabschiedet. Nach fast fünf Jahren Umsetzung: Wie fällt ihre Zwischenbilanz aus? Steht ggf. ein größeres „Update" an?

Strobl: Unsere Bilanz ist sehr positiv. So können wir auf große Fortschritte im Bereich der Cyber-Sicherheit, der Künstlichen Intelligenz, der Green-IT und beim Gigabit-Ausbau zurückblicken. Dies bestätigt uns auch eine 2021 erstellte Studie des Zentrums für Europäische Wirtschaftsforschung ZEW zu Chancen und Herausforderungen der Digitalisierung in Baden-Württemberg. Derzeit gehen wir die uns dort aufgezeigten weiteren Optimierungspotenziale und Herausforderungen an. So haben wir bereits Ziele und Schwerpunkte für eine weiterentwickelte Digitalisierungsstrategie festgelegt, die wir dieses Jahr verabschieden wollen.

Thomas Strobl ist seit 2016 u. a. Digitalisierungsminister des Landes Baden-Württemberg. Er hat nicht nur das „CyberSicherheitsForum" am 13. April 2022 unterstützt, sondern war im vergangenen Jahr auch Schirmherr des Kongresses „Baden-Württemberg 4.0" am 30. Juni in Stuttgart. Foto: BS/Laurence Chaperon

Die Digitalisierung der Verwaltung hat in den vergangenen Jahren spürbar an Dynamik zugenommen. Dennoch, das sagen auch die Beteiligten, dauert die Implementierung neuer Technologien im Behördenbereich oftmals noch zu lange, insbesondere vor dem Hintergrund immer kürzerer Innovationsintervalle. Was kann man tun, um hier Prozesse zu beschleunigen?

Strobl: Die Corona-Pandemie ist ein Booster für die Digitalisierung: Auch der Letzte hat gemerkt, wie wichtig das schnelle Internet für uns alle ist – und unsere gigantischen Investitionen und unsere ambitionierte Arbeit der letzten fünf Jahre waren so was von richtig. Nun setzen wir alles daran, dass die Menschen im Land die Digitalisierung in allen Lebensbereichen bestmöglich nutzen können. So ist es unser klares Ziel: Das Amt muss zu den Bürgerinnen und Bürgern kommen und nicht umgekehrt. Ob Baugenehmigungen, Elterngeld, Geburtsurkunden oder Gewerbeanmeldungen: All das soll „24/7" – 24 Stunden am Tag, 7 Tage die Woche – vom heimischen Schreibtisch oder Sofa aus erledigt werden können. Mir ist bewusst, dass die Modernisierung der Verwaltung an der einen oder anderen Stelle oftmals noch zu viel Zeit – und übrigens auch viel Kraft – in Anspruch nimmt. Um hier schneller voranzukommen, ist eines ganz wichtig: Digitalisierung bedeutet auch, Dinge auszuprobieren und mit Projekten an die Öffentlichkeit zu gehen, die noch nicht zu 100 Prozent optimiert sind – auch auf die Gefahr hin, dass beispielsweise eine digitale Verwaltungsleistung nicht auf Anhieb perfekt ist. Dies freilich erfordert eine Art und Weise zu arbeiten, die der öffentlichen Verwaltung sowie der politischen und medialen Szene bisher eher fremd ist. In den Behörden ist oftmals und zu Recht ein ausgeprägtes Bedürfnis für Verfahrenssicherheit und Fehlerfreiheit vorherrschend. Das politische Umfeld und die mediale Öffentlichkeit verzeihen keine Fehler – Häme und Spott sind nicht nur im Netz schnell bei der Hand. Gerade bei der Digitalisierung ist dagegen eine agile, ja auch mal mutige Pionierarbeit gefragt: Neues wagen, Risiken eingehen, pfiffige Lösungen erarbeiten. Mut, Ambition und eine anerkannte Fehlerkultur sind hier der Schlüssel zum Erfolg! Hier haben wir bei uns im Land durchaus Luft nach oben ... Aktuell haben gerade im letzten Jahr viele Kommunen auch Einsatz gezeigt, sie haben gemeinsam mit dem Land intensiv getüftelt und dabei tolle Ergebnisse produziert. Doch erst wenn jede einzelne Kommune sich der Digitalisierung annimmt, erreichen wir unser Ziel einer flächendeckenden digitalen Verwaltung im Flächenland Baden-Württemberg. Hierfür brauchen wir klare technische, organisatorische und kommunikative Standards beim Land und bei den Kommunen. Wir reden noch zu oft aneinander vorbei, obwohl wir dasselbe meinen. Wir benötigen mehr Fachkräfte in den Landkreisen, Städten und Gemeinden. Leider macht der Fachkräftemangel auch vor dem Öffentlichen Dienst nicht Halt. Ich spreche hier ausdrücklich nicht nur von Informatikerinnen und Informatikern, sondern von Projektleiterinnen und Projektleitern, von Menschen, die um die Ecke denken und Gegebenes kritisch hinterfragen – zu Neuem bereit sind. Und zu guter Letzt benötigen wir finanzielle Ressourcen bei den Behörden im Land. Den Aufbau einer digitalisierten, den Nutzerinnen und Nutzern zugewandten Verwaltung, aus meiner Sicht ein Mammutprojekt, gibt es eben nicht zum Nulltarif. Das müssen einfach alle wissen: Wer langfristig sparen möchte, muss hier erst mal kräftig investieren. Es gilt wieder mal die einfache Wahrheit: ohne Moos nix los.

Vom Bund ins Land und in die Kommune

(Sichere) digitale Verwaltung für alle

⟩⟩⟩ von **Paul Schubert,** Behörden Spiegel

Sicherheit spielt heute nicht nur in der physischen, sondern auch in der digitalen Welt eine große Rolle. Bund, Land, Kommunen und Kritische Infrastrukturen (KRITIS) vor Gefahren im Netz zu schützen, ist nicht erst seit dem Cyber-Angriff auf den Landkreis Anhalt-Bitterfeld ein Dauerbrenner beim größten Digitalangebot des Behörden Spiegel – dem Digitalen Staat Online (DSO).

Themen des ÖD und mehr

Mit dem Schwerpunkt Spot|On|IT-Security haben wir uns auf DSO insbesondere mit sicherheitstechnischen Aspekten wie der Schatten-IT, IT-Sicherheitsstrukturen und sicheren Verwaltungsnetzen beschäftigt. Die Diskussionsrunden richteten sich dabei vor allem an Mitarbeitende und Interessierte des Öffentlichen Dienstes. Aber auch aktuelle weltpolitische Themen, wie die Auswirkungen des Ukraine-Krieges auf den deutschen und internationalen Raum, wurden beleuchtet. Wie funktioniert Desinformation? Welche Effekte hatte der Ruf der Ukraine nach zivilen IT-Kräften, die das Land in ihrem Verteidigungskrieg unterstützen sollten? Was ist Hybrid Warfare? Zusammen mit Expertinnen und Experten der zivilen IT-Branche, Wissenschaftler und Wissenschaftlerinnen und Verwaltungsmitarbeitenden gingen wir den brandaktuellen Themen aus 2022 auf den Grund.

Der Digitale Staat Online wurde auch für spontane Liveübertragungen – wie hier mit Bundeskanzler Olaf Scholz (SPD) und seinem norwegischen Kollegen Jonas Gahr Støre – genutzt. Screenshot: BS/Schubert

Ausführliche Thementage

Neben der IT-Sicherheit befasste sich die Veranstaltungsplattform 2022 im Rahmen von Thementagen mit ausgewählten Inhalten eindringlicher. Dabei wurden unter anderem die Cloud-Strategie des Bundes mit Entscheidungsträgern beleuchtet oder die digitale Souveränität der deutschen Verwaltung in den Blickpunkt gestellt. Durch Keynotes konnten Gesprächspartnerinnen und Gesprächspartner einzelne Themen thematisch vertiefen – bevor sie in Diskussionsrunden kontrovers debattiert wurden.

Die Chefgespräche waren 2022 integraler Bestandteil des digitalen Programms. Neben den Innenministerinterviews wurden auch andere Personen aus dem Öffentlichen Dienst interviewt – hier Chefredakteur Uwe Proll zusammen mit dem GDP-Bundesvorsitzenden Jochen Kopelke. Screenshot: BS/Schubert

Die Lage im Land

Des Weiteren wurde im vergangenen Jahr eine bei den Zuschauerinnen und Zuschauern beliebte Tradition fortgesetzt: Interviews mit den Innenministerinnen und Innenministern der einzelnen Bundesländer. In jeweils etwa 30-minütigen Gesprächen wurden die Amtsträger zu regionalspezifischen Themen befragt, z. B. ob Bremen den Streit mit der DFL beilegen konnte oder wie Bayern konsequenter gegen Reichsbürger vorgehen möchte.

Spontane Highlights

Doch nicht alles auf der Plattform wurde vorher ausführlich angekündigt, kleinere Highlights entstanden auch spontan. So wurde die Diskussion des deutschen Bundeskanzlers Olaf Scholz (SPD) zusammen mit seinem norwegischen Amtskollegen Jonas Gahr Støre auf der Berliner Sicherheitskonferenz (BSC) exklusiv für Zuschauende von Digitaler Staat Online übertragen. Auch für das laufende Jahr 2023 wird die Plattform mit exklusiven Inhalten aufwarten, ein Blick auf digitaler-staat.online lohnt sich immer!

Digital und kommunal?

Best Practice, Denkanstöße und Problemerörterungen

⟩⟩⟩ von **Malin Jacobson,** Behörden Spiegel

Sind hybride Sitzungen die Zukunft der kommunalen Gremienarbeit? Wie digital kann und muss die kommunale Daseinsvorsorge werden? Welche Chancen bietet die Digitalisierung im Bereich Nachhaltigkeit? Wie funktioniert Counter Speech in der behördlichen Kommunikation? Könnte eine umfassende Digitalisierung kommunale Träger von Kindertagesstätten entlasten? Wie sollte der Öffentliche Dienst mit Fake News umgehen? Werden „graue" Kommunen bei der Breitbandausstattung abgehängt? Wo liegen Chancen und Grenzen bei der Digitalisierung der Gefahrenabwehr?

„Zoom-Meetings" und „Teams-Besprechungen" sind nicht nur für Familientreffen auf Distanz und in der Privatwirtschaft en vogue. Auch in kommunalen Gremien wird mehr und mehr auf technische Kommunikationsmittel zurückgegriffen. Mit unseren Referenten sprachen wir über die Erreichbarkeit von Bürgerinnen und Bürgern, rechtliche Unsicherheiten bei auf „Distanz" gefassten Beschlüssen und technische Voraussetzungen. Screenshot: BS/Jacobson

Digitalisierung zum Anfassen

In Form von themenspezifischen Fortbildungen und kostenfreien Diskussionsrunden befasst sich die Veranstaltungsplattform NeueStadt.org wöchentlich mit verschiedenen Aspekten der kommunalen Verwaltung. So auch deren Digitalisierung und damit einhergehenden Möglichkeiten und Herausforderungen. Nicht nur die Entscheider und Fachleute aus Rathäusern, Gemeinde- und Stadtparlamenten und Landratsbehörden, kommunalen Zweckverbänden, öffentlichen Unternehmen, sondern auch die Vertreter von Bund und Ländern, die in ihren Aufgabenbereichen mit den Kommunen befasst sind, sind Teil des digitalen Austausches.

Es wirkt auf den ersten Blick wie ein Widerspruch: die Digitalisierung der Gefahrenabwehr. So ist doch das Retten von Personen, das Löschen von Bränden oder das Bergen eher physischer Natur. Auf den zweiten Blick ergeben sich doch einige Anwendungsfälle, bei denen eine Unterstützung sinnvoll sein kann. Wir diskutierten, wo Chancen und Grenzen bei der Digitalisierung der Gefahrenabwehr liegen, wie digitale Angebote bei der Ausbildung helfen können und welche Erfahrungswerte es in diesem Bereich bereits gibt. Screenshot: BS/Jacobson

Digital, digitaler, Kommunen

So wurde in der Reihe „Kommunen 2.0" darüber diskutiert, inwiefern sich die Aspekte smart und nachhaltig, digital und sicher sowie intelligent und ethisch miteinander in Einklang bringen lassen. Und auch in den Diskussionen um Entbürokratisierung und Beschleunigung von Verfahren wird immer wieder die Digitalisierung thematisiert. Dabei werden nicht nur die online zugänglichen Formulare betrachtet, sondern auch die Voraussetzungen und Anwendungsoptionen der digitalen Verwaltung.

Vom Problem zum Best Practice

Auf der Veranstaltungsplattform NeueStadt.org finden sich – 100 Prozent digital – zu all diesen und weiteren Themen Best Practice Beispiele, sowie Denkanstöße und Problemerörterungen. Vom Katastrophenschutz über die Nachwuchsförderung bis hin Immobilien der öffentlichen Hand, ist für jeden Interessierten etwas dabei.

CyberSicherheitsTag
Niedersachsen 2022
31. August 2022

Informationssicherheit i
Kommunen för
vorausschauend – verlässlich – ve

Hannover Congress Centrum, Niedersachsenhalle

www.sicherheitstag-niedersachsen.de

Programmpartner Niedersächs für Inneres

CYBERSICHERHEITSTAG NIEDERSACHSEN

Kommunale IT wird geprüft

Es besteht starker Nachholbedarf

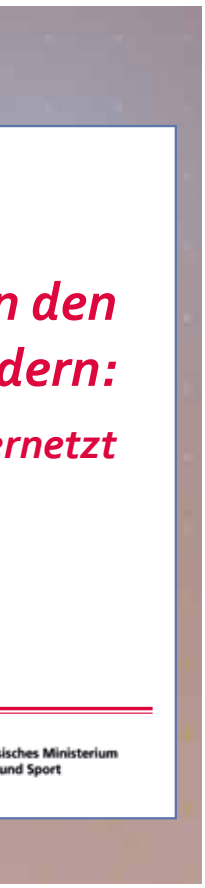
〉〉〉 von **Benjamin Hilbricht,** Behörden Spiegel

Nur zwei von sechs geprüften Kommunen in Niedersachsen haben einen Informationssicherheitsbeauftragten (ISB). Außerdem fehlt es ihnen an einem Notfallmanagement, Sicherheitsmanagement, an Konzepten und Vorgehensweisen. Das geht aus dem Kommunalbericht 2022 hervor, den der Niedersächsische Landesrechnungshof im September letzten Jahres veröffentlicht hat. Dieser prüft seit 2016 in jedem Jahr verschiedene Kommunen. Jedes Jahr gibt es ein Schwerpunktthema. „Grundlage der Prüfung ist eigentlich immer der IT-Grundschutz", erklärte Hans-Jörg Friedrich vom Landesrechnungshof auf dem CyberSicherheitsTag Niedersachsen in Hannover. Aus dem IT-Grundschutz des BSI hat der Landesrechnungshof einen Fragebogen mit rund 190 geschlossenen Fragen entwickelt. Die Kommunen antworten mit „Ja" oder „Nein". Am Ende machen die Prüferinnen und Prüfer einen Ortsbesuch und gehen den Fragebogen gemeinsam mit den Gemeindevertreterinnen und -vertretern durch. Der Landesrechnungshof verfolgt dabei zwei Ziele: Einerseits will er vergleichsfähige Daten über die Cyber-Sicherheit der niedersächsischen Gemeinden sammeln. Andererseits sollen die Geprüften durch den Fragebogen für das Thema sensibilisiert werden. Letzteres sei das Hauptanliegen, betonte Friedrich. „Wir gehen in einer sehr niedrigen Flughöhe durch das Land", sagte er. Es gehe um den Grundschutz der IT. Aus den Antworten der Gemeinden leitet der Landesrechnungshof konkrete Handlungsbedarfe ab.

Cyber-Notfall wie Feueralarm üben

2022 hatten circa drei Viertel der Gemeinden Nachholbedarf beim Notfallmanagement. Katastrophenfälle müsse man üben, sagte Dr. Horst Baier, das gelte für den Feueralarm wie für den Cyber-Notfall. Der CIO der Niedersächsischen Landesregierung konstatierte: „An der Stelle sind wir noch nicht optimal vorbereitet."

Großer Handlungsbedarf bestand auch beim Sicherheitsmanagement. Oftmals fehlte es den Kommunen zum Beispiel



an Vorgaben, wie Passwörter auszusehen haben und wie oft sie erneuert werden müssen. In vielen Kommunen habe es auch kein Konzept für regelmäßige Back-ups oder wie Beschäftigte sich bei einem Cyber-Angriff zu verhalten hätten gegeben.

Eine Gemeinde, die er geprüft habe, habe gar nichts aufgeschrieben, erzählte Friedrich vom Landesrechnungshof. „Die Gemeinde macht alles richtig. Man kann sie am Netz lassen, aber sie schreiben halt nichts auf." Das stelle ein Risiko dar. Er empfahl den Handlungsverantwortlichen, einem Diktiergerät zu erzählen, wie sie Back-ups und andere Sicherheitsaufgaben durchführen. Wenn sie dieses Diktat verschriftlichten und von der Leitung unterschreiben ließen, hätten sie ihr Sicherheitskonzept.

Oder Licht aus

Richter fordert mehr Kooperation für mehr IT-Sicherheit

⟩⟩⟩ von **Benjamin Hilbricht,** Behörden Spiegel

Dr. Markus Richter mahnt mehr Kooperation und Zentralisierung auf allen Ebenen der IT an. Das sei ebenso eine Frage der Sicherheit wie des wirtschaftlichen Handelns. Laut dem Staatssekretär des Bundesministeriums des Innern und für Heimat (BMI) sollen Bundesländer, Kommunen und Wirtschaftsunternehmen mehr und näher zusammenrücken.

„Wir müssen erkennen, dass wir bisher noch keine strukturierte, konzertierte Attacke gegen unsere Infrastruktur hatten", erklärte Richter auf dem CyberSicherheitsTag Niedersachsen. Doch er sagte das nicht, um Entwarnung zu geben. Stattdessen warnte er davor, was passieren könnte, wenn die aktuell in der Ukraine gebundenen Cyber-Aktivitäten frei würden. Die zerklüftete IT-Sicherheitslandschaft in Deutschland würde einen schweren Stand haben.

Dr. Markus Richter, Staatssekretär im Bundesministerium des Innern und für Heimat und Beauftragter der Bundesregierung für Informationstechnik, sprach auf dem CyberSicherheitsTag Niedersachsen.

Foto: BS/Proll

Hinzu komme der Übergang in die Cloud. Kommunen und Unternehmen dürften in der IT nicht länger auf Protektionismus setzen. „Ich fordere Sie auf und bitte Sie, die Kooperation zu suchen", sagte Richter. „Wenn Sie in einer Kommune arbeiten, in der alles funktioniert, prophezeie ich, dass das in der Zukunft keinen Wert haben wird." Denn der Trend gehe hin zu immer mehr geteilten Cloud-Systemen. Hier seien alle nur so stark wie das schwächste Glied in der Kette. Sowohl die technologische als auch die Cyber- Sicherheitsentwicklung gehe zu immer mehr gemeinsamen Systemen. „Diejenigen, die jetzt diese Entwicklung verschlafen, müssen damit rechnen, dass wir ihnen das Licht ausmachen", warnte der CIO des Bundes.

Lob vom Bund

Die Zusammenarbeit zwischen dem Bund und dem Land klappt in Niedersachsen. Das Flächenland war eines der ersten Bundesländer, die eine Kooperationsvereinbarung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) getroffen haben. „Es ist toll, dass wir diese Zusammenarbeit haben", lobte der damalige BSI-Präsident Arne Schönbohm das Land in seinem Grußwort auf dem CyberSicherheitsTag Niedersachsen. Auch Richter erklärte, dass Niedersachsens Zusammenarbeit mit dem BSI vorbildlich sei.

Der damalige Innenminister des Landes erklärte, dass er sogar noch mehr Kooperation wolle. „Wir würden gerne das BSI mit dauerhaften Analysen beauftragen können und uns bei unseren vielen Aufgaben helfen lassen", erklärte Boris Pistorius (SPD).

Nachholbedarf

Doch innerhalb des Landes sieht man in Niedersachsen Nachholbedarf bei IT-Kooperationen. Kleine Gemeinden mit nur einer einzigen IT-Fachkraft könnten von einem Cyber-Angriff leicht überfordert werden, sagte Dr. Horst Baier. Der CIO der Niedersächsischen Landesregierung plädiert dafür, dass solche Gemeinden externe Dienstleister beauftragen. Für die Kommunen würde er sich zudem ein zentrales Angebot eines Beauftragten für die IT-Sicherheit wünschen. Da herrsche großer Mangel.

Der IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung der Stadt Braunschweig berichtete, wie effizient die Zusammenarbeit zwischen Kommunal- und Landesverwaltung sein kann. „Als Emotet intelligenter wurde, hat uns die Landesverwaltung gewarnt", sagte Matthias Hoffmann. Emotet ist eine Schadsoftware, die E-Mail-Kontakte und -inhalte ausliest und dann gefälschte Mails an Freunde und Bekannte verschickt. Unter Anleitung des Landes hätten Hoffmann und sein Team konkrete Maßnahmen implementiert, die die Landesverwaltung empfohlen habe. „Es war sehr gut, sich einmal außer der Reihe zusammenzusetzen", urteilte der IT-Sicherheitsbeauftragte.

Ausbau der Cyber-Sicherheitsarchitektur

Niedersachsen plant robustes Cyber-Sicherheitszentrum

⟩⟩⟩ Gastbeitrag von **Boris Pistorius,** ehem. Innenminister Niedersachsen, Bundesminister der Verteidigung

Vertraulichkeit, Verfügbarkeit und Integrität – diese Eigenschaften sind von erheblicher Bedeutung bei analogen und digitalen Informationen. Öffentliche Verwaltungen erheben und verarbeiten eine Vielzahl an Daten, insbesondere von den Bürgerinnen und Bürgern. Damit sind sie auch für die Informationssicherheit verantwortlich. Die fortschreitende Digitalisierung der Arbeitsläufe bringt viele Vorteile mit sich, birgt aber auch Gefahren: Manipulation, Datendiebstahl oder der Ausfall der IT haben unmittelbare Auswirkungen auf die Arbeitsfähigkeit der Verwaltungen.

Diese Szenarien sind schon längst nicht mehr Gegenstand von theoretischen Planbesprechungen, sondern Realität geworden – 2019 legten Angreifer mit dem Trojaner Emotet die Verwaltung von Neustadt am Rübenberge lahm, die Auswirkungen waren noch lange spürbar.

Die Bedrohungslage aus dem Cyber-Raum ist für die öffentliche Verwaltung, Unternehmen, Kritische Infrastrukturen und Privatpersonen nach wie vor hoch. Diese Entwicklung ist nicht erst seit Putins Angriffskrieg auf die Ukraine zu beobachten, sondern bereits seit Jahren. Cyber-Kriminelle agieren zunehmend professioneller und grenzüberschreitend. Es ist daher zwingend erforderlich, Cyber-Sicherheit als gesamtstaatliche Aufgabe zu verstehen, die nur gemeinsam zu bewältigen ist. Auf allen Hierarchieebenen müssen Akteurinnen und Akteure institutionalisiert und kooperativ zusammenarbeiten.

Abstimmung von Maßnahmen

Eine zentrale Rolle hat dabei das Bundesamt für Sicherheit in der Informationstechnik (BSI). Das Land Niedersachsen profitiert bereits durch eine Kooperationsvereinbarung von den Kompetenzen und Erfahrungen des BSI. Der Ausbau des BSI zu einem zentralen Kompetenzzentrum für alle Bundesländer ist aus meiner Sicht daher von zentraler Bedeutung. Diese Stelle könnte beispielsweise mit gemeinsamen Datenbanken und Lagebildern wesentlich zur frühzeitigen Erkennung von Angriffen beitragen und in besonderen Lagen mit herausgehobenen IT-Vorfällen wichtige operative Unterstützung leisten. Gegenseitige Unterrichtungen und Auskunftserteilungen, wechselseitige Beratungen, Unterstützungen und Hilfestellungen würden außerdem eine bessere Koordination und Abstimmung von Maßnahmen zwischen Bund, Ländern und Kommunen ermöglichen.

In Niedersachsen plant die Landesregierung, ein robustes Cybersicherheitszentrum aufzubauen, um die Bereiche der Cyber Security, Cyber Crime sowie Cyber Intelligence noch enger miteinander zu verknüpfen. Zudem sollen die bestehenden Unterstützungsangebote für die Landesverwaltung, die Kommunen und KRITIS-Einrichtungen ausgebaut werden.

Auf Bedürfnisse der Kommunen eingehen

Dabei kommt den Kommunen im Rahmen der gesamtstaatlichen Cyber-Sicherheits-Architektur eine herausragende Bedeutung zu. Sie erledigen unmittelbar zentrale Verwaltungsaufgaben für die Menschen und Unternehmen vor Ort. Die hierbei verwendeten Daten der Bürgerinnen und Bürger genießen einen besonders hohen Schutz. Das Land Niedersachsen setzt sich daher schon seit Jahren dafür ein, die Informationssicherheit in den Kommunen zu fördern und entwickelt sein bestehendes kostenfreies Unterstützungs- und Beratungsangebot fortlaufend weiter. So stellt beispielsweise das Niedersächsische Computer Emergency Response Team (N-CERT) seinen Warn- und Informationsdienst mittlerweile etwa 120 Kommunen in Niedersachsen zur Verfügung. Darüber hinaus befindet sich eine Informationsplattform über Schadsoftware und Cyber-Angriffe für den kommunalen Bereich in der Erprobungsphase. Auch Fortbildungen und Workshops werden laufend angeboten.

Der CyberSicherheitsTag in Niedersachsen 2022 stand hierbei passend unter dem Motto „Informationssicherheit in den Kommunen fördern. Vorausschauend – verlässlich – vernetzt“. Die gemeinsame Veranstaltung mit dem Behörden Spiegel hat dazu beigetragen, zielgerichtet auf die Bedürfnisse der Kommunen einzugehen.

Seit Juli 2022 bietet das Niedersächsische Ministerium für Inneres und Sport den Kommunen mit der kostenfreien Durchführung von speziell für öffentliche Verwaltungen entwickelten Cyber-Sicherheitsanalysen ein ganz besonderes Unterstützungsangebot an. Mithilfe dieser standardisierten Analyse kann ermittelt werden, ob die bereits getroffenen Schutzmaßnahmen eine ausreichende Widerstandfähigkeit gegen Cyber-Angriffe gewährleisten. Zudem erhalten die Kommunen eine Bewertung ihres aktuellen Sicherheitsniveaus mit eindeutigen Handlungsempfehlungen. Das Land erhält außerdem wichtige Erkenntnisse, wo Unterstützungsmaßnahmen wirkungsvoll angesetzt werden können. Die Resonanz aus den Kommunen war außergewöhnlich hoch, weshalb wir dieses Angebot auch in diesem Jahr fortführen.

Für unsere immer digitaler werdende Gesellschaft werden die Bedrohungen aus dem Cyber-Raum auch künftig weiter zunehmen. Es liegt in unserer Hand, uns hierfür zu wappnen. Wir müssen deshalb auf allen Ebenen – Bund, Länder und Kommunen – die Voraussetzungen für eine möglichst hohe Cyber-Sicherheit schaffen. Klar ist: Wir können diese gesamtstaatliche Aufgabe nur mit gegenseitigem Vertrauen und intensiver Zusammenarbeit meistern. Dafür werden wir uns in Niedersachsen auch in der Zukunft mit Nachdruck einsetzen.

Das Chief Digital Office (CDO) des BAMF – das sind wir!

Das Bundesamt für Migration und Flüchtlinge (BAMF) ist ohne seine moderne IT nicht denkbar. Um unserer Verantwortung gerecht zu werden und unsere Mitarbeitenden zu unterstützen, arbeiten wir mit innovativen Technologien und setzen auf eine serviceorientierte IT-Infrastruktur, Microservices und viele weitere spannende IT-Lösungen! Wir haben uns das Ziel gesetzt, sämtliche Vorgänge und Prozesse im Bundesamt zu digitalisieren oder digital zu unterstützen. Dabei setzen wir auf neue Wege wie die Einführung eines Chief Digital Office (CDO), um die digitale Transformation voranzutreiben (***www.bamf.bund.de/digitalisierungsagenda***).

Hintergrund zum CDO

Eine Umfrage des Branchenverbandes BITKOM zeigt, dass im Jahr 2021 nur 20 Prozent der Behörden und Unternehmen eine oder einen CDO hatten, nahezu ausschließlich als Einzelperson in Form eines Chief Digital Officers. Hier gibt es also deutlichen Entwicklungsbedarf.

Aufgabenspektrum des CDO im BAMF

Das CDO-Team des BAMF steuert die Digitalisierung in einem zukunftsorientierten und fachbereichsübergreifenden Sinne: technisch, organisatorisch und sozio-kulturell. Eine unserer Hauptaufgaben liegt in der Entwicklung und Umsetzung einer nachhaltigen Strategie und eines langfristigen Digitalisierungskonzeptes. Diese Aufgabe hört nicht bei der Formalisierung einer Vision für die Behörde auf, sondern setzt sich in der Mitgestaltung und Optimierung von analogen und digitalen Prozessen und dem internen und externen „Brücken schlagen“ fort. Wir bündeln und verdichten Wissen, vernetzen technische sowie digitale Kompetenzen und Einzelstrategien der Fachabteilungen unseres Hauses.

Für andere Behörden sind wir im BAMF die Kontakt- und Ansprechstelle zum Thema „Digitale Transformation“. Wir wirken an behördenübergreifenden Strategien mit, um verschiedenste Bundes- und Landesbehörden mit der BAMF-IT zusammenzubringen. Wir nehmen an diversen Fachtagungen/-kongressen, Messeveranstaltungen, Workshops und als Vertretung in Fachgremien der Bundesverwaltung/Bundesländer und IT-Dienstleister teil und knüpfen so wertvolle Kontakte. Aus der Recherche von externem und internem Knowhow resultieren ein Monitoring und die Analyse aktueller und künftiger innovativer IT-Themen, IT-Entwicklungen und IT-Strategien.

Dieser Prozess wird nicht über Nacht erfolgen – im Gegenteil: Veränderung braucht Zeit, Ressourcen und vor allem unser gemeinsames Interesse, unsere Offenheit für Neues und den Drang zum Entdecken, zum Forschen und Experimentieren.

» Wir streben eine umfassende Digitalisierung in allen Themenbereichen des BAMF an. Dafür setzen wir nun auch das CDO ein.

Katrin Hirseland, die Vizepräsidentin des BAMF

Ziel: die gemeinsame Digitalisierung

Haben wir Sie neugierig gemacht? Haben auch Sie Bedarf an Gesprächen und einem regen Austausch? Dann kommen Sie mit uns in Kontakt! Schlagen Sie gemeinsam mit uns die Brücke zu einer gemeinschaftlichen Digitalisierung in der Verwaltung! Oder sind Sie selbst in der gleichen Rolle und in einem CDO bzw. als CDO tätig? Wir freuen uns darauf, Erfahrungen mit Ihnen auszutauschen! Kommen Sie mit uns ins Gespräch: ***CDO@bamf.bund.de***

Mitarbeitende des CDO-Teams im BAMF. Obere Reihe von links: Fürkan Gülengil, Durmus-Ali Sinanoglu. Untere Reihe von links: Anastasiia Burdeinaia, Isabell Westphal, Liliana Renye, Julian Buchner. Fotos: BAMF

Informationsaustausch 2.0: das „CIC“

Einen weiteren Meilenstein bietet das in Berlin ansässige „Creative Information Technology Center“ des BAMF, das „CIC“. Mit seinem offenen und kreativen Arbeitsumfeld schafft das CIC Raum für eine enge Zusammenarbeit, nicht nur mit anderen Behörden, sondern auch mit Stakeholdern der Digitalisierung. Das Bundesamt vernetzt sich mit innovativen Start-ups, Unternehmen der Branche, anderen Behörden sowie Universitäten, um neue Technologien und Methoden zu erproben und einen Mehrwert für die gesamte Bundesverwaltung zu schaffen.

Im Jahr 2023 finden acht Thementage statt, an denen die Möglichkeit geboten wird, mit der IT-Community Wissen auszutauschen:

- Künstliche Intelligenz (26.01.)
- Low/No Code Tools (23.03.)
- Agile Methoden in der Praxis (27.04.)
- Modernes Anforderungsmanagement (25.05.)
- Nachhaltigkeit in der IT und deren Messung (22.06.)
- IT-Security & Zero-Trust (28.09.)
- Barrierefreiheit in der IT (26.10.)
- Digitale Souveränität (30.11.)

Wir freuen uns über Ihre Anmeldung unter:
CIC.Bamf@bamf.bund.de

Weitere Informationen rund um das CIC erhalten Sie unter:

Es ist immer noch der Anwender

Cyber-Risiken entstehen zum Großteil vor dem Computer

⟩⟩⟩ von **Paul Schubert,** Behörden Spiegel

Die größten Risiken im IT-Bereich liegen immer noch bei den Nutzerinnen und Nutzern. Das gilt auch für die kommunale Verwaltung, erklärte Dr. Marco Trips, Präsident des Niedersächsischen Städte- und Gemeindebunds auf dem CyberSicherheitsTag Niedersachsen des Behörden Spiegel in Hannover.

Die klassischen Einfallstore seien dabei das Öffnen von E-Mail-Anhängen, das Wählen von zu leichten Passwörtern oder gefährliche Makros. Neben Schulungen von Mitarbeiterinnen und Mitarbeitern seien vor allem Kooperationen zwischen den Entscheidungsträgern nötig. Trips forderte vor allem die verstärkte Zusammenarbeit zwischen kommunalen Rechenzentren, privaten IT-Dienstleistern und dem Land Niedersachsen.

Seit August 2022 gibt es für die Kommunen in Niedersachsen ein einmaliges Budget von einer Million Euro für die Durchführung von Cyber-Sicherheitsanalysen. Niedersachsens damaliger Innenminister Boris Pistorius (SPD) bewertete die ersten Resultate als positiv. Foto: BS/Proll

Budget für Cyber-Sicherheitsanalysen für Kommunen

Um die niedersächsischen Kommunen bei der IT-Sicherheit zu unterstützen, hatte das Ministerium für Inneres und Sport ein einmaliges Budget von einer Million Euro für die Durchführung von Cyber-Sicherheitsanalysen für die Verwaltungssysteme bereitgestellt. Trips hält diesen Betrag nicht für ausreichend: „Cyber Security in Niedersachsen sollte uns mehr wert sein als eine Millionen Euro." Des Weiteren hielt er die „starke Nachfrage" nach dem Angebot, die nach dem damaligen Innenminister Boris Pistorius (SPD) von den Kommunen ausgegangen sei, für „stark überzeichnet".

Der SPD-Politiker bewertete die Finanzierung der Cyber-Sicherheitsanalysen für die Kommunen als Erfolg und kündigte weitere Änderungen in der Cyber-Sicherheitspolitik Niedersachsens an. So solle in dem Bundesland perspektivisch ein Cyber-Sicherheitszentrum geschaffen werden. Dieses soll allerdings nicht als eigenständige Behörde gebildet werden, sondern aus dem Innenministerium ausgehen, wie es bereits beim Hessen3C und der Cybersicherheitsagentur Baden-Württemberg der Fall ist. Dieses Zentrum solle „praktische Unterstützungsangebote für die Kommunen" bieten, erläuterte Pistorius. Allerdings sei die Planung des Cyber-Sicherheitszentrums noch nicht vollends abgeschlossen. So ist noch nicht ersichtlich, ob das niedersächsische Sicherheitszentrum auch weitergehende Funktionen, wie z. B. das Landesamt für Informationssicherheit (LSI) in Bayern, erfüllen wird.

Cyber SEK zur Bekämpfung von Cyber Crime

Des Weiteren berichtete Pistorius über die Einrichtung eines „Cyber SEK" und erläuterte dies im Gespräch mit dem Behörden Spiegel. Es ist zu vermuten, dass der Stelle eine ähnliche Funktion zukommen könnte wie dem Niedersachsen-CERT (N-CERT), welches bei Cyber-Notfällen von allen Kommunen genutzt werden kann. Darüber hinaus bietet das N-CERT auch Workshops für die Kommunen an. Auf Nachfrage erklärte Pistorius, dass beim Cyber SEK in Einzelfällen „eine Gruppe von IT-Spezialisten an einen Tatort entsendet werden könne." Dabei solle es sich aber nicht um Sicherheitsbehörden handeln, ergänzte er. Generell erlange das Thema der IT-Sicherheit vor allem im Bereich Cyber Crime größere Bedeutung. So wurde die Ausplanung von Fachkommissariaten zur Bekämpfung von Cyber-Verbrechen durchgeführt. Cyber-Angriffe machten nicht vor Ländergrenzen halt und deswegen sei ein weitergehender Austausch der Behörden wichtig, ergänzte der Pistorius.

ONLINE-AKADEMIEN

Damit Sie noch mehr bewirken können!

Unsere Fortbildungen unserer Online-Akademien halten Sie nicht nur zu aktuellen Themen auf dem Laufenden, sondern sie bieten Ihnen gleichzeitig die Chance, in einen Dialog mit einem breiten Netzwerk zu treten.

Die Webinare bringen regelmäßig Führungs- und Fachkräfte, Praktikerinnen und Praktiker aus Verwaltung und Politik, Wissenschaft und Forschung sowie Privatwirtschaft und Beratung zusammen. Sie erhalten die einmalige Gelegenheit, Ihr Wissen und Ihre Erfahrungen zu teilen und gleichzeitig von neuen Ideen zu profitieren.

DIGITALER STAAT ONLINE

DIGITALE AKADEMIE

www.digitaler-staat.online/akademie

NeueStadt.org

KOMMUNALE AKADEMIE

www.neuestadt.org/akademie

NORDL@NDER DIGITAL

Verwaltung der Zukunft in SH, HH, HB, MV, NI, ST

5. SEPTEMBER 2022 | ROSTOCK

#diginordland

www.nordlaender-digital.de

NORDL@NDER DIGITAL

Fehlerkultur und Vertrauen entscheidend

Auch interdisziplinäres Arbeiten fördern

〉〉〉 von **Matthias Lorenz,** Behörden Spiegel

Bloß keine Fehler machen – diese Haltung herrscht in vielen deutschen Behörden noch immer vor. Dies ist in vielerlei Hinsicht auch eine sinnvolle Einstellung. Schließlich verursachen Fehler immer Kosten und diese müssen aus Steuermitteln gedeckt werden, die sonst an anderer Stelle verwendet werden könnten. Doch die Einstellung, um alles in der Welt fehlerfrei zu agieren, kann auch hinderlich sein. Ohne den Mut, auch ein Scheitern in Kauf zu nehmen, gibt es schließlich selten Innovationen. Genau diese braucht die Verwaltung allerdings gerade bei der Digitalisierung. Der fällige Kulturwandel war deswegen eines der bestimmenden Themen beim letztjährigen Nordl@nder-Kongress des Behörden Spiegel in Rostock.

Schon in seiner Eröffnungsrede legte Christian Pegel, Mecklenburg-Vorpommerns Minister für Inneres, Bau und Digitalisierung, einen Schwerpunkt auf diese „Transformation im Kopf". Es müsse erstens erlaubt sein, Fehler zu machen, und zweitens sollten Projekte schon bei einem Umsetzungsstand von beispielsweise 80 Prozent live gehen. Dieses Vorgehen ergebe viel mehr Sinn, als bis zu einem Stand von 100 Prozent zu warten und dafür jahrelange Wartezeiten in Kauf zu nehmen. An dieser Stelle seien auch die Führungskräfte in der Verwaltung gefragt. „Diese müssen zu einem Projekt stehen und dann auch Verantwortung übernehmen, wenn etwas nicht funktioniert", forderte Pegel. Ähnliches betonte auch Sven Thomsen, Chief Information Officer (CIO) des Landes Schleswig- Holstein. Die Rolle der Vorgesetzten sei es, „Lösungen zu ermöglichen und diese nicht nur zu bewerten oder entgegenzunehmen, wenn sie abgeschlossen sind". Es sei wichtig, projektorientiert mit einem Team an Lösungen so lange zu arbeiten, bis diese auch geliefert würden. Dazu gehöre es, Ressourcen und Geld an Land zu ziehen.

Fehler müssen akzeptiert werden

Laut Thomsen ist es aber auch wichtig, in der Politik das Bewusstsein dafür zu schaffen, dass man auch mit nicht

perfekten Produkten live gehen dürfe. „Wenn wir nicht mit 80 Prozent starten, wird es schwierig." Dieses Bewusstsein zu schaffen, sei die Aufgabe einer „dienenden Führung", wie Thomsen sie nennt. Minister Pegel ergänzte, auch die Medien und die Gesellschaft müssten akzeptieren, wenn Fehler gemacht würden.

Wie wichtig es ist, das Bewusstsein für Digitalisierungs-Bedürfnisse in der Politik zu schärfen, stellte auch Eva-Maria Kröger in einer Wortmeldung heraus. Die Digital-Politikerin der Linken sitzt seit 2016 im Schweriner Landtag und engagiert sich seit 2009 außerdem in der Rostocker Bürgerschaft. Gerade in der Kommunalpolitik arbeiteten die meisten Vertreterinnen und Vertreter ehrenamtlich. „Gleichzeitig wird erwartet, dass wir immer zu allen Themen sprechfähig sind", beschrieb Kröger die Situation. Deswegen sei es schlicht und einfach nicht möglich, als Politikerin oder Politiker von sich aus auf die Experten zuzugehen. Man sei darauf angewiesen, dass diese sich mit ihrer Expertise an die Entscheidungsträger wendeten, um auf Schwierigkeiten und Probleme hinzuweisen, welche die Politik dann lösen könnte.

Ina-Maria Ulbrich, Staatssekretärin im Ministerium für Inneres, Bau und Digitalisierung des Landes Mecklenburg-Vorpommern und Schirmherrin des Kongresses, hob als wichtigen Punkt für das Gelingen der Verwaltungsdigitalisierung das Vertrauen hervor. Dabei betrachtete sie diesen Aspekt aus mehreren Blickwinkeln. Erstens müssten die Führungskräfte Vertrauen in die Mitarbeitenden haben. Doch auch andersherum müssten die Mitarbeitenden den Führungskräften dahingehend vertrauen können, dass diese akzeptierten, wenn etwas nicht so gelaufen sei wie ursprünglich geplant. Doch auch im Verhältnis zwischen dem Staat und den Bürgern brauche es mehr wechselseitiges Vertrauen, erklärte Ulbrich. Momentan vertrauten die Bürgerinnen und Bürger dem Staat beispielsweise beim Thema Datenschutz nicht. Auf der anderen Seite habe der Staat beim Erbringen von Leistungen auch ein Vertrauensdefizit gegenüber den Bürgern. Diese müssten heutzutage meist extrem viele Anträge stellen und Nachweise erbringen, um eine Leistung zu erhalten. Würde der Staat den Bürgern an dieser Stelle mehr vertrauen, könnten manche Anträge wegfallen. „Die Vertrauenskultur ist also ein ganz wesentlicher Punkt", bilanzierte Ulbrich.

Interdisziplinäres Team gefragt

Des Weiteren wurde vielfach betont, wie wichtig eine projektorientierte Arbeit innerhalb der Verwaltung ist. „Wir müssen zunächst den Blick auf das Produkt lenken und uns überlegen, was wir eigentlich haben wollen", erläuterte CIO Thomsen. Wenn das gelinge, könne man alle nötigen Mitarbeitenden identifizieren und an einen Tisch bringen. Dafür müsse die Verwaltung interdisziplinäres Arbeiten fördern und belohnen. Es brauche ein interdisziplinäres Team, welches ein Projekt vollständig bearbeite.

Dem stimmte Staatssekretärin Ulbrich zu. Ressortübergreifende Arbeit sei in der Landesverwaltung Mecklenburg-Vorpommerns rechtlich sogar möglich. In der Realität müssten jedoch zunächst Anträge gestellt werden, bevor Mitarbeitende

Mecklenburg-Vorpommerns Digitalminister Christian Pegel forderte eine veränderte Fehlerkultur in der Verwaltung.

Foto: BS/Eva-Charlotte Proll

formal zugewiesen würden. Ein langwieriger Prozess. „Es liegt also nicht an den Regeln, sondern am Mindset", so Ulbrich.

Ähnliches beobachtete auch der IT-Bevollmächtigte der niedersächsischen Landesregierung, Dr. Horst Baier. „In der Landesverwaltung erlebt man eher eine organisierte Nicht-Zusammenarbeit." Die Ressorts würden immer zunächst schauen, wo sie Kompetenzen verlieren könnten. Als Beispiel nannte Baier die IT-Zentralisierung. Hier erinnere ihn das Agieren der Ressorts an Häuserkampf. Dahingegen sei die Kultur der Zusammenarbeit in den Kommunen meist ausgeprägter. „Dort hat man kürzere Wege, ist flexibler", sagte Baier. Allerdings erlebe er auch in der Landesverwaltung an einigen Stellen ein Umdenken. Beispielsweise empfänden manche Landesbehörden das Thema Cyber-Sicherheit inzwischen als so kompliziert, dass sie es lieber an eine andere Stelle abgeben würden. Für Baier ist dies eine gute Entwicklung.

Denkmodell Netzwerkkommune

Digitale Daseinsvorsorge im Fokus

⟩⟩⟩ von **Matthias Lorenz,** Behörden Spiegel

Im föderalen System spielen die Kommunen eine besondere Rolle. Sie sind meist der direkte Kontaktpunkt zwischen dem Bürger und dem Staat. Darüber hinaus spielen sie auch eine wichtige Rolle für das Leben der Bürgerinnen und Bürger. Das Stichwort lautet Daseinsvorsorge. Doch wie verändert sich die Rolle der Kommunen durch die Digitalisierung und wie sollte eine „digitale" Daseinsvorsorge aussehen?

Für Prof. Dr. Moreen Heine, Professorin für E-Government und Open Data Ecosystems an der Universität zu Lübeck, kann digitale Daseinsvorsorge aus drei Komponenten bestehen. „Zunächst geht es um den Zugang: Wo finde ich was, welche Leistungen kann ich digital in Anspruch nehmen", erklärt die Wissenschaftlerin. Als zweites müsse man die Transformation, also die Reorganisation von Leistungen durch Digitalisierung nennen. Drittens müsse die Kommune durch die Digitalisierung auch völlig neue Bedürfnisse erfüllen. „Beispielsweise braucht jeder einen Zugang zur digitalen Infrastruktur. Dies ist ein völlig neues Element, welches die Daseinsvorsorge leisten muss."

Die Daseinsvorsorge umfasst längst nicht mehr nur den analogen Raum.
Foto: BS/heleiqiang, pixabay.com

Kompetenzen und Teilhabe

Die zentrale Frage, die gestellt werden müsse, ist laut Anika Krellmann, Referentin im Programmbereich Organisations- und Informationsmanagement bei der Kommunalen Gemeinschaftsstelle für Verwaltungsmanagement (KGSt): „Was ist der kommunale Auftrag im digitalen Zeitalter?" Grundsätzlich könne die Digitalisierung bei der Lösung vieler kommunaler Herausforderungen helfen. Man müsse jedoch immer darüber nachdenken, was eine Gemeinschaft heutzutage brauche, um ein gutes Leben zu führen. Politik und Verwaltung müssten sich aktiv fragen, welche Aufgabe sie übernehmen müssten, um das Gemeinwohl zu stärken.

In dieser Hinsicht sei vor einigen Jahren noch viel an Breitband gedacht worden, so Krellmann weiter. Inzwischen seien einige Themen hinzugekommen. Es gehe unter anderem darum, die digitalen Kompetenzen sowie die digitale Teilhabe der Bürger zu stärken. „Da übernehmen die Kommunen eine sehr wichtige Aufgabe." Krellmann betont auch, dass sich das Selbstbild der Kommune geändert habe. Heutzutage müssten sie als „Netzwerkkommunen" denken. Schließlich sei eine Kommune mehr als die reine Verwaltung. „Im Bereich der Daseinsvorsorge wurden Dinge schon immer nicht allein von der Verwaltung, sondern gemeinsam mit Partnern, auch aus der Zivilgesellschaft, geleistet", erläutert Krellmann. Kommunen müssten sich also immer fragen, welche Kompetenzen man selbst habe und welche Dinge gemeinsam mit Partnern angegangen werden müssten. Für viele Kommunen sei es allerdings eine Herausforderung, so zu denken, weil daraus manchmal ein Steuerungsverlust entstehe.

Synergien zwischen Schule und Bauakte

Auch plädiert Krellmann für mehr interkommunale Zusammenarbeit, gerade zwischen kleinen Gemeinden: Eine Gemeinde könne sich auf eine Aufgabe konzentrieren, eine andere auf ein weiteres Thema. Kreisen käme in diesem Fall eine besondere Orchestrierungsaufgabe zu. Wie wichtig kommunale Zusammenarbeit ist, wird auch immer wieder von der politischen Seite betont. So sagt Lars Prahler, Bürgermeister der Stadt Grevesmühlen: „Es gibt keinen anderen Weg als die interkommunale Zusammenarbeit." Auch der Schweriner Oberbürgermeister Dr. Rico Badenschier hebt die Relevanz von Kooperation hervor. Die Stadt Schwerin habe zusammen mit der Stadt Ludwigslust und dem Landkreis Ludwigslust-Parchim ein gemeinsames Kommunalunternehmen gegründet. „Hier entwickeln wir Verwaltungsleistungen zusammen. Das erzeugt Synergien unter anderem in den Bereichen Schule und digitale Bauakte", berichtet der SPD-Politiker. Ebenfalls entstünden durch die Konsolidierung Synergieeffekte im Bereich der Fachkräftegewinnung.

Flexibel, aber sicher

Hybride Arbeit in Behörden

Ob im Büro, daheim oder unterwegs – für viele Menschen ist das Arbeiten von überall zur täglichen Routine geworden. Möglich machen es portable Endgeräte sowie schnelles mobiles Internet auf der einen und eine sich wandelnde Arbeitskultur auf der anderen Seite. Laut einer Bitkom-Umfrage aus März 2022 arbeiten aktuell 50 Prozent der Erwerbstätigen in Deutschland ganz oder teilweise mobil beziehungsweise im Homeoffice. Dabei muss berücksichtigt werden, dass 36 Prozent der Arbeitnehmerinnen und -nehmer eine Tätigkeit ausüben, die sich nicht für das Homeoffice eignet. Auch im öffentlichen Dienst setzen sich flexible Arbeitsmodelle immer stärker durch und werden zunehmend von den Angestellten nachgefragt. In einer PwC-Studie gaben Ende 2021 – also noch inmitten der Pandemie – 88 Prozent der öffentlichen Mitarbeiter an, dass sie in Zukunft genauso viel oder mehr im Homeoffice arbeiten möchten.

Mit der wachsenden Popularität hybrider Arbeitsmodelle, wächst auch der Bedarf an Headsets, die effiziente virtuelle Zusammenarbeit ermöglichen sowie größtmögliche Sicherheit garantieren und zugleich mobil einsetzbar sind. Beliebt sind hier professionelle Bluetooth-Headsets wie die Jabra Evolve und Evolve2 Serie, die es erlauben mit mehreren Endgeräten gleichzeitig verbunden zu sein und so ein nathloses Hin- und Herwechseln zwischen Laptop und Smartphone ermöglichen. Jabra hat es sich aber ebenfalls zur Aufgabe gemacht auch seine DECT-Headsets so anzupassen, dass sie den veränderten Arbeitsbedingungen gerecht werden. Die Antwort ist das Jabra Engage 55 – das mit seiner extrem hohen Reichweite und dem kompakten USB-DECT-Adapter das wahrscheinlich flexibelste reine DECT-Headset auf dem Markt ist.

Mehr Sicherheit für Behörden

In den letzten Jahren ist die Cyberkriminalität sehr stark gestiegen und Lauschangriffe gehören zu den gängigen Spionagemethoden. Auch der öffentliche Sektor ist betroffen und befürchtet, dass Homeoffice und mobiles Arbeiten ein zusätzliches Risiko für die Datensicherheit darstellen. Einige Kommunen und Behörden haben zudem generelle Sicherheits-Bedenken, was die schnurlose Kommunikation betrifft, und bevorzugen kabelgebundene Headsets. Sowohl Bluetooth als auch DECT-Headsets sind aber nahezu vollkommen abhörsicher. Die Modelle der Jabra Engage Serie sind die sichersten kabellosen Headsets für Büros auf dem Markt – sie gehen sogar noch über die höchste Stufe der DECT Level C-Zertifizierung hinaus und verwenden AES 256-Bit-Verschlüsselung. Somit erfüllen sie selbst die vom US-Militär und der US-Regierung geforderten FIPS 140-2-Standards.

Mehr Freiraum für Bewegung

Ganz gleich, von wo man arbeitet, ist es angenehm, sich dabei frei bewegen zu können. Wenn Beschäftigte allerdings viel telefonieren und an virtuellen Konferenzen teilnehmen, ist

dies ohne Headset kaum möglich. Der kompakte und äußerst robuste USB-DECT-Adapter des Engage 55 bietet eine schnurlose Reichweite von bis zu 150 Metern, ausgehend von dem damit verbundenen Laptop. Da sie durch das Dongle auf eine stationäre Basisstation verzichten können, haben Nutzerinnen und Nutzer zudem die Möglichkeit sich mit ihrem Laptop zu bewegen, während sie telefonieren, und können so auch von unterwegs arbeiten.

Mehr Schutz für das Gehör

Alle schnurlosen Modelle der Engage Serie bieten ausgezeichneten Gehörschutz und verfügen über die Jabra SafeTone Technologien. Zu diesen gehört Jabra PeakStop™ 105 dB, das plötzliche Schallspitzen, die durch Störungen im Telefon- und Kommunikationsnetz verursacht werden können, ausblendet, ohne das Gespräch zu beeinträchtigen. Eine weitere Technologie namens IntelliTone™ 2.0 hält den durchschnittlichen Schallpegel während des ganzen Tages unterhalb der vordefinierten Grenzwerte. In lauten Büroumgebungen neigen Benutzer zudem dazu, die Lautstärke bei Anrufen zu erhöhen, um den Kunden zu hören. Diese anhaltend hohe Lautstärke kann sich negativ auf das Gehör auswirken. Mit Jabra BalancedVoice™ wird der eingehende Ton eines Anrufs klarer und schärfer wiedergegeben, ohne dass der Schallpegel erhöht wird, wodurch die Wahrscheinlichkeit von Hörschäden durch laute Geräusche über einen längeren Zeitraum hinweg verringert wird.

Weitere Informationen zur Jabra Engage Reihe finden Sie unter:

www.jabra.com.de/engage

OZG-Finanzierungsdebatte

Unklarheiten deutlich erkennbar

⟩⟩⟩ von **Matthias Lorenz,** Behörden Spiegel

Wenn sich Expertinnen und Experten im vergangenen Jahr 2022 über die Umsetzung des Onlinezugangsgesetzes (OZG) austauschten, wurden sie sich in vielen Punkten schnell einig: Ja, die Frist Ende 2022 war nicht mehr zu halten. Ja, man hätte von vornherein die Ende-zu-Ende-Digitalisierung mitdenken müssen. Doch was folgt aus diesen Erkenntnissen? Hierüber herrscht noch Diskussionsbedarf.

Neben der Debatte um ein mögliches OZG 2.0 ist hierfür die Finanzierung ein gutes Beispiel. Aus dem Corona-Konjunkturprogramm hatte der Bund drei Milliarden Euro für die OZG-Umsetzung bereitgestellt. Über eine mögliche Anschlussfinanzierung wird zwischen Bund, Ländern und Kommunen auch Anfang 2023 noch gestritten. Eine langfristige Lösung scheint noch in weiter Ferne zu liegen.

Dr. Moritz Karg, Referatsleiter Grundsatzangelegenheiten Digitalisierung und E-Government in der Staatskanzlei des Landes Schleswig-Holstein, hält schon die Art der Zurverfügungstellung der Konjunkturmittel für den „größten Fehler des Bundes". Die Mittel seien lediglich mit der unkonkreten Anweisung, jetzt doch bitte loszulegen, bereitgestellt worden. „Deswegen hat man sich irgendwelche Projekte vorgenommen, ohne die dahinterliegenden Prozesse zu verstehen."

Prozessdigitalisierung braucht Zeit

Der zweite Fehler des Bundes sei es gewesen, die Finanzierung Ende 2022 auslaufen zu lassen. Vielmehr müsse der Bund nun durchhalten und dafür sorgen, dass bisher getätigte Investitionen auch ihre Wirkung entfalten könnten, forderte Karg auf dem Nordl@nder-Kongress 2022. In der aktuellen Situation würden Unternehmen, mit denen die Verwaltung zusammenarbeitet, nur noch laufende Projekte beenden, aber die Zusammenarbeit 2023 nicht fortsetzen wollen. Dies sei verständlich. „Es braucht Zeit für die Prozessdigitalisierung", so Karg. Jahrzehntelang gewachsene Prozesse könnten nicht zufriedenstellend in zwei Jahren digitalisiert werden.

Gute Prozesse sparen Geld

Luise Kranich, Referatsleiterin Digitalisierungsprogramme Bund und Föderal im Bundesministerium des Innern und für Heimat, wies hingegen darauf hin, man sei nicht unzuverlässig gewesen. „Es war von vornherein klar, dass die Finanzmittel Ende 2022 auslaufen." Sie gab jedoch zu, man hätte von Anfang an darauf achten müssen, was bis zu bestimmten Terminen zu schaffen sei. Kranich regt an, sich nicht so sehr auf die Frage der Finanzierung zu fokussieren, schließlich könne man die Argumentation umdrehen: „Wenn eine Behörde einen guten Prozess aufsetzt und sauber digitalisiert, spart sie viel Geld." Dadurch stelle sich die Finanzierungsfrage gar nicht mehr so sehr.

Der Bund müsse bei der Finanzierung der OZG-Umsetzung durchhalten, forderte Dr. Moritz Karg, Referatsleiter Grundsatzangelegenheiten Digitalisierung und E-Government in der Staatskanzlei des Landes Schleswig-Holstein von Luise Kranich, Referatsleiterin im BMI. Foto: BS/Eva-Charlotte Proll

Führungskräfte müssen mehr ausprobieren

In diesem Zusammenhang entgegnet Zehra Öztürk, die im Amt für IT und Digitalisierung der Senatskanzlei Hamburg die Projektleitung MODUL-F und die stellvertretende Referatsleitung Steuerung Fachverfahren und Neue Technologien innehat: „Am Anfang fehlt das Geld! Deswegen brauchen wir eine Anschubfinanzierung." Führungskräfte der Verwaltung müssten beispielsweise auch den Mut haben, Steuergelder auszugeben, um Dinge auszuprobieren. Insgesamt habe man nicht die Unterstützung gehabt, die es gebraucht hätte, und viel auf Vorgaben vom Bund gewartet, anstatt den Flow, den das OZG schon einmal ausgelöst habe, mitzunehmen.

Cyber-Attacken sicher aus allen Daten entfernen!

Die zunehmende Digitalisierung und Vernetzung, verstärkt den Zufluss von Daten von außen. Durch das Onlinezugangsgesetz (OZG) und viele Standardverfahren wie Internetdownloads oder E-Mail-Anhänge bei Bewerbungen im Personalbereich müssen betriebsbedingt Daten von unbekannten Absendern verarbeitet werden.

Das deutsche Unternehmen itWatch hat eine Software-basierte Datenwaschmaschine (www.itWash.de) entwickelt, die es ermöglicht, jede ausführbare Software – unabhängig davon, wie diese eingebettet ist – zu erkennen und zu entfernen. Dadurch können alle Dokumente direkt durch den Anwender genutzt werden.

Höchste Qualität des Schutzes

itWatch hat viele tausend Lizenzen im GEHEIM-Umfeld sowie weit über 100.000 Lizenzen in VS-NfD-Umgebungen. Dem Einsatz in GEHEIM Umgebungen gehen intensive Prüfungen voraus. Auf der Skala der Common Criteria Prüfungen sind diese höher als eine CC EAL 4+ Prüfung zu bewerten, da nicht gegen ein vom Hersteller definiertes Protection Profile geprüft wird, sondern alle Facetten der Produkte in realen vernetzten Einsatzumgebungen professionell verschiedensten Angriffsszenarien ausgesetzt werden.

Welche Anwendungsszenarien gibt es?

Daten vom Handy des Bürgers oder aus öffentlich zugänglichen IoT Geräten können leicht mit Schadcode oder Überwachungswerkzeugen infiltriert sein. Trotzdem sollen die Daten genutzt werden, wenn es sich z. B. um Beweismittel oder Schadensinformation handelt. Seit vielen Jahren ist itWash zur Übernahme von Daten aus unsicherer Umgebung bei Polizeien, Diensten, Energieversorgern, Justiz, Kommunen, der äußeren Sicherheit und vielen weiteren im Einsatz:

- Personalabteilungen-Mailanhänge der Bewerber „waschen“
- Polizei – für Beweisdaten, Standardisieren von Kameradaten und Bodycams, digitale Asservate
- Gerichte – Übergabe digitaler Beweismittel – auch vor Ort – an Richter
- Stadtwerke – Schadensmeldungen der Bürger, Datenaustausch mit dem Maschinenpark, (Updates, Neukonfigurationen etc.)
- Staatsanwaltschaft – Lieferung von digitalen Asservaten verschlüsselt (auch VS-NfD) inkl. Bandbreiten- und Prioritätenmanagement)
- Darknet-Recherche
- OZG – Bürgerdaten
- Integriert in Fachverfahren
- Internetdownloads, USB und vieles mehr

Gelebte Transformation

Mit effizienten Strukturen und Prozessen zum Erfolg

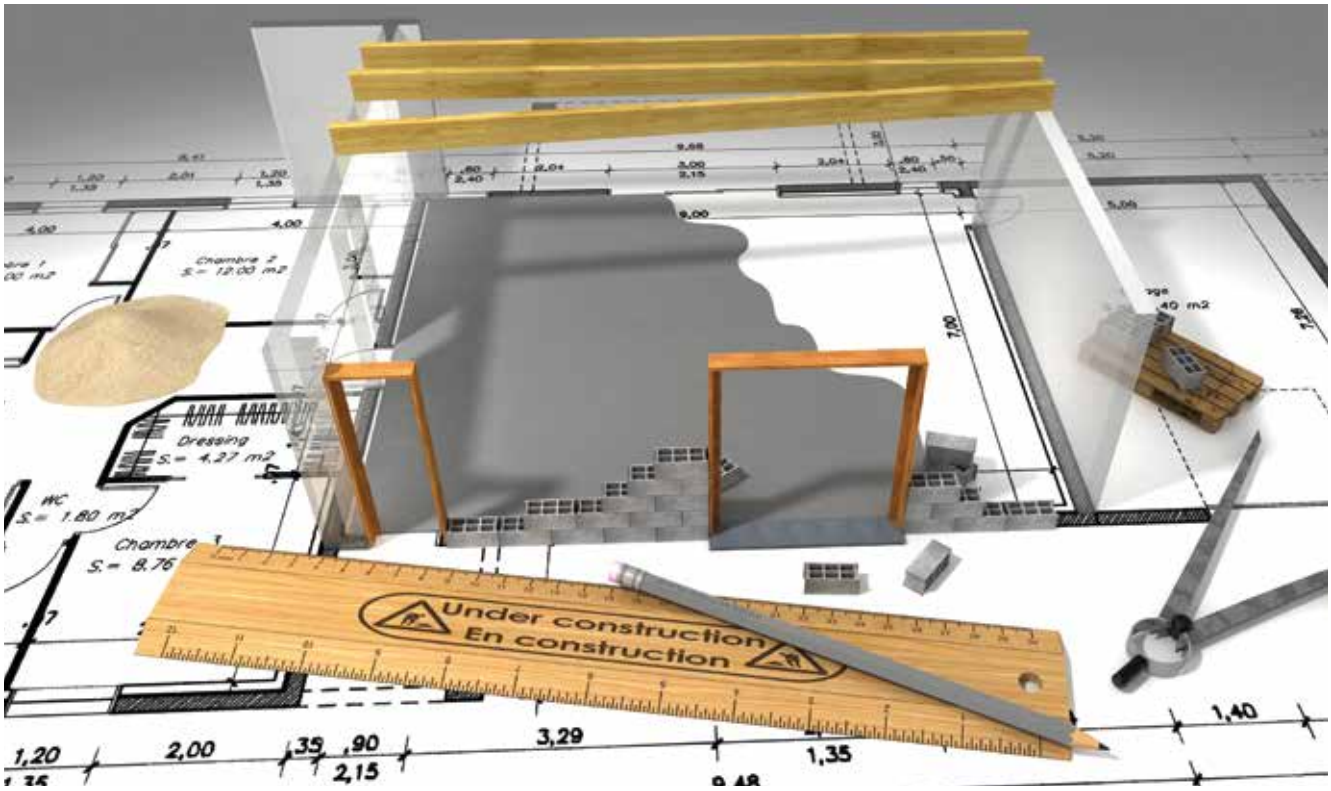
⟩⟩⟩ Gastbeitrag von **Ina-Maria Ulbrich,** CIO des Landes Mecklenburg-Vorpommern

Die digitale Verwaltung in Deutschland ist in den vergangenen Jahren ein ganzes Stück vorangekommen. Dabei haben wir bereits eine ganze Reihe von Erfolgen gefeiert und Lektionen gelernt. Diesen Erfahrungsschatz sollten wir jetzt nutzen für unsere weitere Zusammenarbeit. Denn ein großes Verdienst des OZG ist: Es hat uns näher zusammengebracht. Die Digitalisierung von Verwaltungsleistungen erfordert eine über alle föderalen Ebenen hinweg gelebte Zusammenarbeit von Bund, Ländern und Kommunen, wie sie es bisher in dieser Qualität und Tiefe in Deutschland noch nicht gegeben hat. Darauf sollten wir aufbauen.

Eine wichtige Erkenntnis ist aus meiner Sicht: Digitalisierung unterstützt vor allem dann, wenn wir aus der Sicht der Nutzerinnen und Nutzer entwickeln und effizientere Strukturen und Prozesse aufbauen – für die Antragstellung wie auch die -bearbeitung. Die Digitalisierung einer Leistung darf nicht wie bisher von der Technik dominiert werden. Vielmehr muss sich die Verwaltung selbst an die Spitze setzen und die Prozesse konsequent durchdenken.

Der preisgekrönte und viel beachtete EfA-Dienst „Digitaler Bauantrag", den Mecklenburg-Vorpommern federführend und in Kooperation mit dem Bundesinnenministerium umgesetzt hat, ermöglicht eine ortsungebundene, vollständig digitale Antragstellung unter Einbeziehung der Verwaltungsebene bis hinter die „Rathaustür". Unser ganzheitliches Herangehen beweist, dass hierdurch nicht nur deutlich größere Qualitäten erzielbar sind, sondern auch eine höhere Geschwindigkeit in der konkreten Umsetzung selbst. Trotz der hohen Komplexität des Bauantrags konnte dieser Service mit als erste Leistung im FIT-Store der Föderalen IT-Kooperation betriebsbereit anderen Ländern zur Nachnutzung angeboten werden.

Der Digitale Bauantrag ist das Ergebnis gelebter Transformation der Verwaltung. Im Vorfeld war der Bauantrag aus der klassischen Perspektive des E-Governments und vor dem Hintergrund von Front- und Backend, uneinheitlicher IT-Architektur und verschiedenem Landesrecht als ein Paradebeispiel für eine nicht EfA-taugliche Leistung eingeschätzt worden. Daher brauchte es einen vollständigen Perspektivwechsel und eine neue Herangehensweise. Initial war die Einbindung der Nutzerinnen und Nutzer, in unserem Fall etwa Architektinnen und Architekten sowie Bauherren und Verwaltungsmitarbeitenden. In einem Digitalisierungslabor haben wir zunächst die analogen Prozesse neu ausgerichtet. Hier wurde, getragen von den Wünschen der Nutzerinnen



Der Digitale Bauantrag ist Mecklenburg-Vorpommerns OZG-Leuchtturmprojekt. Foto: BS/Jean-Paul Jaudrain, pixabay.com

und Nutzer, der digitale Kollaborationsraum geboren. Er ermöglicht die Zusammenarbeit der Beteiligten in Echtzeit. Ganz wesentlich war hierbei: Die Verwaltungsmitarbeitenden sollten gleichberechtigte Nutzerinnen und Nutzer sein, Vorteile im sog. Frontend müssen sich im Backend wiederfinden. Die Lösung sollte in jedem Bundesland ohne zusätzlichen Programmieraufwand nachnutzbar, hinsichtlich vorhandener IT-Strukturen offen sein, die Trennung von Front- und Backend aufheben sowie zukunftsoffen für Weiterentwicklungen sein.

Ausschlaggebend in der Umsetzung war ein Projektteam, das von Anfang an vom Erfolg überzeugt war und mit agilem Projektmanagement zügig und ergebnisorientiert darauf hingearbeitet hat. Diese Erfolgsfaktoren überträgt Mecklenburg-Vorpommern inzwischen auch auf die Ebene der mitnutzenden Länder. Sie werden unter anderem im Steuerungskreis zur Mitnutzung frühzeitig einbezogen und umfassend informiert. Als sehr erfolgreich hat sich die Bereitstellung einer Task Force erwiesen, welche die Länder beim Know-how-Transfer ganz praktisch vor Ort unterstützt. Mecklenburg-Vorpommern hat damit in vielerlei Hinsicht Neuland in Deutschland betreten. Erste Erfahrungen zeigen, dass gerade hierüber der Rollout sehr zügig voranschreiten kann. Zehn Länder haben sich 2022 für eine Mitnutzung entschieden, wovon bereits sechs durch die Task Force beim Roll-out unterstützt werden.

Vorgehensweise auch für andere Verfahren nutzbar

Wie richtungsweisend unser Vorgehen insgesamt war, zeigen die von IT-Experten im Rahmen des Bund-Länder-Pakts Planungsbeschleunigung zusammengetragenen Empfehlungen für die Zukunft. Die Auswertung verschiedener EfA-Dienste im Kontext von Planungs- und Genehmigungsverfahren zeigen den Wert des von Mecklenburg-Vorpommern eingeschlagenen Wegs, der über den Bauantrag hinaus auch für andere Verfahren nachnutzbar ist. Das EfA-Prinzip sollte den Experten nach gestärkt werden, weil unterschiedliche Planungs- und Genehmigungsverfahren auf abstrakter Ebene einem ähnlichen Ablauf folgen. Das legt eine Übertragbarkeit nahe. Echte Beschleunigungseffekte gibt es, wenn der gesamte Prozess von Anfang bis Ende über alle Verfahrensschritte digitalisiert und die Verfahrenssteuerung einbezogen ist. Empfohlen wird ein kollaborativer Informations- und Datenaustausch, wie z. B. beim Building Information Modeling (BIM), für eine beschleunigte Planung und Realisierung. Open BIM sollte daher bundesweit Standard werden und in die Umsetzung von EfA-Projekten integriert werden. Hierbei soll dem Digitalen Bauantrag eine Schlüsselrolle zukommen.

Mecklenburg-Vorpommern hat von Anfang an in diese Richtung gedacht und schon entsprechende Überlegungen zur Weiterentwicklung der Lösung angestellt, um dann die einzelnen Leistungen in einem Baulebenszyklus miteinander zu verknüpfen. Damit wird es möglich sein, alle Leistungen vom Bauantrag bis zum Abriss eines Gebäudes digital abzuwickeln und auch verwandte Leistungen zusätzlich anzukoppeln. Der Leitsatz hinter dieser Optimierung ist immer das Once-Only-Prinzip.

Ina-Maria Ulbrich ist Staatssekretärin im Ministerium für Inneres, Bau und Digitalisierung des Landes Mecklenburg-Vorpommern

Foto: BS/Ministerium für Inneres, Bau und Digitalisierung Mecklenburg-Vorpommern

Auf Experten hören, EfA-Prinzip umsetzen

Mit unserem Digitalen Bauantrag haben wir die Transformation der Verwaltung ein Stück vorangebracht. Insgesamt stehen wir aber noch am Beginn eines größeren Umbruchs in der Verwaltung, den wir konsequent weiterverfolgen müssen. Bei der weiteren Digitalisierung von Verwaltungsleistungen sollten die Expertenempfehlungen die Richtung vorgeben und das EfA-Prinzip konsequent gestärkt werden.

// SAVE THE DATE

Die Vorbereitungen für den nächten Kongress Nordl@nder DIGITAL laufen bereits. Das Event findet am 12. Oktober in Bremen statt.

PITS – PUBLIC IT-SECURITY

Enormer Vertrauensverlust droht

Kommunen im Fadenkreuz von Cyber-Kriminellen

⟩⟩⟩ von **Matthias Lorenz,** Behörden Spiegel

Der Tag, an dem der Landkreis Anhalt-Bitterfeld zum Symbol für die Gefahr von Cyber-Angriffen für deutsche Kommunen wurde, war 2022 schon weit über ein Jahr her. Trotzdem war nach der Ransomware-Attacke in der Landkreisverwaltung noch immer „überall Sand im Getriebe", berichtete Sabine Griebsch, damals CDO des Landkreises, auf der PITS. Seitdem in Anhalt-Bitterfeld der erste Cyber-Katastrophenfall Deutschlands ausgerufen wurde, fielen noch mehr Kommunen Angriffen zum Opfer. Die reale Bedrohung sorgt für ein gesteigertes Gefahrenbewusstsein bei den Verantwortlichen.

Doch dafür brauchte es offensichtlich erst das Gefühl, die Gefahr vor der eigenen Haustür zu haben. Wie Andreas Ebels, Beauftragter für Datenschutz und IT-Sicherheit beim Zweckverband Kommunales Rechenzentrum Niederrhein (KRZN), berichtete, sei er nach dem Angriff auf Anhalt- Bitterfeld oft auf eine Einstellung gestoßen, die von dem Gedanken getrieben worden sei, Anhalt-Bitterfeld sei schließlich weit weg. „Als es dann wenige Monate später Witten im Ruhrgebiet traf, sind bei uns die ersten aufgewacht." Dies war angesichts der weiter steigenden Bedrohung höchste Zeit: Nicht nur agieren Cyber-Kriminelle inzwischen höchst professionell und effektiv, auch staatliche Mächte versuchen immer wieder, die demokratische Gesellschaft mittels Cyber-Attacken zu destabilisieren.

Schwerwiegende Auswirkungen

Wird eine Kommune, egal aus welcher Motivation heraus, erfolgreich angegriffen, können die destabilisierende Wirkung und der damit einhergehende Vertrauensverlust in den Staat enorm sein. Laut Dr. Uda Bastians, Beigeordnete und Leiterin des Dezernats Recht und Verwaltung beim Deutschen Städtetag, sind Arbeitsfähigkeit und Angebote dann massiv eingeschränkt. Bürgerinnen und Bürger könnten Dienstleistungen nur noch äußerst eingeschränkt nutzen – wenn überhaupt. „Schon jetzt werden staatliche digitale Angebote teilweise

Foto: ©JumalaSika ltd, stock.adobe.com

nicht genutzt, weil das Vertrauen in die Sicherheit der digitalen Dienste fehlt." Hinzu kommen andere Auswirkungen wie hohe Schadenssummen oder die Veröffentlichung sensibler Daten.

An vorderster Front

Aus diesem Grund hält es Henning Voß, der im nordrhein-westfälischen Innenministerium zu den Themen Wirtschaftsschutz und Geheimschutz in der Wirtschaft arbeitet, für falsch, wenn schlecht geschützte Kommunen als überschaubares Problem dargestellt würden. „Die Kommune ist eine tragende Säule der Gesellschaft", so Voß. Er fordert deswegen, trotz des Prinzips der kommunalen Selbstverwaltung über eine Grundschutz-Regulierung für Kommunen nachzudenken. „Der Staat sollte sich selbst als Kritische Infrastruktur (KRITIS) einstufen und sich Spielregeln vorschreiben." Bis jetzt habe man sich den finanziellen Mehraufwand, der mit solchen Regeln einherginge, nicht zumuten wollen. Dieser Forderung schließt sich Holger Berens, der Vorstandsvorsitzende des Bundesverbands für den Schutz Kritischer Infrastruktur (BSKI), an. „Aus unserer Sicht sind Kommunen KRITIS, weil sie immer die First Line of Defence darstellen." Schließlich seien sie meist an vorderster Front mit der Bewältigung von Krisen konfrontiert – seien es Naturkatastrophen, die Pandemie, die Aufnahme von Geflüchteten oder eben Cyber-Angriffe.

Unabhängig von einem gesetzlichen Zwang stehen Kommunen jedoch schon heute vor einer Reihe praktischer Herausforderungen, wenn es um die Umsetzung von IT-Sicherheitsmaßnahmen geht. Der Markt für IT-Security-Fachkräfte ist leergefegt. Darüber hinaus haben gerade kleinere Kommunen oft einfach nicht genug Angestellte, um das Thema adäquat bearbeiten zu können. „Wir sind ein kleiner Flächenlandkreis, in dem es Kommunen mit 1.500 Einwohnern und einer Verwaltung mit 20 Mitarbeitenden gibt. Dort ist meist niemand hauptamtlich für die IT verantwortlich", beschreibt der IT-Sicherheitsbeauftragte des Landkreises Marburg-Biedenkopf, Olaf Kirsch, die Situation. Als Landkreis sei man personell besser aufgestellt, trotzdem sei es neben dem Alltagsgeschäft schwierig, beispielsweise ein vollständiges Monitoring zu machen. Genau dieses sei aber inzwischen essenziell. „Abwehrmechanismen müssen grundsätzlich auf dem aktuellsten Stand gehalten werden, weil auch die Angreifer sich weiterentwickeln", erklärt Henning Voß. Der IT-Sicherheitsbeauftragte der niedersächsischen Landeshauptstadt Hannover, Heiko Hußmann, ergänzt: „Heutzutage hat man vielleicht noch ein bis zwei Stunden Reaktionszeit, bevor eine bekannt gewordene Lücke genutzt wird, weil auch Angreifer inzwischen viel Automatisierung und KI einsetzen." Deswegen habe man mit bestimmten Mitarbeitenden Sondervereinbarungen für den Krisenfall getroffen, damit Überstunden geleistet und auch am Wochenende gearbeitet werden könne.

Externe Partner benötigt

Um darauf zu reagieren, haben IT-Sicherheitsfirmen Techniken wie Security Information and Event Management (SIEM) oder Extended Detection and Response (XDR) entwickelt. „Solche Dinge können wir selbst mit mehreren 100 Mitarbeitenden in der IT nicht leisten", konstatiert Hußmann. An dieser Stelle sei man auf externe Partner angewiesen. Momentan habe man solche Tools noch nicht, wisse allerdings, dass man sie brauche. Hierfür sei jedoch auch die Einsicht der Verwaltungsleitung erforderlich.

Nach dem Wochenende ist es zu spät

Vertreter eines solchen externen Partners, welcher vollständige Monitoring-Lösungen auch für staatliche Stellen anbietet, ist Danial Kamran. Er arbeitet bei der Firma Sophos als Managed Threat Response Specialist. Gerade im öffentlichen Sektor beobachtet der IT-Sicherheitsspezialist immer wieder Verhaltensweisen, die davon zeugen, dass das Bewusstsein für die Gefahr von Cyber-Angriffen und das richtige Verhalten bei einer Attacke noch nicht flächendeckend verankert sind. „Es ist Fakt, dass viele Stellen freitags um 16 Uhr dichtmachen, selbst wenn es einen Sicherheitsvorfall gibt." Dann würden entgegen den Empfehlungen Systeme ausgeschaltet, anstatt nur das Netzwerk herunterzufahren. Systeme müssten zwingend

Der Landkreis Anhalt-Bitterfeld hatte 2022 immer noch mit den Folgen des Cyber-Angriffs aus dem Sommer 2021 zu kämpfen, so die damalige CDO Sabine Griebsch. Foto: BS/Trenkel

angeschaltet bleiben, um wichtige Daten analysieren zu können. Wenn die Reaktion schließlich nach dem Wochenende erfolge, sei es zu spät.

Die Frage, ob man auch im Landkreis Anhalt-Bitterfeld vor dem Angriff zu nachlässig agiert habe, verneint Sabine Griebsch. Vielmehr seien viele Faktoren zusammengekommen. So sei die IT-Infrastruktur gezwungen gewesen, Zugeständnisse an die Organisation und die Abläufe zu machen. Griebsch versprach: „Das passiert heute nicht mehr. Hier hilft der Angriff in der Argumentation sehr weiter."

Einer muss sagen: „Jetzt alle raus!“

Zwei Grundgesetzänderungen zum Preis von einer

⟩⟩⟩ von **Benjamin Hilbricht,** Behörden Spiegel

„Alle behalten ihre Zuständigkeiten, aber wir arbeiten besser zusammen, wenn wir die Zentralstelle der Cyber-Sicherheit werden.“ Das verspricht das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Cyber-Sicherheitsbehörden der Länder. Diese schwanken zwischen der offenkundigen Notwendigkeit der Neuaufstellung und Befürchtungen, dass ihre Hoheit in der Sicherheit langsam untergraben werden könnte.

Er war gekommen, um zu werben. Um die Cyber-Sicherheitsbehörden der Länder, um die Informationssicherheitsbeauftragten (ISB) der Kommunen, die Polizeikräfte, die Militärs sowie die Leute aus den Innenministerien, die sich auf der Public IT-Security versammelt hatten. Sie alle hängen irgendwie mit drin in der deutschen Cyber-Sicherheitsarchitektur.

Der CIO der Bundesregierung und Staatssekretär des Bundesministeriums des Innern und für Heimat (BMI), Dr. Markus Richter, gab sich gelassen. „Wenn wir über Grundgesetzänderungen sprechen, zum Beispiel mit Blickrichtung auf das BSI oder auch mit der Blickrichtung, dass der Bund komplementär – also ergänzend – eine Zuständigkeit im Bereich der Gefahren-Abwehr im Cyber-Raum braucht, dann heißt das nicht, dass alle Behörden die Griffel fallen lassen“, erklärte er. Im Gegenteil, es komme nur hinzu, dass man in bestimmten Szenarien zusammenarbeiten könne.

Deckmantel des Notstands

„Wir sind zu oft unter dem Deckmantel des Notstands unterwegs“, kritisierte der Staatssekretär. Das BSI, das Kernstück der Cyber- Sicherheitsarchitektur, biete den Ländern Informationsaustausch und Cyber Emergency Response Teams (CERT) an. Nur dürfe es das bislang ausschließlich im Rahmen der Amtshilfe oder von Kooperationsvereinbarungen.

Der Vizepräsident des BSI stimmte zu und ergänzte: „Kooperationsvereinbarungen sind gewagte Instrumente.“ Laut BSI-Vize Dr. Gerhard Schabhüser bewegen diese Vereinbarungen sich am Rande des juristisch Möglichen. „Der Bund darf eigentlich nur das für die Länder übernehmen, was im Grundgesetz explizit erlaubt ist. Wir dürfen für die Wirtschaft viel mehr machen als für die Länder.“ Für umfassende Cyber-Sicherheit müssten aber Bund, Länder und Kommunen Hand in Hand arbeiten.

Abseitsfalle

Die Länder wollen ja kooperieren. Da ist zum Beispiel die Föderale IT-Kooperation (FITKO), eine Initiative der Bundesländer. Auch sie mischt bei der Cyber-Sicherheit mit. Ihr Leiter für Föderales IT-Architekturmanagement, Jörg Kremer, nimmt eine Fußballweisheit als Sinnbild für das, was die IT-Sicherheit braucht. „Wenn es darum geht, die Abseitsfalle aufzustellen“, sagt Kremer, „muss einer auf dem Feld sagen: Jetzt alle raus! Ob es das BSI ist oder jemand anders – einer muss das sagen.“

Kompetenzverschiebung

Ein Cyber-Sicherheitskapitän auf dem Feld. Kooperativ und komplementär arbeiten. Klingt gut. Aber in den Ländern schwanken sie. Die Zusammenarbeit mit dem BSI sei gut. Aber da ist auch die Sorge, dass hier eine massive Kompetenzverschiebung im Gange ist.

„Auf der operativen Ebene bin ich bereit, zu sagen, ich glaube Ihnen aufs Wort, dass es hier nicht um eine Kompetenzverschiebung geht“, sagte Martin Wiegand, stellvertretender Leiter des Hessen CyberCompetenceCenter (Hessen3C) in Richtung des BSI-Vizepräsidenten Schabhüser. Doch die Polizeiführung, die er bei seiner Arbeit im hessischen Ministerium des Innern und für Sport (HMDIS) kennengelernt

Der BSI-Vize Dr. Gerhard Schabhüser (1. v. l.) diskutierte mit Dr. Barbara Held (2. v. l.), Martin Wiegand (3. v. l.), Jörg Kremer (2. v. r.) und Dr. Claudia Warken (1. v. r.) über die kommende Zentralstellenfunktion des Bundesamts für Sicherheit in der Informationstechnik (BSI). Foto: BS/Trenkel

habe, „sieht gerade etwas ganz anderes: eine Ausweitung der Kompetenzen des Bundeskriminalamts“. In der Diskussion über eine Grundgesetzänderung für die Cyber-Sicherheit werde zweierlei vermischt.

Zwei zum Preis von einer

In Richters Worten steckte schon das, was Wiegand wie der Wolf im Schafspelz vorkommen musste. Der CIO der Bundesregierung sprach von Grundgesetzänderungen mit zwei Blickrichtungen: Zentralstellenfunktion und Gefahrenabwehr. Die Frage ist, ob beides zusammengehört oder ob der Bund versucht, zwei Grundgesetzänderungen zum Preis von einer zu bekommen.

Aus Sicht des BSI betrifft nur die erste Gesetzesinitiative das Amt selbst. „Die zweite Initiative – Rechtsetzungsbefugnis und Gefahrenabwehrbefugnisse für den Bund – zielt eher auf die Sicherheitsbehörden der Länder. Das hat mit dem BSI erst einmal nichts zu tun“, erklärte Schabhüser. Er verstehe die Sorge, aber: „Zwei Pakete, zwei unterschiedliche Zielsetzungen.“

In der Diskussion wurden diese beiden Vorhaben – Informationszentralstelle und Gefahrenabwehr – vermischt. Es sieht in den Augen mancher so aus, als würde das BMI versuchen, zwei verschiedene Vorhaben mit einer einzigen Kraftanstrengung durchzusetzen. Das liegt auch daran, dass zur Cyber- Sicherheit im Verständnis des BMI nicht nur die Detektion von Bedrohungen und die Vorbeugung gehören, sondern eben auch Mittel der aktiven Cyber-Abwehr. Diese sind aber als Eingriffe bei den Sicherheitsbehörden mit entsprechenden Befugnissen, also bei Polizei und Nachrichtendiensten angesiedelt.

Eckpunktepapier angekündigt

Da ist etwas in Bewegung. Richter, der Staatssekretär, der den Umbau der Cyber-Sicherheitsarchitektur schon seit der Cybersicherheitsstrategie aus dem letzten Jahr begleitet, kündigte ein Eckpunktepapier an. Bis Ende des Jahres 2022 würden darin die genaue Ausgestaltung der Zentralstellenfunktion des BSI und damit die Grundgesetzänderungen präzisiert. Die Zuhörenden hatten die Möglichkeit, Vorschläge zu machen. Das Publikum klatscht. Hinter geschlossenen Türen diskutierten sie viel miteinander, die Menschen vom Land und vom Bund.

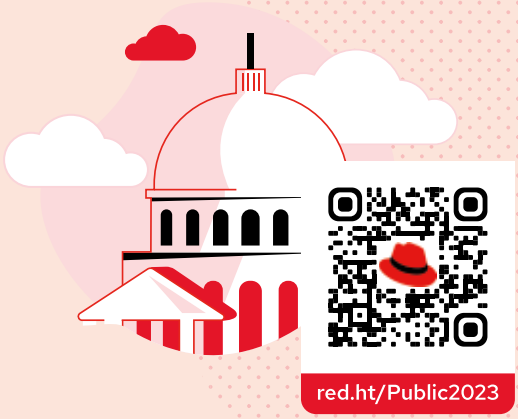
„Wir sind zu oft unter dem Deckmantel des Notstands unterwegs“, erklärte der CIO der Bundesregierung und Staatssekretär im Bundesministerium des Innern und für Heimat (BMI), Dr. Markus Richter, auf der Public IT-Security. Foto: BS/Trenkel

Red Hat

Digitale Souveränität der Verwaltung

Innovative Services und Komponenten für leistungsfähige Datacenter und digitale Prozesse

Enterprise OpenSource von Red Hat:
Sicher. Skalierbar. Standardkonform. Wirtschaftlich.



Computerhirne für Behörden

Ist KI in der Verwaltung eine Chance oder Herausforderung?

⟩⟩⟩ von **Jonas Brandstetter,** Behörden Spiegel

Mit Künstlicher Intelligenz (KI) in der öffentlichen Verwaltung sind viele Hoffnungen, aber auch Ängste verbunden. Ein nüchterner Blick auf den Themenkomplex offenbart jedoch: Anwendungsfelder für KI in der öffentlichen Verwaltung sind noch nicht klar umrissen. Zunächst müssen Handlungsparadigmen definiert und Sicherheitsaspekte abgewogen werden.

Seit der Industrialisierung haben Maschinen systematisch Arbeitsaufgaben übernommen. Über die maschinelle Webmaschine, elektronisch gesteuerte Produktionsstraßen bis hin zur Digitalisierung lässt sich dieser Prozess bis in die Gegenwart nachzeichnen. „Der nächste Transformationsschritt in dieser Dynamik ist die sogenannte ‚Cyberisierung', also die unmittelbare Kommunikation zwischen Mensch und Maschine", prognostiziert Prof. Dr. Jivka Ovtcharova, Institutsleiterin am Karlsruher Institut für Technologie (KIT). Weil die Globalisierung nicht zukunftsfähig sei, müsse man die globale Wirtschaft in intelligente regionale Wirtschaften transformieren. Eine entscheidende Rolle in diesem Prozess komme KI zu. Ein Themenfeld, über das jedoch viele falsche Vorstellungen kursieren. Diese reichen von Dystopien bis hin zu Heilsvorstellungen. Solche eindimensionalen Schwarz-Weiß-Bilder lässt Ovtcharova jedoch nicht gelten. KI sei ein von Menschen gemachtes Tool, das es korrekt einzusetzen gelte. Denn digitale Bildung bedeute Befähigung: „Es gilt sich zu fragen, was kann ich als Mensch zur KI beitragen, damit sie mich unterstützt?" Statt schlicht Prozesse durch die KI bearbeiten zu lassen, liege das große Potenzial der Technik darin, völlig neue Einsatzfelder aufzutun. Um dies zu verdeutlichen, bedient sich die Professorin einer Analogie. Während bei der Digitalisierung des technischen Zeichnens zunächst dem Tuschestift lediglich ein digitales Pendant entgegengestellt wurde, schöpfte erst ein völlig neuer Ansatz, eine unmittelbare, dreidimensionale Konstruktionsplattform, das Potenzial digitalen technischen Zeichnens voll aus. Auch beim Einsatz des Werkzeugs KI müssten solche neuen Wege eingeschlagen werden. Eine voraussetzungsvolle Erkenntnis, denn um KI in die Prozesse einzubinden oder diese sogar zu transformieren, muss zuerst eine genaue Beschreibung besagter Prozesse vorliegen.

Für Prof. Dr. Jivka Ovtcharova, Institutsleiterin am Karlsruher Institut für Technologie (KIT), ist KI ein hochkomplexes Werkzeug, das es richtig einzusetzen gilt. Foto: BS/Karlsruher Institut für Technologie

Sicherheitsfragen noch ungeklärt

Welche KI-Systeme in welchem Kontext das richtige und sichere Werkzeug sind, damit befasst sich unter anderem das Bundesministerium für Sicherheit der Informationstechnik (BSI). Insbesondere das Referat für Künstliche Intelligenz unter der Leitung Dr. Arthur Schmidts ist mit dieser Aufgabe betraut. Eines der zentralen Anliegen des Referats ist die Entwicklung von Kriterien zur Bewertung der Sicherheit von KI-Cloud-Systemen. Mit dem Artificial Intelligence Cloud Service Compliance Criteria Catalogue (AIC4) hat das BSI einen ersten Operationalisierungsansatz entworfen. Nach den Kriterien Sicherheit und Robustheit, Performance und Funktionalität, Zuverlässigkeit, Datenqualität, Datenmanagement, Erklärbarkeit sowie Bias unterscheidet der AIC4 sichere von unsicheren KI-Cloud-Systemen. Offen bleibt allerdings die Frage, wie man die verschiedenen Kriterien überprüft. Während für das Kriterium Sicherheit bereits ein Tool zur Verfügung steht, existieren für Themenfelder wie Verlässlichkeit noch keine hinreichenden Messkriterien. „Wir sind auf die Wissenschaft bei der Entwicklung potenzieller Tools angewiesen", konstatiert

Schmidt im Hinblick auf diesen Mangel. Der Zeitplan des BSI sieht deshalb die Entwicklung entsprechender Tools in den nächsten vier Jahren vor. Durch Kooperationen im Anwendungsbereich sollen Methoden zur Qualitätsprüfung für die verschiedenen Kriterien erprobt werden. Die auf diese Weise gesammelten Erfahrungen gelte es zu generellen Lösungen zu verallgemeinern. Es sei allerdings verkürzt, davon auszugehen, dass eine allgemeine Zertifizierung mit universeller Einsetzbarkeit einhergehe. Neben der operativen Prüfung der Angemessenheit einer spezifischen KI-Lösung, müsse auch die Sicherheitsstufe des Systems im Anwendungsfall bedacht werden. Vollständige Sicherheit und Fehlerlosigkeit seien illusorisch. Auch sei Nachvollziehbar- und Begründbarkeit in bestimmten Aufgabenfeldern der öffentlichen Verwaltung unabdinglich. Besonders in solchen, in denen Ermessen ein Faktor im Entscheidungsprozess sei. Mit dem Bewusstsein um die Kontextabhängigkeit des KI-Einsatzes müsse man sich auch die Frage nach der Verantwortlichkeit stellen. Auch eine gewisse gesellschaftliche Akzeptanz für Risiken müsse der Einführung von KI-Systemen in der öffentlichen Verwaltung vorausgehen.

Kein Allheilmittel

Dr. Jan Remy ist CISO des Freistaates Bayern. Er möchte mit der Vorstellung aufräumen, KI könne verschlafene Prozesse in der Digitalisierung aufholen. Um KI gewinnbringend einzusetzen, müsse man sich zunächst über die Prozesse selbst und die vorhandenen Ressourcen Gedanken machen. Durch KI ließen sich Probleme nicht überbrücken. Remy stellt sich deshalb die Frage, wann KI in der öffentlichen Verwaltung überhaupt sinnvoll genutzt werden kann. „KI ist immer dann umsetzbar, wenn man sie in Prozesse einbetten kann, wenn sie Entscheidungen vorbereiten und unterstützen kann. Daten durchforschen und Kunden akquirieren ist hingegen kein Anwendungsfall für Behörden.“ Ein weiterer denkbarer Nutzungsbereich – die Evaluierung von Prozessen – gehöre bereits zur gängigen Praxis in der öffentlichen Verwaltung. Ob KI in diesem Prozess einen Beitrag leisten könne, sei abhängig von der Akzeptanz in der Bevölkerung. Zusätzlich gehen mit der Einführung KI-gestützter- Prozesse auch weitreichende operative Veränderung einher. Um einen Prozess für den Einsatz von KI urbar zu machen, bedarf es eines gewissen Bearbeitungsvolumens. „Für fünf Anträge im Jahr lohnt sich KI nicht“, macht der Experte deutlich. Zudem müssten Prozesse zentralisiert werden. Hätten Bearbeitungsparadigmen früher noch im Ermessen der jeweiligen Sachbearbeitenden gelegen, müssten für die KI zentrale Handlungsanweisungen bereitstehen. Remy plädiert deshalb dafür, Souveränität zu wahren und KI als Werkzeug zu sehen und nüchtern, mit klarem Blick, Chancen und Risiken zu beurteilen.

Wir müssen es habitualisieren

Wie die digitale Selbstverteidigung gestärkt werden kann

⟩⟩⟩ von **Jörn Fieseler,** Behörden Spiegel

Phishing-Angriffe zählen zu den größten Übeln der IT-Sicherheit. Denn nach wie vor erfolgen neun von zehn Cyber-Angriffen über die Beschäftigten. Doch wie können das Sicherheitsbewusstsein und das Wissen um diese Angriffe vermehrt und verstetigt werden?

„Tagtäglich werden 3,4 Milliarden Phishing-Mails versendet“, berichtet Amin Motalebi, Awareness Spezialist bei SoSafe. Zwar kämen nur 18 Prozent letztlich beim Adressaten an, doch seien dies immer noch rund 600 Millionen Mails, die sämtliche Spamfilter überwinden würden. Jede Zweite werde geöffnet. „Das sind 300 Millionen potenzielle Infizierungen“, rechnet Motalebi vor. Die durchschnittliche Klickrate beim Öffnen der Anhänge liege bei über 28 Prozent (rund 84 Millionen Infizierungen; Anmerkung der Redaktion). In 74 Prozent dieser Fälle würden die Beschäftigten auf falsche Login-Seiten weitergeleitet, um persönliche Daten, Benutzernamen und Passwörter abzugreifen.

„Warum ist das so einfach?“, fragt der Awarness-Spezialist – und gibt selbst die Antwort: „Weil wir Menschen sind.“ Wir seien neugierige, soziale und hilfsbereite Wesen und das sei gut. Das Problem liege darin, dass die Technik uns evolutionär überholt und abgehängt habe. Doch auf die menschliche Neugierde sei weiterhin Verlass. Deshalb seien Phishing-Mails immer wieder erfolgreich. Und: Die Nutzer dieser Attacken würden immer professioneller. Zu Beginn der Corona-Pandemie sei eine Phishing-Mail über einen Account der World Health Organisation (WHO) versendet worden. Die Klickrate habe bei über 75 Prozent gelegen.

Und die Angriffe seien sehr leicht. „Einer unserer IT-Techniker hat eine Phishing-Mail innerhalb von drei Minuten erstellt“, berichtet Motalebi. Die Klickrate lag bei 50 Prozent. „Bei den üblichen Lösegeldforderungen ist das ein sehr, sehr guter Stundenlohn.“

Das Problem ist erkannt. Laut einer Umfrage haben 57 Prozent der befragten Organisationen aus Wirtschaft und Verwaltung ihre Awareness-Maßnahmen erhöht. Weitere 40 Prozent hielten den bisherigen Status quo. Zu den Maßnahmen zählen klassische Kommunikationsformate wie Plakate und Rundschreiben, öffentliche Formate und Webinare. „Aber die tägliche Umsetzung von Wissen in Handeln bleibt ein Problem“, so der Experte von SoSafe. Motalebi rät deshalb zum täglichen Training. Awareness müsse zur Gewohnheit werden. Das könne jeder üben. Zum Beispiel indem bei jeder E-Mail die Absenderadresse genau gelesen werde.

Gemeinsam stark sein

Wie kann sich Deutschland gegen Attacken aus dem Cyber-Raum schützen?

⟩⟩⟩ von **Tim Rotthaus,** Behörden Spiegel

Was passiert eigentlich, wenn Deutschland aus dem Cyber-Raum angegriffen wird? Handelt es sich um einen kriminellen oder kriegerischen Angriff und wie lassen sich diese Angriffe effektiv abwehren? Auf der letztjährigen Public-IT-Security-Konferenz (PITS) des Behörden Spiegel wurden neben diesen Fragen auch weitere Möglichkeiten der deutschen Cyber-Abwehr in Expertenrunden diskutiert.

Die Gefahr von Angriffen auf die deutsche Verwaltung oder Kritische Infrastrukturen aus dem Cyber-Raum hat in den letzten Jahren enorm zugenommen. Attacken auf die digitale Verwaltungsinfrastruktur, wie zum Beispiel in Falle Anhalt-Bitterfeld, haben gezeigt, dass Sicherheitslücken in der deutschen Cyber-Abwehr leicht ausgenutzt werden konnten. Als Konsequenz daraus ergab sich, dass die digitale Infrastruktur des Landkreises fast komplett lahmgelegt wurde und Verwaltungsprozesse auch 2022 immer noch gestört waren.

„Kooperation, Kooperation, Kooperation!" In der Expertenrunde „Cyber Defence und ihre Möglichkeiten gegen Attacken von außen" waren sich die Experten einig, dass Deutschland nur durch bessere Zusammenarbeit effektiv geschützt werden kann. V. l. n. r.: Max Tarantik, Aris Koios, Matthias Mielimonka, Dr. Regiene Grienberger, Katharina Sook Hee Koch, Dr. Dirk Häger, Oberst i. G. Lars Ebinger

Foto: BS/Trenkel

Fehler wurden begangen

Auch wenn die Angriffe meist überraschend kommen, so sind sie dennoch nicht unabwehrbar. Dr. Dirk Häger, Abteilungsleiter Operative Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik (BSI), räumte während einer Expertenrunde zum Thema „Cyber-Defence" auf der PITS Fehler ein. „Wir haben die Gefahr, welche von Ransomware-Angriffen ausgeht, unterschätzt beziehungsweise übersehen", so Häger. Aus diesen Gründen sei erst sehr spät reagiert worden. Es sei nun aber an der Zeit für die Behörden, mehr miteinander zu kooperieren und sich besser untereinander zu vernetzen, damit es nicht noch mehr Opfer gebe, so Häger weiter. „Wenn die Bösen sich untereinander austauschen, dann müssen die Guten dasselbe tun. Ziel muss es sein, dass Cyber-Kriminalität sich einfach finanziell nicht mehr lohnt!" Es müsse jedoch schnell gehandelt werden, sagt Häger, da sonst die Gefahr eines Vertrauensverlusts der Bürgerinnen und Bürger in die deutschen Behörden steige.

Die Hacker von heute

Eine Frage, die sich in diesem Kontext natürlich stellt, ist, wer diejenigen sind, die sich in die digitale Infrastruktur einer Behörde oder eines Wirtschaftsunternehmens hacken. „Der typische Hacker von heute ist männlich und etwa 30 Jahre alt", erklärt Max Tarantik, welcher im Business Development der Firma Enginsight tätig ist. Interessant sei jedoch, dass, im Gegensatz zu anderen Kriminellen, Hacker meist aus guten sozialen Verhältnissen stammten. Tarantik sieht das Problem darin, dass junge Menschen nicht frühzeitig für die Problematik sensibilisiert würden. Schon in der Schule müsse Cyber-Sicherheit gelehrt werden, so Tarantik weiter.

Kriminell oder kriegerisch?

Was passiert nun, wenn es sich bei dem Angreifer um einen staatlichen Akteur handelt? Auch für staatliche Hacker sei die deutsche Verwaltungsinfrastruktur sehr attraktiv. „Vor allem das Auswärtige Amt ist ein sehr attraktives Ziel für Hacker", erklärte Dr. Regina Grienberger, Beauftragte für Cyber-Außen- und Cyber-Sicherheitspolitik des Auswärtigen Amtes. Hier sei es natürlich wichtig, schnell zu erkennen, ob es sich bei dem Angreifer um eine Privatperson mit kriminellem Hintergrund oder um einen staatlich unterstützten Akteur handle, sagte Dr. Grienberger. Hinweise auf einen staatlichen Akteur könnten die Größe und das Ausmaß des Angriffs sein. „Ab einer gewissen Größenordnung kann es sich nur um einen staatlichen Akteur handeln, da die benötigte Finanzierung und Infrastruktur sich für einen Kriminellen einfach nicht mehr lohnt", so Matthias Mielimonka, Chef-Koordinator des Nationalen Cyber-Abwehrzentrums. Mielimonka sieht vor allem durch Spionage- und Sabotageakte eine große Gefahr für die Wirtschafts- und Verwaltungsinfrastruktur in Deutschland. Er wünscht sich, dass Cyber-Sicherheit nicht national, sondern auch international gedacht werde. „Das Motto der Cyber-Sicherheit lautet Kooperation, Kooperation, Kooperation!", betonte Mielimonka. Oberst i. G. Lars Ebinger, Gruppenleiter CIT I 1 im Bundesministerium der Verteidigung, sieht jedoch noch ein weiteres Problem: Momentan sei nicht fest definiert, wann es sich um einen kriminellen Akt und wann es sich um einen kriegerischen Angriff handle. „Auch im Cyber-Raum müssen feste Grenzen definiert werden", so Ebinger.

Blick in die Zukunft

In einem Punkt sind die Experten sich jedoch einig: Um Deutschland effektiv vor Angriffen aus dem Cyber-Raum zu schützen, braucht es eine bessere Zusammenarbeit zwischen Verwaltung, Wirtschaft und Zivilgesellschaft. „Wir brauchen die richtigen Werkzeuge, um Angriffe rechtzeitig zu erkennen. Das bedeutet vor allem eine bessere Ausbildung von Fachkräften", so Aris Koios, Technology Strategist der Firma Crowdstrike. Koios betonte, nur gemeinsam könne ein effektiver Schutz gewährleistet werden.

(K)eine Erfolgsgeschichte – der Digitale Staat am Beispiel Onlinezugangsgesetz

⟩⟩⟩ Von **Andreas E. Thyen,** Diplom-Volkswirt und Präsident des Verwaltungsrats der LizenzDirekt AG

Wie schwer offenbar die Umsetzung des irgendwie gearteten Digitalen ist, zeigt sich am Stand der Umsetzung des Onlinezugangsgesetz (OZG) zum Ende der Frist mit Ablauf des vergangenen Jahres.

Zugang zur Onlinewelt

Der regelmäßigen Komplexität von IT-Projekte stehen die vergleichsweisen einfachen Aufgaben des Onlinezugangsgesetz gegenüber. Im Prinzip kann zur Aufgabenerfüllung bereits das Zurverfügungstellen eines Online-PDF genügen, welches nicht einmal online übersandt werden muss.

Das Gesetz begnügt sich dem Namen entsprechend damit mit dem bloßen Online-Zugang. Um die Verarbeitung der online eingegebenen Daten kümmert es sich nicht entscheidend. Wenn also Anträge für Kindergeld, Parkausweis oder Baugenehmigung digital gestellt werden, ist ungewiss, wie sich die Daten in der jeweiligen Behörde überhaupt verarbeiten lassen.

Wenn dann noch bedacht wird, dass ganze 5 Jahre Umsetzungsfrist vergangen sind, um von 575 Verwaltungsleistungen offenbar 123 auf dem zuvor geschilderten Niveau umzusetzen („Go-live"), kommen grundlegende Zweifel auf.

Föderalismus

Eine Ursache für die säumige Umsetzung kann im Föderalismus begründet sein. Denn Länder haben teilweise bereits funktionierende Online-Lösungen und der Bund umgekehrt ihnen gegenüber kein Durchgriffsrecht. Hinzu kommen die zu beachtenden extensiven rechtlichen Rahmenbedingungen, einschließlich länderspezifischen Regelungen.

Damit muss versucht werden, durch intensive Abstimmungen Lösungen zu finden. Hinzu kommt das „Einer-für-alle" Prinzip, wodurch verschiedene Bundesländer sich jeweils selbst um Antragsverfahren kümmern und diese für andere Bundesländer lizenzieren sollen. Die Schwierigkeiten sind vorprogrammiert.

Gleichzeitig wurden im Zuge des OZG etwa in den Servicestandards beachtliche Prinzipien aufgestellt, die auch im weiteren Kontext der IT-Beschaffung und -Strategie Anklang finden sollten. Zu erwähnen sind hier insbesondere offene Standards, Interoperabilität, Wiederverwendung und Nachnutzung sowie Datenschutz.

Zielvorgaben

Trotz des bescheidenen Resümees zur Umsetzung des OZG kann und darf der moderne Staat sich damit nicht begnügen. Die weiteren Herausforderungen sind im digitalen Kontext nochmals ungleich größer. Es geht um die grundlegende Digitalisierung des Staates und Resilienz staatlicher IT. Das wird nicht gelingen, wenn trotz enormer Mittel keine gesamtheitliche Strategie und Agenda aus Technologie, Prozessen, Daten und Interaktionen auf menschlicher Ebene entwickelt wird. Gleichzeitig muss eine attraktive Arbeitsumgebung geschaffen werden, in welcher die besten Experten und neue Talente ihren Platz finden, um den Staat von morgen zu bauen und Neues zu wagen. Dazu bedarf es geeigneter, nicht nur finanzieller Anreize. Tragend bleiben die grundlegenden rechtlichen Prinzipien, die keinesfalls gestatten, Ausnahmen zur Regel zu machen und das Vertrauen in den Staat begründen.

Dazu zählen europäische Prinzipien wie Produktneutralität, Wettbewerb und Mittelstandsförderung gerade bei der öffentlichen Beschaffung. Während bereits die Abhängigkeit im staatlichen Kontext insbesondere von Microsoft Produkten im On-Premise-Basis vor mehreren Jahren als kritisch erachtet wurde, nimmt diese durch unnötige Abonnements und teils sogar Cloud-Leistungen nochmals zu. Daneben werden unverblümt noch „Rahmenvereinbarungen" geschlossen und damit die Abhängigkeit perpetuiert.

Wenigstens ist und bleibt etwa der durch den Europäischen Gerichtshof 2012 etablierte Handel mit sogenannter Gebrauchter Software zu fördern und weitestgehend zu unterstützen. Damit werden in einem stark herstellerkontrollierten Markt nicht nur freier Wettbewerb gefördert und das Gebot der Wirtschaftlichkeit umgesetzt, sondern noch dazu die fundamentalen Prinzipien von Souveränität, Nachhaltigkeit und Nachnutzung gefördert.

Ausblick

Die Ziele des OZG und weiterer Initiativen sind richtig und allen kundigen Akteuren ist bewusst, dass Jahrzehnte der Versäumnisse nicht über Nacht und vielleicht auch nie aufgeholt werden können. Dennoch darf nicht verkannt werden, dass Digitalisierung nicht Selbstzweck ist, sondern der Mensch im Mittelpunkt stehen muss. Damit haben wir alle es in der Hand, Europa im digitalen Kontext auch zu erfinden und unseren Beitrag zu leisten.

Folglich kann es noch gerade zu akzeptieren sein, auf spezifische kommerzielle Produkte zu setzen. Gerade dann sind aber sämtliche Vergabegrundsätze und liberalisierende Möglichkeiten auszuschöpfen. Das bedeutet, nicht ohne Not auf „Software Assurance" oder „Abonnements", einfache Vertragsverlängerungen von EAs oder möglichst nur noch einen einzigen Hersteller zu setzen, sondern umgekehrt etwa vom wettbewerbsstarken freien Markt der Gebrauchtsoftware und vorhandenen europäischen IT-Angeboten zu profitieren.

Auf ein unabhängiges digitales 2023 in Europa und das Nachfolgesetz zum OZG!

Hohe Anfälligkeit

Cyber Security als ungelöstes Problem

⟩⟩⟩ von **Marco Feldmann,** Behörden Spiegel

Das Problem der Cyber-Sicherheit sei hierzulande immer noch nicht gelöst. Aus diesem Grunde gebe es auch weiterhin keine resiliente Cyber-Sicherheitsinfrastruktur in Deutschland. Darauf machte der ehemalige Chief Information Officer (CIO) des Saarlandes, Ammar Alkassar, aufmerksam. Ein weiteres Problem sei die Anfälligkeit Kritischer Infrastrukturen (KRITIS) für Angriffe aus dem digitalen Raum.

Darauf wies Dr. Simon Vogt, Abteilungsleiter bei der „Agentur für Innovation in der Cybersicherheit" hin. Erhebliche Schwierigkeiten sieht auch der Präsident des Cyber-Sicherheitsrates Deutschland, Hans-Wilhelm Dünn. Ex-CIO Alkassar forderte dort zudem eine stärkere Zentralisierung der Gefahrenabwehr im Cyber-Raum auf Bundesebene. Auch brauche es neue Ansätze im Beschaffungs- und Vergabebereich.

Dr. Claudia Warken, Vizepräsidentin der CSBW, verlangte auf der PITS 2022 eine verstärkte Einbindung von Hochschulen und Unternehmen in den Kampf gegen Cyber Crime. Foto: BS/Trenkel

Vertrauen ist der Türöffner

Für Letzteres erhielt er Zuspruch von Dr. Claudia Warken. Die Vizepräsidentin der „Cybersicherheitsagentur Baden- Württemberg" (CSBW) verlangte zudem, die Vernetzung aller Akteure im Kampf gegen Cyber Crime zu verbessern. Dies gelte auch in den Beziehungen zu Unternehmen und Hochschulen. Hier sei der Austausch sehr wichtig. „Vertrauen ist der Türöffner", so Warken, die Cyber-Sicherheit als kontinuierlichen Prozess betrachtet.

Christine Schönig, Regional Director Security Engineering CER bei Check Point Software Technologies, warnte vor dem großen Dunkelfeld im Bereich der Cyber Security. Hier würden die Gefahren noch zu oft unterschätzt. Und das, obwohl die Angreifenden inzwischen äußerst globalisiert und professionell agierten. Hier gebe es bereits unternehmensähnliche Strukturen. Auch würden im digitalen Raum schon Stellvertreterkriege geführt. Diese seien nicht mehr finanziell, sondern politisch-ideologisch motiviert. Oberst Tim Zahn, Kommandeur des Zentrums für Cyber-Sicherheit der Bundeswehr, sieht die Truppe derweil mit Blick auf die Absicherung gegen Attacken aus dem Digitalen gut aufgestellt. Selbstverständlich könne man hier noch besser werden. Dafür setzt er auch große Hoffnungen in die Arbeit der „Agentur für Innovation in der Cybersicherheit".

Es bleibt viel zu tun

Nicht nur im Cyber-Sicherheitsbereich gibt es noch viel zu tun. Auch beim Datenschutz existieren zahlreiche Herausforderungen. Dazu gehört u. a. die Abwägung zwischen einer großen Datenlage einerseits und der Wahrung und Erfüllung von Grundrechten andererseits. Hier müsse die Interessensabwägung in Zukunft anders erfolgen als bislang, fordert Prof. Dr. Dirk Heckmann, Inhaber des Lehrstuhls für Recht und Sicherheit der Digitalisierung an der Technischen Universität München.

Aus seiner Sicht sollten datenschutzrechtliche Bedenken gegebenenfalls zurückstehen, um andere Grundrechte (z. B. jenes auf Bildung oder auf körperliche Unversehrtheit) durchzusetzen. Dafür seien z. B. eine smarte Datennutzung sowie ein gutes Datenmanagement notwendig, so der Hochschullehrer. Denn Datennutzung sei wichtig und Datenschutz nicht schuld an der fehlenden Digitalisierung in Deutschland.

Auch der Datenschutz sei kein Verhinderer der Digitalisierung, sondern zwingende Voraussetzung für sie, unterstrich die niedersächsische Datenschutzbeauftragte Barbara Thiel. Vielmehr sei der Datenschutz erforderlich, um Vertrauen gegenüber politischen Entscheidungen innerhalb der Bevölkerung aufzubauen. Aus Thiels Sicht dürfen grundrechtsrelevante Abwägungen von der Politik nicht auf die Datenschutzaufsichtsbehörden, die zu oft stigmatisiert würden, abgewälzt werden. Hier dürften sich Politikerinnen und Politiker nicht aus der Verantwortung stehlen.

Maximal nutzfreundlich und leicht bedienbar

Thiel kritisierte, dass die Abwägung zwischen den Schutzgütern Freiheit und Sicherheit zu oft in Richtung Sicherheit erfolge. Dies erschwere die Arbeit der Datenschutzaufsichtsbehörden massiv. Denn hier hätten ihre Amtskolleginnen und -kollegen und sie deutlich weniger Befugnisse als in den übrigen Kontrollbereichen. Lob erhielt die Datenschutzbeauftragte Niedersachsens vom CEO des Unternehmens Comcrypto, Georg Nestmann. Die Datenschutzaufsichtsbehörden seien – wenn sie ein aktives Amtsverständnis hätten – durchaus Antreiber der Digitalisierung im Öffentlichen Dienst. Denn hier fehle in zahlreichen Behörden noch das entsprechende Bewusstsein für die Vorteile der Digitalisierung. Aus Nestmanns Sicht ist ein gewisser Mut zu Pragmatismus erforderlich – sowohl bei den Aufsichtsbehörden als auch bei den Anwenderinnen und Anwendern. Außerdem müssten Lösungen maximal nutzerfreundlich und leicht bedienbar sein, war er sich mit Stefan Klein, CEO von Seppmail Deutschland, und dem Country Manager von Tixeo, Valentin Boussin, einig. Sensibilität für Fragen der IT-Sicherheit sowie die Verschlüsselung von E-Mails entstünden oft erst nach einem Schadensfall, schloss der Chief Operation Officer von FTAPI, Ari Albertini.

Hilfe im Kampf gegen Ransomware & Co.

Die Zahl der Ransomware-Angriffe steigt von Jahr zu Jahr. Unternehmen, die nicht selbst zum Opfer werden wollen, dürfen sich bei der Gefahrenabwehr keine Schwächen erlauben. Die Organisationsgröße spielt in dem Zusammenhang keine Rolle mehr. Es kann jeden treffen – von der kleinen Anwaltskanzlei bis hin zum Großkonzern.

Es besteht kein Zweifel daran, dass die Bedrohung durch diese Form der Malware, die darauf abzielt, geschäftskritische Daten zu stehlen oder zu verschlüsseln, um Lösegeld zu fordern, in unserer digitalisierten Welt allgegenwärtig ist.

Für viele Organisationen wird es angesichts der Komplexität der Gefahrenlandschaft und vielfältiger Angriffsflächen jedoch immer schwieriger, den nötigen Schutz sicherzustellen. Gerade in kleinen und mittelständischen Betrieben sind IT-Budgets und Personalkapazitäten begrenzt.

Aufklärung als Grundvoraussetzung

Die Sensibilisierung aller Mitarbeiter gegenüber der konkreten Bedrohung ist eine entscheidende Maßnahme. Darüber hinaus zählen moderne IT-Security-Lösungen, die maximalen Schutz bei gleichzeitig überschaubarem Aufwand gewährleisten. Um den Gefahren die Stirn bieten zu können, wird die Umsetzung eines ganzheitlichen, mehrschichtigen Sicherheitskonzepts – das sich sowohl über Netzwerke als auch Anwender, Endpoints, Daten und Anwendungen hinweg erstreckt – zum Gebot der Stunde.

Effektive Abwehr an jeder Front

Genau an dieser Stelle setzt die Unified Security Plattform von WatchGuard Technologies an. Das Produktspektrum des IT-Security-Anbieters, der vor allem bei mittelständischen Unternehmen mit leistungsstarken und gleichzeitig einfach administrierbaren Lösungen punktet, umfasst vielfältige IT-Security-Funktionalitäten rund um Netzwerkschutz, Multifaktor-Authentifizierung, Endpoint Security und WLAN.

Maximaler Nutzen durch Unified Security

Die Stärke wurde durch die Verschmelzung aller Produktbereiche auf einer End-to-End-Plattform vereint. Auf diese Weise können Unternehmen gleich mehrere Fliegen mit einer Klappe schlagen. Auffälligkeiten sind über alle Bereiche hinweg korrelier- und bewertbar, wodurch sich gerade vielschichtigen Angriffsmustern deutlich besser auf die Spur kommen lässt. Vorfälle aus unterschiedlicher Richtung ergeben ein aussagekräftiges Gesamtbild. Durch konsequente Automatisierung werden Unternehmen in die Lage versetzt, Gefahren viel schneller und ohne manuelles Zutun zu erkennen und abzuwehren – bei gleichzeitig deutlich weniger Aufwand.

Hohe Sicherheit muss also nicht zwangsläufig mit mehr Aufwand einhergehen. Mit den neuen Möglichkeiten können selbst kleine Unternehmen umfassenden Schutz gewährleisten und Ransomware sowie anderen modernen Gefahren gezielt den Schrecken nehmen.

WatchGuard

b.o.c. IT-SECURITY

WatchGuard Unified Security Platform –
eine einheitliche Sicherheitsplattform für:

Unser **Service** für Sie:

» Sonderkonditionen für Behörden
» Alle Produkte auch online bestellbar
» Schnelle Lieferung direkt ab Lager
» Ausschreibungsservice

WatchGuard ONE PLATINUM PARTNER

BOC IT-Security GmbH | (0800) 9440440 | www.boc.de | info@boc.de

Verschiedene Ebenen der IT-Sicherheit

Nur weil es Compliance gibt, wird nicht sicher gehandelt!

⟩⟩⟩ von **Malin Jacobson,** Behörden Spiegel

Wie die ärztliche Vorsorge kann ein regelmäßiger Check-up der eigenen Sicherheitsinfrastruktur ganze Existenzen retten. Wie beim Arzt sollte man sich nicht schämen, Probleme anzusprechen – nur dann kann geholfen werden. Und wie beim Arzt bedarf es einer Nachsorge, sprich einer regelmäßigen Schulung aller Mitarbeitenden und Updates aller Technologien.

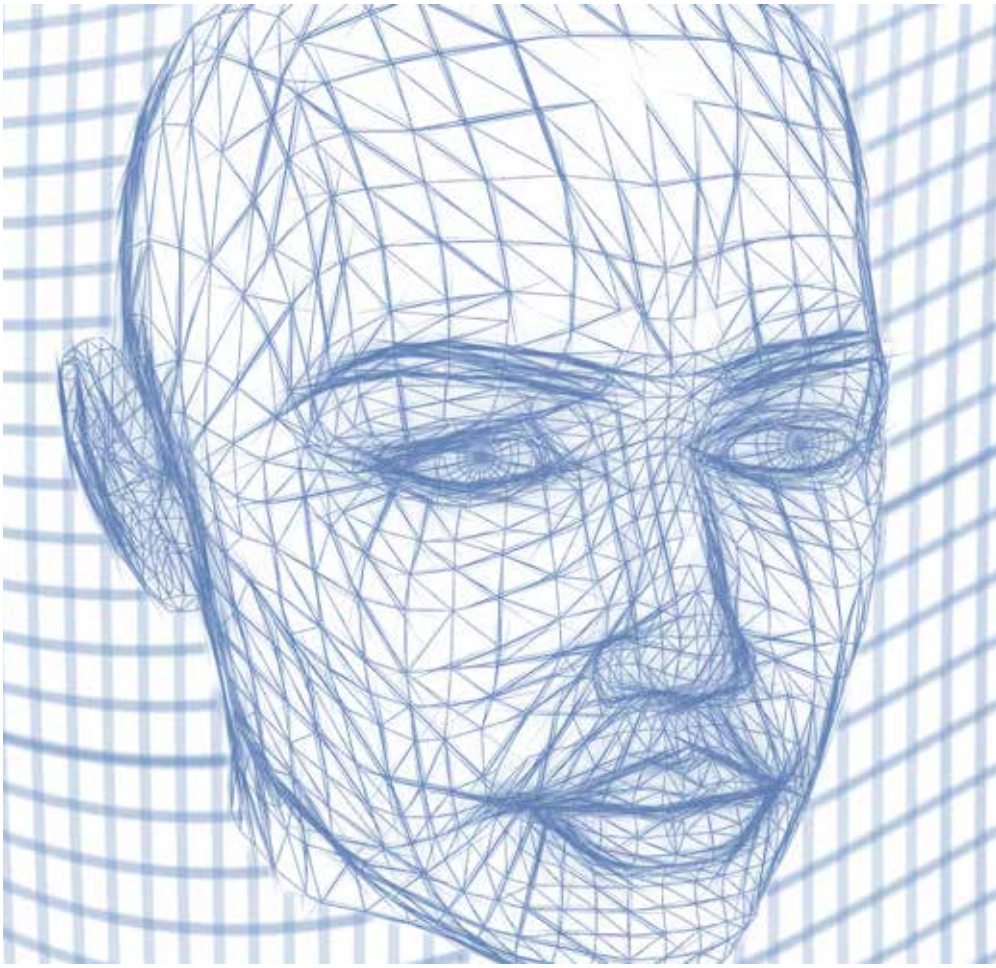
„There is no glory in prevention", zitierte Stefan Becker, Referatsleiter Cyber-Sicherheit für die Wirtschaft im Bundesamt für Sicherheit in der Informationstechnik (BSI), auf dem Public-IT-Security-Kongress (PITS) 2022. Dabei sei die Prävention so wichtig und viele würden gar nicht erkennen, wie viel Geld sie damit sparen könnten, ergänzte der IT-Sicherheitsexperte. Gerade die Schulung von Mitarbeitenden könne Unternehmen und Verwaltung auf lange Sicht viele Sorgen und Kosten ersparen. Konkret ging es in seinen Ausführungen um die Sensibilisierung für Social Engineering – die systematische zwischenmenschliche Beeinflussung zum Zweck, Informationen zu erhalten. Dr. Peter Mayer, Mitarbeiter der Forschungsgruppe: „Security, Usability, Society" des Karlsruher Instituts für Technologie (KIT), ergänzte in diesem Zusammenhang, dass gerade soziale Interaktionen wie einander helfen von Kriminellen ausgenutzt würden. „Daher sind viele IT-Sicherheitsschulungen nicht zielführend, da sie nur die Sicherheit der Software ansprechen und nicht auf das dahinterliegende soziale System eingehen."

Gamification und Simplification

Dabei sei auch wichtig, wie die Mitarbeitenden für das Thema IT-Sicherheit sensibilisiert würden, ergänzte Becker. „In dem Moment, in dem man mit dem Oberlehrerfinger kommt", erläuterte er, „bleiben nicht mehr viel Wissen oder Kompetenzen hängen." Stattdessen begrüßte er den Ansatz der Gamification, mit dem die Mitarbeitenden bereits nach dreißig Minuten die Mechanismen von Social Engineering erkennen und auf eigene Situationen übertragen könnten.

Laut Mayer sollte man sich zudem überlegen, welches Niveau an Expertise man gegenüber Mitarbeitenden kommunizieren wolle, die nicht in der Informationstechnik bewandert seien. Es sei für Verwaltungs- oder Unternehmensmitarbeitende nicht relevant, ob sie von einem Trojaner oder Virus angegriffen würden. Es als „Schadsoftware" zu bezeichnen, reiche vollkommen aus.

Man müsse generell mehr an die Endnutzerin und den Endnutzer denken, betonte der KIT-Mitarbeiter und stellte fest: „Die Technik ist nicht mit dem Fokus auf den Menschen gebaut, der sie benutzen soll, sondern für die Sicherheitslücke." Ein Beispiel seien komplexe Passwörter, die sich kein Mensch merken könne, weswegen viele eben doch auf Namen und Geburtsdaten zurückgriffen – welche sich sehr leicht im



Der Mensch wird häufig als schwächstes Glied in der IT-Sicherheit bezeichnet. Aber stimmt das und gäbe es Möglichkeiten, dieses Risiko abzuschwächen?

Foto: BS/geralt, pixabay.com

Gespräch erfragen ließen. „So entstehen unsichere Praktiken, weil sie nicht auf die Mitarbeitenden und deren Workflows abgestimmt sind“, erklärte Mayer. Gerade Crudentials, also Passwörter, in Erfahrung zu bringen, sei nach wie vor eine sehr gängige Methode von Kriminellen, um sich virtuell Zutritt zu Unternehmen zu verschaffen, betonte auch der BSI-Mitarbeitende. „Das heutzutage nicht mehr zu beachten und progressiv mit dem Thema umzugehen, ist fahrlässig!“

Unternehmenskultur ist ausschlaggebend

Neben der Prävention brauche es aber auch einen besseren Umgang mit Gefahrensituationen durch Cyber-Angriffe im Allgemeinen, waren sich die Teilnehmenden der Expertenrunde „Der Mensch als Sicherheitslücke – Social Engineering“ auf der PITS einig. „Es braucht überall Plakate mit Notfallnummern – ähnlich den Hinweisen zum Verhalten im Brandfall –, wo man anrufen kann und nicht abgemahnt wird, wenn man doch mal auf die Malware geklickt hat“, forderte Becker und ergänzte: „Moderne, fortschrittliche Fehlerkulturen sind da erforderlich.“ Des Weiteren müssten die Mitarbeitenden sich Zeit nehmen können, um die Maileingänge zu hinterfragen und gegebenenfalls Rücksprache mit Kolleginnen und Kollegen oder Vorgesetzten zu halten, meinte der Mitarbeiter der Forschungsgruppe Security, Usability, Society. „Denn dann zeigen sich die Mitarbeitenden untereinander gut gemachte und diverse Schadmails und schulen sich so gegenseitig.“

Über die Relevanz von Vorsorge und geschulter Reaktion bei Cyber-Angriffen waren sich auch die Teilnehmenden der Expertenrunde „Notfallteams im Einsatz – CERT hilft CERT“ einig. Michael Dwucet, Referatsleiter CERT-Bund, Vorfallsbearbeitung und Verbindungsstelle Nationales Cyber-Abwehrzentrum des Bundesamts für Sicherheit in der Informationstechnik (BSI), stellte in diesem Zusammenhang fest: „Wir können nicht bei jeder Bundesverwaltung die komplette Incident Response übernehmen.“ Auch im Ernstfall müssten die Zuständigen vor Ort selbstständig handeln und gegebenenfalls, beispielsweise bei Angriffen auf Netzwerkgeräte wie Router, selbst ungewöhnliche Wege finden, wieder Zugang zum System zu bekommen. „Wir haben vor allem die Rolle der Unterstützung“, betonte er. Und Volker Presse, Chief Information Security Officer beim Auswärtigen Amt, erklärte: „Bei spezifischen Angriffen mit spezifischen Geräten oder Systemen kann man nicht die gesamte Expertise vorhalten, weil der Angriff immer etwas anderes ist.“

Social Engineering

Um dennoch flexible Hilfestellung bieten zu können, habe das BSI einzelne Unternehmen weitergebildet und zertifiziert, die im Ernstfall angefragt werden könnten, erzählte Dwucet. Er gab aber auch zu bedenken, dass es im Fall eines Angriffs schon zu spät sein könnte, Kontakt zu Sicherheitsdienstleistern aufzunehmen, da diese oft schon ausgelastet seien – es sei daher wichtig, vorzusorgen und sich frühzeitig um Kontakt zu bemühen. „Nicht alle Sicherheitsabteilungen passen in CERT-Verbünde, aber ab einer gewissen Größe sollte man sich mit anderen Unternehmen und regional vernetzen.“ Und abschließend erklärte der BSI-Referatsleiter: „Für den Einstieg empfehle ich SIM3, da gibt es übersichtliche und eindrückliche rot-gelb-grüne Grafiken.“

Sandra Balz, Leitung des Bereichs Mittelstand bei Deutschland sicher im Netz, gab im Rahmen der Expertenrunde zu Social Engineering zu bedenken, dass es nicht reiche, wenn die Führungsebenen in Verwaltungen und Unternehmen sich lediglich auf Guidelines verließen und das Thema IT-Sicherheit vollkommen in die Hände der Mitarbeitenden gäben. Oder in Mayers Worten: „Mehr Menschen müssen den Unterschied zwischen Security durch Compliance und Security durch Kultur verstehen – nur weil es Compliance gibt, wird nicht sicher gehandelt!“

// SAVE THE DATE

Die Vorbereitungen für den nächten Kongress PITS – Public-IT-Security laufen bereits. Das Event findet vom 21.–22. September in Berlin statt.

Digitale Verwaltung
Rheinland-Pfalz 2022
Wandeljahre gestalten
Beschäftigte und Behörden auf dem Weg ins 4.0-Zeitalter
10. Oktober 2022 | Mainz
www.dv-rlp.de #dvrlp22

DIGITALE VERWALTUNG RLP

Resilienz im Fokus

Sozialer Aspekt muss mitgedacht werden

⟩⟩⟩ von **Matthias Lorenz,** Behörden Spiegel

Die Sorge um den gesellschaftlichen Zusammenhalt war dem Minister anzumerken. Alexander Schweitzer, in der rheinland-pfälzischen Landesregierung zuständig für die Themen Arbeit, Soziales, Transformation und Digitalisierung, mahnte auf dem Kongress „Digitale Verwaltung Rheinland-Pfalz" des Behörden Spiegel: „Resilienz ist kein Zukunftsthema mehr." Angesichts von Ukraine-Krieg, Energiekrise und Sabotage-Anschlägen müssten sich alle auf weitere schlechte Nachrichten einstellen. „Inwieweit die Menschen den Staat als handlungsfähig wahrnehmen, entscheidet darüber, wie sehr sie bereit sind, sich mit der Demokratie insgesamt zu identifizieren", so der SPD-Politiker und Schirmherr des Kongresses.

Die Überzeugung des Ministers lässt sich dabei folgendermaßen auf den Punkt bringen: Ein handlungsfähiger Staat muss ein digitalisierter Staat sein. Dabei steht für ihn nicht nur die digitale Verwaltung im Fokus. Vielmehr geht es ihm auch um soziale Aspekte: „Wir rennen gegen die Zeit an, beispielsweise beim Thema Demografie", sagt Schweitzer. Je größer ihm die Herausforderungen erschienen, desto mehr gelange er zu der Überzeugung, dass man die Digitalisierung auf allen Ebenen durchsetzen müsse. „Es gibt kaum noch andere Möglichkeiten, Menschen in ihrer jeweiligen Lebenssituation zu unterstützen und auch zukünftig für gleichwertige Lebensverhältnisse zu sorgen." Digitalisierung müsse auch dazu beitragen, das Teilhabeversprechen der Demokratie aufrechtzuerhalten.

Riesennachholbedarf

Trotzdem ist eine effektive Verwaltung für einen handlungsfähigen Staat unerlässlich. Durch die Pandemie hätten viele Bürgerinnen und Bürger die Erfahrung gemacht, dass die Digitalisierung den Alltag präge, erklärt Schweitzer. Die Wahrnehmung sei allzu oft, dass der Staat hier noch nicht so weit sei. „Wir haben einen Riesennachholbedarf und müssen weiter an Tempo zulegen, um die Ansprüche der Bürger zu erfüllen."

Grafik: BS/Hoffmann unter Verwendung von stock.adobe.com, Panithan

Auch der Staatssekretär und CIO des Landes Rheinland-Pfalz, Fedor Ruhose, ist der Ansicht, dass der Staat durch digitale Verwaltung resilienter werde. „Durch die Digitalisierung und Automatisierung von Prozessen werden Freiräume für die Verwaltung geschaffen, durch die sie sich wieder verstärkt um die wichtigen Anliegen kümmern kann." Deswegen sei es unter anderem wichtig, dass es nach der Umsetzung des Onlinezugangsgesetzes (OZG) eine neue Dynamik für eine durchgängige und nutzerorientierte Verwaltungsdigitalisierung gebe. Hierfür müsse unter anderem das Einer-für-alle-Prinzip weiterentwickelt werden. Daneben brauche es auch eine dauerhafte Finanzierung. Schließlich müsse auch ein Anreizsystem für die Digitalisierung entwickelt werden. „Digitalisierungsdividenden sollen dort verbleiben, wo sie erwirtschaftet werden", fordert Ruhose.

Ebenfalls wird in der Landeshauptstadt Mainz die Meinung vertreten, dass bei der Digitalisierung der soziale Aspekt nicht zu kurz kommen dürfe. Wie die Mainzer Wirtschaftsdezernentin Manuela Matz (CDU) erläutert, betrachte man in der städtischen Digitalstrategie „mainzDIGITAL" neben den Handlungsfeldern Digitale Verwaltung, Intelligente Infrastruktur, Wirtschaft und Mobilität auch das Handlungsfeld Bildung und Zusammenleben. „Digitale Fähigkeiten müssen so selbstverständlich in der Gesellschaft verankert sein wie Lesen, Schreiben und Rechnen", sagt Matz.

Deswegen setze man an den Mainzer Schulen Digitalscouts ein. Dadurch würden digitale Themen schon dort beleuchtet, erläutert die Wirtschaftsdezernentin. Ein anderes Schulprogramm habe sich speziell mit der IT-Sicherheit befasst. „In dem Moment, wo die Themen bei den Schülern adressiert sind, werden auch die Eltern mit eingebunden", weiß Matz. Eine digitale Grundbildung erachtet auch Minister Schweitzer als sehr relevant. „Wir müssen auch jene ansprechen, bei denen die Digitalisierung in der Ausbildung noch keine Rolle gespielt hat." Inzwischen würden rund 400 Digitalbotschafter in ganz Rheinland-Pfalz die Weiterbildungsarbeit in Sachen Digitalisierung unterstützen.

Breitbandausbau weiter forcieren

Damit die Gesellschaft die Vorteile der Digitalisierung nutzen kann, muss schließlich auch für eine passende Infrastruktur gesorgt werden. Aufgrund der Topografie sei der Breitband-Ausbau im Land nicht ganz einfach, beschreibt Schweitzer die Situation. Falls der eigenwirtschaftliche Ausbau nicht funktioniere, müsse auch der Staat eingreifen. Manuela Matz fordert in diesem Zusammenhang, eine Förderung auch für die Bekämpfung von grauen Flecken im städtischen Raum aufzuerlegen. Bisher habe man sich weitestgehend auf den ländlichen Raum fokussiert.

Der Breitbandausbau soll in Rheinland-Pfalz demnächst mit einer weiteren digitalen Antragsplattform unterstützt werden. Bereits zur Verfügung steht das OZG-Breitband-Portal, welches von Rheinland-Pfalz gemeinsam mit Hessen und der Metropolregion Rhein-Neckar (MRN) entwickelt wurde. Im Rahmen des Kongresses startete Minister Schweitzer nun auch das neue Daten-Informations-Portal für den Breitbandausbau. „Auf der neuen Plattform können rheinland-pfälzische Kommunen ihre Anträge auf eine Landesförderung im Rahmen der Graue-Flecken-Förderung künftig auch digital und medienbruchfrei beim Land einreichen", erklärt Schweitzer in diesem Zusammenhang. Neben der digitalen Antragstellung für Kommunen soll das Portal künftig auch relevante Informationen zur Breitbandversorgung sowie zum Breitbandausbau bereithalten. Dazu gehören etwa die durch das Land initiierten, flächendeckenden Netzdetailplanungen, welche den Kommunen einen Überblick über den geplanten Netzausbau durch die Telekommunikationsunternehmen liefern.

Alexander Schweitzer, der Digitalminister des Landes Rheinland-Pfalz, hält die Digitalisierung für unerlässlich, damit der Staat handlungsfähig bleibt. Foto: BS/Albert

Zukunft nach dem OZG

Es muss noch viel getan werden

⟩⟩⟩ von **Tim Rotthaus,** Behörden Spiegel

Dass es sich bei der Verwaltungsdigitalisierung und der Umsetzung des Onlinezugangsgesetztes (OZG) um eine Daueraufgabe handelt, ist den meisten Experten und Verantwortlichen schon lange klar. Wie der aktuelle Stand der Verwaltungsdigitalisierung ist, was bisher erreicht wurde und wo die Reise in Zukunft hingeht, wurde auf dem Kongress Digitale Verwaltung Rheinland-Pfalz 2022 kontrovers diskutiert.

Die Bilanz fiel eher nüchtern aus. „Wir stehen noch ganz am Anfang und müssen noch viel mehr machen", erklärte Marco Brunzel, Dozent an der Universität Speyer. Für die schleppende Umsetzung gebe es viele Gründe, zwei der größten Hürden seien jedoch die fehlenden Nutzerkompetenzen und niedrige Anwenderzufriedenheit, so Brunzel weiter. Um die Umsetzung voranzutreiben, müsse in diesen Bereichen noch einiges getan werden. Dennoch sieht der Digitalisierungsexperte eine positive Entwicklung. Es gebe jetzt schon mehr Kooperationen zwischen den einzelnen Akteuren. So werde auf Bundes- und Landesebene erfolgreich miteinander kommuniziert und zusammengearbeitet. „Wir müssen uns den Maschinenraum des Föderalismus genau anschauen", erklärt Brunzel. Dort, wo Kooperationen möglich und sinnvoll seien, müssten diese auch eingegangen werden.

Die Verwaltungsdigitalisierung betrifft jedoch nicht nur die Bürgerinnen und Bürger, sondern auch die Wirtschaft. Dr. Christine Brockmann, Vorstand des Arbeitskreises Wirtschaftliche Verwaltung e. V., ist der Meinung, dass bei Diskussionen über die OZG-Umsetzung und der Verwaltungsdigitalisierung ein zu großer Fokus auf die Bürgerinnen und Bürger gelegt wird. Es gebe viel zu wenig Angebote, die sich an die Wirtschaft richteten, so Brockmann. „Die Prozesse wurden für die Wirtschaft nicht zu Ende gedacht." Firmen und Wirtschaftsvertreter hätten häufig mit den gleichen Verwaltungsapparaten und -prozessen zu tun, erläutert Brockmann weiter. Es wäre daher von Vorteil, wenn diese Prozesse so einfach wie möglich gehalten würden. Momentan sei die Interaktion zwischen der Wirtschaft und der Verwaltung, aber auch zwischen Verwaltung und Bürgern, immer noch zu analog.

Bei der OZG-Umsetzung gebe es zu wenig Angebote, welche sich an die Wirtschaft richteten, kritisiert Dr. Christine Brockmann.

Foto: BS/Janno Nivergall, pixabay.com

Brockmann sieht in dem Once-Only-Prinzip eine Lösung des Verwaltungsstaus. Mit dieser Herangehensweise soll es möglich sein, dass Unternehmen und Bürger gewisse Nachweise nur noch einmalig erbringen müssen. Diese Nachweise werden dann zwischen den verschiedenen Behörden digital geteilt, damit sie nicht nochmals erbracht werden müssen. Ziel müsse es sein, dass die Verwaltung für alle Beteiligten nicht spürbar sei, so Brockmann.

Eine weitere Gefahr der eher schleppenden Umsetzung des OZG sieht Marcel Boffo vom Referat E-Government, Kooperation mit EU, Bund, Ländern und Kommunen aus dem Ministerium für Arbeit, Soziales, Transformation und Digitalisierung Rheinland-Pfalz, darin, dass Deutschland im europaweiten Vergleich abgehängt werden könnte. Viele Nachbarn der Bundesrepublik würden schon seit einiger Zeit Konzepte wie das Once-Only-Prinzip erfolgreich anwenden. „Wir können nicht warten, bis wir ein Gesamtkonzept entwickelt haben", warnt Boffo.

Eine gute Bilanz

Neuer Ressortzuschnitt hat sich bewährt

Mitte Mai 2021 übernahm Alexander Schweitzer in Rheinland-Pfalz die Führung des neu geschaffenen Ministeriums für Arbeit, Soziales, Transformation und Digitalisierung (MASTD). Staatssekretär Fedor Ruhose wurde CIO/CDO der Landesregierung und Vertreter des Landes im IT-Planungsrat. Nach rund einem – durch Pandemie, Ukraine-Krieg und die Naturkatastrophe im Ahrtal – sicherlich nicht leichten Jahr, zogen beide im Gespräch mit Behörden Spiegel-Redakteur Guido Gehrt eine Zwischenbilanz, blickten jedoch auch in die Zukunft der digitalen Transformation im Lande. Das Interview wurde im Sommer 2022 geführt.

***Behörden Spiegel:** Herr Minister Schweitzer, Sie haben vor gut einem Jahr das neu geschaffene Ressort für Arbeit, Soziales, Transformation und Digitalisierung übernommen. Wie fällt Ihre Zwischenbilanz aus?*

Schweitzer: Die Bilanz fällt ausgesprochen gut aus. Das Jahr war vollgepackt mit Themen, Vorhaben, öffentlichen Anlässen und Terminen. So wurde unser Haus sehr schnell innerhalb des Landes und in den öffentlichen politischen Debatten, den Fach-Communities und darüber hinaus sichtbar. Gleichzeitig muss man sagen, dass das zurückliegende

Alexander Schweitzer ist Minister für Arbeit, Soziales, Transformation und Digitalisierung des Landes Rheinland-Pfalz. Foto: BS/MASTD

Jahr für Rheinland-Pfalz ein schweres Jahr war. Wir haben bis heute als Sozial- und Arbeitsministerium sehr intensiv mit der Pandemie zu tun. Wir hatten im Sommer 2021 eine furchtbare Naturkatastrophe im Ahrtal, wo wir als das für den Arbeitsmarkt, die Pflege, die Eingliederungshilfe und die digitale Infrastruktur zuständige Ministerium unmittelbar betroffen waren. Zudem haben wir es seit dem 24. Februar 2022 mit den furchtbaren Folgen eines Angriffskrieges der Russischen Föderation auf die Ukraine zu tun, mit all den Auswirkungen auf den Arbeitsmarkt, aber auch was Themen wie IT-Sicherheit angeht. Somit sind wir insgesamt über das Portfolio des Ministeriums sehr stark in der Krisenreaktion und Krisenbewältigung engagiert. Gleichzeitig haben wir einen sehr ehrgeizigen Koalitionsvertrag, der einen starken Fokus auf unser Ministerium legt.

Angesichts dieser Vielfalt der Herausforderungen: Hat sich der neue Ressortzuschnitt als sinnvoll und leistungsfähig herausgestellt?

Schweitzer: Eindeutig ja! Es ist ein ungewöhnlicher Ressortzuschnitt, der aber nach meiner Ansicht sehr gut zusammenpasst. Nehmen Sie das Thema Transformation: Wir haben sehr schnell festgestellt, dass alle unsere Partner im Land, ob das Pflegeeinrichtungen oder Unternehmen aus jeglichen Bereichen des Arbeitsmarktes sind, mit ganz spezifischen Herausforderungen der Transformation befasst sind. Diese Partner wünschen sich einen Rahmen, brauchen eine entsprechende Infrastruktur und letztlich auch Unterstützung, wenn es um Qualifizierung und Weiterbildung geht. Dies hängt maßgeblich mit den Themen Digitalisierung und Demografie zusammen, beides Zuständigkeiten meines Hauses. Um weiterhin erfolgreich zu sein, brauchen wir in allen Bereichen – von der Pflege über den Mittelstand bis hin zu den Großunternehmen – Fachkräfte, um auch in Zukunft weiterhin gute Produkte und Dienstleistungen anbieten zu können. Auch hier sind wir als Arbeitsmarktministerium für Weiterbildung und Qualifizierung zuständig. Somit haben wir einen Zuschnitt, der das ganze Thema Arbeiten, Teilhabe und Zukunft durch gute Infrastruktur insgesamt um-

Fedor Ruhose ist Staatssekretär im Ministerium für Arbeit, Soziales, Transformation und Digitalisierung Rheinland-Pfalz und CIO/CDO der Landesregierung. Foto: BS/MASTD/Peter Pulkowski

fasst. Digitalisierung ist keine reine technologische Frage, sondern der Grad der Digitalisierung und der Erfolg einer Digitalisierungsstrategie bemisst sich nach meiner Auffassung daran, ob ich es schaffe, möglichst viele Menschen zu überzeugen und mitzunehmen, wenn es darum geht die Chancen der Digitalisierung im Privaten, im Bereich der Bildung und im Bereich des Arbeitsmarktes für sich zu erkennen und zu erleben. Genau das ist unsere Aufgabe.

Herr Staatssekretär Ruhose, Sie sind seit gut einem Jahr CIO und CDO

der Landesregierung. Wie fällt Ihre bisherige Bilanz aus?

Ruhose: Wenn man auf das Jahr zurückblickt, dann haben wir – gemeinsam mit den kommunalen Spitzenverbänden und den Kommunen – neuen Schwung in die Verwaltungsdigitalisierung und insbesondere in den OZG-Prozess in Rheinland-Pfalz gebracht. Seit Mai 2021 haben der Minister und ich auf der Bundesebene wiederholt Impulse gesetzt, um uns in der Diskussion über das Onlinezugangsgesetz ein Stück weit ehrlicher zu machen. Gleichzeitig haben wir aber auch nie den Ehrgeiz aufgegeben, die gesteckten Ziele, in Bereichen in denen dies möglich ist, auch tatsächlich zu erreichen. Hier haben wir uns ebenfalls mit den rheinland-pfälzischen Kommunen auf den Weg gemacht und Priorisierungen vorgenommen. Dabei haben wir den Fokus einerseits darauf gelegt, welchen Nutzen die digitalen Verwaltungsleistungen für die Bürgerinnen und Bürger vor Ort haben, aber andererseits auch auf die Auswirkungen auf verwaltungsinterne Prozesse. Unter dieser Prämisse haben wir in Rheinland-Pfalz dann mit Blick auf die OZG-Umsetzung Priorisierungen vorgenommen, was nun im IT-Planungsrat unter dem Stichwort „OZG-Booster" nachvollzogen wurde. Vor diesem Hintergrund sind wir entschlossen, bis zum Jahresende 2022 möglichst viele OZG-Leistungen in den Roll-out zu bekommen.

Das Einer-für-alle-Prinzip bietet Bund, Ländern und Kommunen eine neue Art der Zusammenarbeit. Foto: BS/Gerd Altmann, pixabay.com

Momentan muss die OZG-Umsetzung viel Kritik einstecken, gerade auch mit Blick auf die Geschwindigkeit. Was kann man denn an positiven Erfahrungen aus dem Prozess mitnehmen, auch im Hinblick auf ein OZG-Folgegesetz?

Ruhose: Ich finde es grundsätzlich überaus positiv, dass die OZG-Umsetzung zu einer neuen Form der Zusammenarbeit zwischen Bund, Ländern und Kommunen geführt hat. Wenn es uns gelingt, die Vorteile, die der Einer-für-alle-Ansatz bietet, in die Zukunft zu übertragen und in einem OZG-Folgegesetz entsprechend zu verankern, wäre das aus meiner Sicht ein großer Fortschritt. Ganz unabhängig davon, was bis zum 31. Dezember 2022 alles umgesetzt ist, hat der OZG-Prozess unbestreitbar – gerade auch durch die Fristsetzung – eine ziemlich große Dynamik bei der Verwaltungsdigitalisierung entfaltet. Dies muss man, bei aller Kritik, dem OZG einfach auch mal positiv anrechnen. Mit unserer Priorisierung im Land und dem OZG-Booster bringen wir jetzt nochmal eine zusätzliche Dynamik in den Gesamtprozess. Klar ist für mich beim OZG-Folgegesetz, dass die Fortführung der Digitalisierung nach dem OZG letztlich nur in eine vollständige Ende-zu-Ende-Digitalisierung der Verwaltungsprozesse münden kann. So verstanden, wird Verwaltungsdigitalisierung zu einem anderen Verständnis von Verwaltung führen. Sie wird zudem eine Daueraufgabe. Dieser permanente Modernisierungs- und Digitalisierungsprozess kennt im Grunde kein Ende.

Herr Minister Schweitzer, wie krisenfest ist der Prozess des digitalen Wandels vor dem Hintergrund Corona/Ukraine und damit verbundener wirtschaftlicher Herausforderungen?

Schweitzer: Die Zeitenwende, die durch den Ukraine-Krieg ausgelöst wurde, ist ein überdeutlicher Hinweis darauf, dass wir uns mit der Transformation keine Zeit lassen können. Wir hatten schon vor der Ukraine-Krise das Pariser Abkommen und andere Vereinbarungen, was die $C0_2$-Neutralität unserer Wirtschaft angeht. Aber jetzt ist jedem klargeworden, dass es keine Alternative dazu gibt, dass wir zukünftig unabhängiger werden müssen. Dies wiederum setzt die heimische Industrieproduktion, die Zuliefererbetriebe und die kleinen und mittleren Dienstleister– also die überwiegende Mehrheit der Unternehmen in Rheinland- Pfalz – unter enormen Druck. Die Transformationsaufgaben haben sich somit nochmals beschleunigt. Plastisch ausgedrückt: Die Transformation wird nun nicht mehr leise anklopfen, sondern gleich die Tür eintreten. Darauf müssen sich die Organisationen mit unserer Unterstützung entsprechend vorbereiten. Die Aufgaben unseres Ressorts sind also in dieser Krise wichtiger denn je. Ein weiterer Punkt kommt hinzu: Es gibt eine enorm hohe Erwartung vieler Bürgerinnen und Bürger, dass die Verwaltung aus diesen zwei Jahren Pandemie mit einem anderen Gesicht herauskommt. Staatssekretär Ruhose hat den OZG-Prozess bereits angesprochen. Auch hier erlebe ich Rückenwind. Das ganze Thema Autonomie im Bereich Wirtschaft, im Bereich digitale Verwaltung oder im Bereich digitale IT-Sicherheit hat Rückenwind bekommen. Das heißt, aus Gründen, die ich mir nicht gewünscht hätte, sind die Themen meines Ministeriums eher noch mal priorisiert worden. An politischer Unterstützung für diese notwendigen Prozesse wird es meiner Ansicht nach auch zukünftig nicht fehlen. Ich sehe die Herausforderung insbesondere darin, ob wir das Tempo, welches wir uns für die digitale Transformation kollektiv vorgenommen haben, letztlich auch werden halten können, etwa beim Ausbau der digitalen Infrastruktur. Hier stehen meiner Ansicht nach genug finanzielle Mittel zur Verfügung. Meine Sorge ist zurzeit eher, dass wir

es nicht schaffen, die öffentlichen Investitionsvorhaben von Bund, Ländern und Kommunen im geplanten Zeitrahmen auch tatsächlich umzusetzen, etwa weil nicht genügend Baukapazitäten zur Verfügung stehen und andere limitierende Faktoren hinzukommen. Daher müssen wir uns auf allen staatlichen Ebenen darauf verständigen, dass wir nicht Strohfeuer organisieren, sondern wir eine Perspektive in den Blick nehmen, die über eine Wahlperiode hinausgeht. So geben wir den Anbietern am Markt auch die erforderliche Sicherheit und Verlässlichkeit, um sich dauerhaft für den erfolgreichen Ausbau der digitalen Infrastruktur zu engagieren.

Im Ahrtal läuft nach dem verheerenden Hochwasser des Juli 2021 derzeit der Wiederaufbau. Wo liegen hier die Schwerpunkte mit Blick auf die Digitalisierung?

Schweitzer: Die dramatischen Ereignisse der Flutnacht vom Juli 2021 werden uns noch sehr lange beschäftigen. Umso wichtiger ist es, dass konkrete Ergebnisse beim Wiederaufbau wahrnehmbar sind. Uns war bereits unmittelbar in den ersten Stunden nach dem Ereignis wichtig, dass wir sofort Kontakt zu den Telekommunikationsunternehmen aufnehmen, um gemeinsam mit diesen die Mobilfunkerreichbarkeit wiederherzustellen. Hier war ich sehr froh, dass alle Unternehmen – ob Telekom, Telefónica oder Vodafone – umgehend ihre Kapazitäten im Ahrtal und in der Region konzentriert haben. So ist es gelungen, innerhalb von wenigen Tagen die telefonische Erreichbarkeit wiederherzustellen. Anschließend haben wir uns gemeinsam Gedanken gemacht, wie man die Infrastruktur bestmöglich wiederaufbauen könnte. Das Ergebnis kann ich schnell zusammenfassen: Es wird dort zukünftig die modernste digitale Infrastruktur einer ländlichen Region in Rheinland-Pfalz geben. Denn anstelle der zerstörten Kupfer-Infrastruktur, und das sind mehrere tausend Kilometer, wird die Deutsche Telekom eigenwirtschaftlich Glasfaser ausrollen. Im Ahrtal werden so in den nächsten Wochen und Monaten rund 1.500 Kilometer Glasfaser verlegt und rund 22.000 Haushalte mit FTTH versorgt. Für den Mobilfunk gilt dies ähnlich. Wenn die Mobilfunkmasten mit Glasfaser angebunden sind, bietet das auch Möglichkeiten für 5G und 5G-Plus. Diese Stärkung der digitalen Infrastruktur soll die Bürgerinnen und Bürger zusätzlich ermutigen, in der Region zu bleiben. Ein leistungsfähiger Glasfaseranschluss an der Kellertür ist hier sicherlich ein nicht zu unterschätzender Standortfaktor. Daher bin ich sehr froh, dass die Telekommunikationsunternehmen hier zukünftig entsprechende Angebote bereitstellen werden.

// SAVE THE DATE

Die Vorbereitungen für den nächten Kongress Digitale Verwaltung Rheinland-Pfalz laufen bereits. Das Event findet am 27. November in Mainz statt.

Grundsätze der Beschaffung gebrauchter Software-Lizenzen

durch öffentliche Auftraggeber

2. erweiterte Auflage 2021 (erhältl. in Deutsch, Englisch u. Französisch)

Aus dem Inhalt:

- Einleitung und Maßstab
- Zusammenfassung von Grundlagen
- Rechtliche Ausgestaltung der EuGH-Grundsatzentscheidung
- Vergaberechtliche Grundlagen unter Berücksichtigung von EuGH und BGH
- Die Beschaffung gebrauchter Software-Lizenzen in der Praxis
- Fazit
- Checkliste

Das Praxishandbuch steht kostenfrei zum Download bereit unter: www.behoerden-spiegel.de/sonderpublikationen/

e-nrw. Zukünftige IT-Strategien in Nordrhein-Westfalen

Krisen – Hemmschuh oder Katalysator für die Digitalisierung in NRW?

3. November 2022, Stadthalle Neuss

Referenten und Referentinnen, u. a.:

Foto: © MWIDE NRW/M. Hermenau

Prof. Dr. Andreas Meyer-Falcke,
Beauftragter des Landes Nordrhein-Westfalen für Informationstechnik (CIO)

Foto: © Stadt Bad Salzuflen

Lena Sargalski,
Chief Digital Officer, Stadt Bad Salzuflen

Foto: © Landkreistag NRW

Dr. Martin Klein,
Hauptgeschäftsführer Landkreistag Nordrhein-Westfalen

Ausführliche Informationen zum Programm und Anmeldung unter: www.e-nrw.info

E-NRW

„Deutschland kann Krise!“

Qualität schafft Vertrauen – Vertrauen schafft Nutzung

〉〉〉 von **Tanja Klement / Matthias Lorenz / Guido Gehrt,** Behörden Spiegel

Es geht längst nicht mehr um die Bewältigung einzelner Krisen, sondern wir sind seit vielen Jahren mit Herausforderungen verschiedenster Art konfrontiert“, konstatierte Daniel Sieveke, Staatssekretär im nordrhein-westfälischen Ministerium für Heimat, Kommunales, Bau und Digitalisierung, auf dem Kongress e-nrw. Neben dem Krieg nannte er die Energiekrise, die Pandemie oder den demografischen Wandel. Auch die Flüchtlingskrisen, den Klimawandel oder der Fachkräftemangel führte er an. Doch wie wirkten sich diese Krisen auf die Digitalisierung der Verwaltung aus?

Staatssekretär Sieveke hatte hierüber eine klare Vorstellung: Nach Corona habe es oft geheißen, die Pandemie habe die Digitalisierung vorangetrieben. Dies sei zwar richtig, aber eigentlich müsse es anders sein, nämlich „digital durch die Krise“. Bürgerinnen und Bürger erwarteten, dass die staatliche Verwaltung auf Krisen effektiv reagieren könne. „Darüber hinaus müssen wir uns auch für die Zukunft wappnen. Hierfür braucht es Krisenfestigkeit und Resilienz, das ist nur mit digitaler Verwaltung möglich“, so Sieveke.

Der CIO des Landes Nordrhein-Westfalen, Prof. Dr. Andreas Meyer-Falcke, betonte in diesem Zusammenhang: „Deutschland kann Krise! Dies gilt sowohl für die Bürgerinnen und Bürger als auch für die Verwaltung.“ Meyer-Falcke verwies dabei auf die große Hilfsbereitschaft der Bevölkerung bei der Aufnahme von Geflüchteten. Während der Pandemie habe die Verwaltung entgegen der Erwartung der breiten Masse auch im Lockdown von zu Hause aus funktioniert, zum Beispiel weil Tools wie die E-Laufmappe bereits verfügbar gewesen seien.

Kommunen machen mit

Daneben betonte Meyer-Falcke die Funktion von Krisen als Katalysator: „Eine Krise zwingt uns zum Handeln und zum Zusammenstehen, also zum Zusammenarbeiten unterschiedlicher Strukturen.“ Inzwischen gebe es einige Beispiele für eine solch gut funktionierende Zusammenarbeit zwischen

föderalen Ebenen, sagte der Landes-CIO und nannte als Beispiel unter anderem das CERT NRW. Dieses sei ursprünglich für die Landesverwaltung gedacht gewesen, mittlerweile sei es als kommunaler Warn- und Informationsdienst ausgerollt worden. „Wir sehen jetzt: Die Kommunen machen mit!", freute sich Meyer-Falcke. Es brauche also nicht jeder ein eigenes CERT.

Für mehr Vorgaben ist auch der Dezernent für Stadtentwicklung, Wirtschaft, Digitalisierung und Regionales der Stadt Köln: „Wir müssen als Kommune auch auf das Land oder den Bund hören, falls von dort Lösungen vorgegeben werden", sagte Andree Haack, der das Dezernentenamt in der Domstadt seit August 2022 bekleidet. Man müsse sich unterordnen, damit es kein Durcheinander gebe. Wenn Kommunen solche Lösungen implementierten, müssten parallel allerdings auch Schulungs- und Supportstrukturen aufgebaut werden, forderte er.

Daneben nannte Haack eine spezifisch „kölsche" Eigenheit. Als jemand, der neu in die Stadt gekommen sei, sei ihm aufgefallen, dass in Köln unglaublich viele Menschen mitreden wollten. „Das macht die Prozesse nicht einfacher und schlanker." Genau eine solche Verschlankung müsse aber stattfinden, ansonsten verheddere man sich in Details.

Komplexität senken

Der Hauptgeschäftsführer des Landkreistages (LKT) NRW, Dr. Martin Klein, stellte angesichts der multiplen Krisen und der demografischen Entwicklung neun Handlungsempfehlungen vor, um die Komplexität der Verwaltungsdigitalisierung in NRW und bundesweit zu senken:

1. Es müsse eine Umkehr von der Online-Portal-Vielfalt der föderalen Ebenen und Ressorts erfolgen. Alle Verwaltungsportale sollten zu einer standardisierten Mehrschichten- Plattform-Infrastruktur konsolidiert werden, die eine mandantenfähige und konfigurierbare Schicht für alle Behörden biete, so der LKT-NRW-Hauptgeschäftsführer.

2. Die Ressourcen zur Konsolidierung der Service- und Nutzerkonten des Bundes und der Länder sollten, so Klein, zu einem einzigen „Nutzerkonto Deutschland" mit abgestuften Vertrauensniveaus gebündelt werden.

3. Nach Ansicht Kleins sollten technische und rechtliche Rahmenbedingungen für standardisierte und gesetzlich normierte Basisdienste geschaffen werden, die von Bund und ggf. auch von den Ländern betrieben werden. Dabei sollten folgende Punkte erfüllt werden:
   - Umsetzung eines rechtssicheren Postfaches, das eine bidirektionale, verbindliche und vertrauliche Kommunikation ermögliche.
   - Erhöhung der Anstrengungen zum Ausbau eines benutzerfreundlichen Einsatzes der eID des Personalausweises unter Einbeziehung der Bürger, der Wirtschaft sowie Zivilgesellschaft. Gleiches gelte für das ELSTER-Unternehmenskonto.
   - Bereitstellung eines dauerhaften rechtssicheren elektronischen Siegel- und Signaturdienstes.
   - Entscheidung über einen deutschlandweiten, einheitlichen verschlüsselten Datentransportstandard (OSCI, XTA oder FIT-Connect).
   - Einführung einer souveränen, standardisierten und verbindlichen Zahlungsschnittstelle bzw. eines entsprechenden Zahlungsdienstes.

4. Klein fordert eine Straffung der Gremienstrukturen auf Bundesebene durch Einführung eines mit Generalvollmachten, Budget und Gesetzgebungsvorschlagsrecht ausgestatteten Boards, das ressortübergreifend und über Legislaturperioden hinweg die Digitalstrategie Deutschlands führt. Alle föderalen Ebenen müssten im Board in ausreichendem Maße mit angemessenem Stimmrecht vertreten sein. Dabei sei insbesondere die kommunale Selbstverwaltungsgarantie zu achten. Auch beim NRW-Kooperationsrat sei eine Weiterentwicklung erforderlich, damit es zu verbindlicher wirkenden bzw. steuernden Handlungsoptionen komme. Dabei müssten die kommunale Organisationshoheit einerseits und das Konnexitätsprinzip andererseits gewahrt bleiben. Nach den bisherigen Erfahrungen könne der IT-Kooperationsrat mit seinen empfehlenden Beschlüssen nur selten der zentralen Bedeutung des Gremiums für die NRW-Verwaltungsdigitalisierung gerecht werden, so Klein.

5. Klein will die IT-Dienstleister des Bundes, des Landes sowie der Kommunen einer Aufgaben- und Leistungskritik unterziehen, damit eine Verzahnung mit den Potenzialen der freien Wirtschaft und Wissenschaft erfolgen kann. Vor diesem Hintergrund werde in NRW aktuell ein von den kommunalen Spitzenverbänden und dem Land angestoßenes Gutachten zur Überprüfung und Weiterentwicklung der kommunalen IT auf den Weg gebracht.

6. Für den Hauptgeschäftsführer bedarf es zudem einer Konzeption für ein Bund, Länder und Kommunen umfassendes Finanzausgleichssystem für die dauerhafte Bereitstellung von digitalen Verwaltungsleistungen. So soll dauerhaft eine adäquate personelle, finanzielle und technische Ausstattung ermöglicht werden, um die oben erwähnten Aufgaben zu bewältigen.

7. Es müsse eine digitale Lernumgebung für die Beschäftigten der öffentlichen Verwaltung geschaffen werden. In diesem Zusammenhang sei auch zu prüfen, inwiefern Behörden ihre Bediensteten verstärkt zur kontinuierlichen Qualifizierung und Weiterbildung anhalten könnten.

8. Open Code, Open Source, Open Data und ein stringentes Open Government stärkten das Vertrauen der Bürgerinnen und Bürger in ihren Staat und müssten daher häufiger eingesetzt bzw. angeboten werden. Klein ist sich sicher: „Nur mit größtmöglicher Transparenz werden Bürger ihre Daten dem Staat dauerhaft elektronisch anvertrauen wollen und gegegenüber einer potenziellen zentralen Bürger-ID aufgeschlossen sein."

9. Beim Thema Datenschutz müssten bestehende Rechtsunsicherheiten geklärt werden. Vor dem Hintergrund, dass sich mindestens 370 Verwaltungsleistungen im kommunalen Vollzug befänden, sei es im Sinne einer schnellen Umsetzung

notwendig, dass nicht jede Kommune bei jeder nachnutzbaren Leistung eine eigene Datenschutzbeurteilung zu beauftragen habe, sondern eine zentrale Beurteilung erfolge.

Gemeinsamer Anspruch müsse es sein, so Klein abschließend, qualitativ hochstehende, sichere und nutzerzentrierte digitale Verwaltungsleistungen anzubieten. Denn der aktuelle „eGovernment MONITOR" zeige, dass die Wiedernutzungsbereitschaft der Nutzenden bei über 90 Prozent liege. Das bedeute, dass ein guter, digital gestützter Verwaltungsdienst, der einmal genutzt worden sei, Vertrauen schaffe. „Dies sollte der Maßstab für unsere weitere Agenda sein", forderte Klein.

Gerade im kommunalen Bereich geht es jedoch um mehr als digitale Verwaltungsleistungen. Wenn es um nachhaltige und moderne Stadtentwicklung geht, lässt das Buzzword Smart City nicht lange auf sich warten. Dabei seien die beiden Grundsätze bei Weitem nicht gleichbedeutend, so Andreas Ueckert, Senior Expert Smart City bei der Bechtle Systemhaus Holding. Nachhaltige Stadtentwicklung müsse sich an ökologischen, ökonomischen und sozialen Faktoren messen lassen. Smarte Lösungen könnten dabei unterstützen, im Einzelfall müsse jedoch immer abgewogen werden, ob eine konventionelle Lösung den Bedürfnissen der Kommune nicht eher gerecht werde. Der Smart-City-Experte trennt die möglichen Zielsetzungen für Smart-City-Projekte grob in zwei Gruppen auf: Entweder sollen damit bekannte Tätigkeiten effizienter bzw. schneller erledigt werden oder aber vollkommen neue Möglichkeiten geschaffen werden. Der spürbare Nutzen – auch für Bürgerinnen und Bürger – müsse dabei immer im Kern der Planung stehen, erklärt Ueckert. Das steigere die Akzeptanz in der Bevölkerung und biete zudem einen guten Indikator für die Sinnhaftigkeit des Unterfangens. Für die Kommunen bedeuten nachhaltig umgesetzte Smart-City-Projekte, dass die zugrunde liegende Datenbasis nicht nur geschaffen, sondern auch langfristig gepflegt werden muss. Denn, so Ueckert: „Daten liegen nicht auf dem Boden." Man müsse genau eruieren, welche Daten bereits vorlägen. Besonders wichtig dabei ist eine gute Data Governance. Welche Daten werden von welcher Stelle gesammelt? Welche Qualität haben sie? In welcher Struktur müssen Daten hinterlegt werden, um die Bildung einzelner Datensilos zu vermeiden? Nur wenn diese Fragen geklärt sind, kann die Umsetzung smarter Lösungen auch über einen Projektzeitraum hinaus gelingen. Und nicht jede geplante Anwendung ist im ersten Anlauf erfolgreich. So musste die Stadt Freiburg im Breisgau feststellen, dass die gewählten Datenquellen für die Echtzeiterfassung des Fahrradverkehrs nicht von den bereits automatisch erfassten Bewegungsdaten für den Fuß- und Autoverkehr getrennt werden konnten.

Der CIO der nordrhein-westfälischen Landesregierung, Prof. Dr. Andreas Meyer-Falcke, sprach auf dem e-nrw-Kongress.

Foto: BS/van Groen

Abseits des Modells

Aber auch die Finanzierung muss nachhaltig geklärt sein. So berichtete Marcel Böttcher, Chief Digital Officer (CDO) der Stadt Bergisch Gladbach, dass es schwierig sei, Förderungen zu erhalten, wenn in der Region bereits Modell-Kommunen unterstützt würden. Und selbst wenn der Förderantrag bewilligt werde, müssten laufende Kosten für den langfristigen Betrieb von der Kommune finanziert werden.

In Bergisch Gladbach sei es nach zwei erfolglosen Bewerbungen gelungen, auch ohne Fördermittel eine eigene Smart-City-Agenda auf die Beine zu stellen, so Böttcher. Im Think-Tank „Digitale Papierstadt" sollen Vertreterinnen und Vertreter aus unterschiedlichen Teilen der Stadtgesellschaft zusammenkommen und erste Schritte gestalten, um die Stadt smarter zu gestalten. Da die Stadt selbst kein Budget dafür habe, würden Lösungen durch verschiedene Akteure finanziert. Ein eigenes Digital-Budget gibt es in Bergisch Gladbach nur für die OZG-Umsetzung. „Smart City muss immer auch die Lebensrealität verbessern", forderte Böttcher. Besonders in puncto Nachhaltigkeit gehe es hier oft um kleine Dinge. „Dass an einer Bushaltestelle, an der heute kein Bus mehr kommt, das Licht ausgeht, das ist Smart City", so der CDO weiter. In dieser Größenordnung gehe es vielmehr eher darum, kluge Gedanken zusammenzubringen als Finanzierungen zu sichern. Smarte Lösungen müssten nicht immer teuer sein. Eine der großen Herausforderungen für jedes neue Projekt sei es, die richtigen Akteure für die Umsetzung zu gewinnen. Dabei müsse man den Blick auch von der Kommune auf die gesamte Region richten, zum Beispiel wenn es um Akteure im Bereich des Öffentlichen Personennahverkehrs gehe. Böttcher plädierte dafür, in stetigem Austausch zu bleiben, nachzufragen und mit Ideen auch in einem frühen Stadium nach außen zu treten. „Sonst kann es passieren, dass man irgendwann feststellt, dass die anderen genau an derselben Sache arbeiten."

Hochsicher und benutzerfreundlich

Der moderne VS-NfD-Arbeitsplatz

In Behörden werden immer mehr Prozesse und Abläufe ins Digitale verlegt. Dabei müssen jedoch höchste Sicherheitsanforderungen beachtet werden, insbesondere wenn klassifizierte Dokumente und Informationen bearbeitet werden. Der IT-Sicherheitsexperte Rohde & Schwarz Cybersecurity befähigt Bund, Länder und Kommunen mit R&S®Trusted Endpoint Suite, New-Work-Konzepte und digitale Prozesse umzusetzen sowie Arbeitsplätze so abzusichern, dass VS-NfD-eingestufte Informationen einfach gespeichert und bearbeitet werden können. R&S®Trusted Endpoint Suite ist ein softwarebasiertes Sicherheitssystem für mobile und stationäre Microsoft® Windows-Endgeräte und besteht aus einem VPN-Client sowie einer Festplattenvollverschlüsselung. Die innovative Sicherheitslösung erhielt vom Bundesamt für Sicherheit in der Informationstechnik (BSI) die VS-NfD-Zulassung als „Sicherer VS-Arbeitsplatz". Zusätzlichen Schutz bietet optional ein hochsicherer Browser.

R&S®Trusted Endpoint Suite verfolgt einen reinen Softwareansatz, der eine einfache Anbindung von Remote-Nutzern an VS-NfD-eingestufte Netze ermöglicht. Der hochsichere VS-NfD-Arbeitsplatz überzeugt zudem durch intuitive und komfortable Bedienbarkeit sowie flexibler Hardwareauswahl: Benutzer können bereits vorhandene Endgeräte nutzen und es muss gemeinhin keine zusätzliche Hardware angeschafft werden. Darüber hinaus ermöglicht das zentrale und intuitive Managementsystem eine leichte Administration. Nicht zuletzt, da für alle Komponenten der Plattform nur eine Smartcard benötigt wird. Auch die Beibehaltung von Rollout-Prozeduren und Workflows zur Softwareinstallation machen R&S®Trusted Endpoint Suite zu einer einfach administrierbaren, effektiven und sicheren Anwendung für Behörden und Organisationen mit erhöhtem Sicherheitsbedarf.

Zwei Komponenten für umfassenden Schutz

Der VS-NfD-Arbeitsplatz auf Basis von R&S®Trusted Endpoint Suite besteht aus zwei Komponenten auf einer vereinheitlichten Softwarearchitektur: R&S®Trusted VPN Client und R&S®Trusted Disk. R&S®Trusted VPN Client schützt die Netzwerkkommunikation einer Client-Plattform (Windows-Laptop, -Tablet) mit einem Behörden- oder Unternehmensnetzwerk über ein nicht vertrauenswürdiges Netzwerk wie zum Beispiel dem Internet. Für zusätzliche Sicherheit sorgt der „Always On"-Modus. Nutzer befinden sich so zu keinem Zeitpunkt ungeschützt in einem nicht vertrauenswürdigen Netzwerk – egal ob im Büro oder auf Dienstreise im Hotel, Zug oder Flugzeug. R&S®Trusted VPN Client setzt eine Zero-Trust-to-OS-basierte VPN-Lösung um, bei der kein Vertrauen in potenziell unsichere Komponenten wie einem Betriebssystem bestehen muss.

Die Festplattenverschlüsselung R&S®Trusted Disk schützt sensible Daten mit einer sicheren und transparenten Verschlüsselung in Echtzeit ohne Produktivitätseinschränkung sogar im Falle von Verlust oder Diebstahl vor unbefugtem Zugriff. Neben den Daten verschlüsselt R&S®Trusted Disk auch das komplette Betriebssystem und die temporären Daten. Selbst der Zugriff auf mobile Datenträger wie USB-Sticks oder externe Festplatten kann geschützt werden.

Virtueller Browser schickt Angreifer in die Quarantäne

Zusätzlichen Schutz bietet optional die vollvirtualisierte Surfumgebung R&S®Browser in the Box. Der virtuelle Browser erlaubt das Surfen im Internet, ohne dass Angreifer Zugriff auf Behörden- oder Unternehmensnetzwerke erlangen können. R&S®Browser in the Box schließt die Sicherheitslücke „Internet", indem er eine „digitale" Quarantäne für Hackerangriffe ermöglicht. Auf der Rechnerebene erfolgt eine komplette Isolation, sodass Schadsoftware vom restlichen PC des Nutzers ferngehalten wird. Zusätzlich wird auf der Netzwerkebene der Zugang zum Internet vom Intranet getrennt. Das interne Netzwerk (Intranet) ist somit komplett vom Internet getrennt. Dieser Mechanismus schützt auch vor Angriffen via E-Mail-Anhängen oder bei Webkonferenzen mit Mikrofonnutzung und Webcam-Unterstützung. Anstatt – wie bei Antivirenprogrammen – Schadcodes zu erkennen, werden alle potenziell gefährlichen Aktivitäten in diesem virtuellen Browser isoliert. Jeder Browserstart beseitigt die Schädlinge und versetzt den Browser in seinen Ausgangszustand.

Für eine VS-NfD-konforme E-Mail- und Datenverschlüsselung kann R&S®Trusted Endpoint Suite außerdem um GnuPG VS-Desktop® erweitert werden. GnuPG VS-Desktop® ist eine VS-NfD-zugelassene Kryptolösung für die sichere Ende-zu-Ende-Verschlüsselung von Dateien und E-Mails. Sie verhindert das Mitlesen jeglicher verschlüsselten, digitalen Kommunikation und in der Cloud gespeicherter Daten durch Dritte. Selbst wenn verschlüsselte E-Mails auf dem Übertragungsweg abgefangen und gespeichert werden sollten, bleiben diese für nicht autorisierte Personen unmöglich zu entschlüsseln.

R&S®Trusted Endpoint Suite eignet sich ideal für den mobilen und stationären Einsatz in Behörden, Organisationen mit Sicherheitsaufgaben und geheimschutzbetreuten Unternehmen und unterstützt Anwender auf dem Weg in eine sichere und digitalisierte Welt.

Mehr erfahren:

Unverhofft digital kommt nur einmal

Ein Erfahrungsbericht aus der digitalen Modellkommune Soest

⟩⟩⟩ Gastbeitrag von **Jörg Radandt,** CIO der Stadt Soest

Als das Land Nordrhein-Westfalen 2018 das Förderprogramm „Digitale Modellregionen in NRW“ ins Leben rief, traf die Stadt Soest die Wahl als Modellkommune eher unvorbereitet. Die Lernkurve war dementsprechend sehr steil. Doch letztlich waren es die Impulse aus dem Modellprojekt, die dabei halfen, in Soest die Strukturen für den Weg hin zu einer Smart City aufzubauen.

Der Anruf aus Düsseldorf kam Ende 2017, passenderweise kurz vor Weihnachten. Das damalige Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie („MWIDE“) von Minister Andreas Pinkwart beabsichtigte, ab 2018 ein ambitioniertes Förderprogramm ins Leben zu rufen. In fünf Modellregionen – eine in jedem Regierungsbezirk – sollten innovative Projekte in den Bereichen „E-Government“ und „digitale Stadtentwicklung“ entwickelt werden. Soest war hierbei die Rolle als Leitkommune für den Regierungsbezirk Arnsberg zugedacht. Während mit Aachen, Gelsenkirchen, Paderborn und Wuppertal vier große Standorte mit entsprechenden Strukturen ausgewählt wurden, sollte die Modellregion Soest für Südwestfalen stehen: eine ländlich geprägte, aber industriestarke Region mit vielen erfolgreichen und auf dem Weltmarkt aktiven mittelständischen Unternehmen. Neben der Stadt Soest sollten weitere südwestfälische Kommunen beteiligt sein, nämlich Iserlohn, Lippstadt sowie der Kreis Soest.

Hohe Erwartungen

Die Nachricht aus Düsseldorf löste durchaus zwiespältige Gefühle bei den Beteiligten in Soest aus. Einerseits freuten wir uns über das Vertrauen und die Chance, beträchtliche Mittel für digitale Projekte ausgeben zu dürfen. Andererseits gab es von Beginn an hohe Erwartungen von Ministerium und Öffentlichkeit und damit einen entsprechenden Umsetzungsdruck. Soest ist mit knapp 50.000 Einwohnern und etwa 480 Beschäftigten in der Verwaltung die deutlich kleinste der Leitkommunen. Anfang 2018 wurde allein im Bereich E-Government systematisch gearbeitet; für das Handlungsfeld Smart City bestanden allenfalls Vorüberlegungen. Gleichzeitig waren die Erwartungen aus Düsseldorf hoch: Bereits zum Jahresanfang 2018 sollten erste Projektideen entwickelt und der Öffentlichkeit vorgestellt werden. Dies ließ wenig Zeit, in Ruhe geeignete Strukturen aufzubauen.

Schon die interne Verortung des Projektes stellte eine Herausforderung dar. Den Verfasser traf es wohl deshalb, weil er als Fachbereichsleiter den Bereich E-Government verantwortet und damit dem Thema Digitalisierung noch

2018 wurde die Stadt Soest überraschend digitale Modellkommune. Foto: BS/Klaus Päth, pixabay.com

am nächsten stand. Folgerichtig bestand das Projektteam in der Stadtverwaltung Soest zu Anfang auch zuallererst aus Mitarbeitenden aus dem Querschnittsbereich ohne Erfahrungen beispielsweise auf dem Gebiet der Stadtentwicklung.

Um die Zusammenarbeit der beteiligten Kommunen Iserlohn, Lippstadt und Kreis Soest zu koordinieren, wurden zwei Gremien gebildet: einerseits der Steuerkreis mit den jeweiligen Hauptverwaltungsbeamten sowie Vertretern der Bezirksregierung und der Südwestfalenagentur sowie zum Zweiten ein Austauschgremium zu Projektideen und deren Umsetzung.

Jörg Radandt ist Chief Digital Officer und Gesamtverantwortlicher des Projekts Digitale Modellregion der Stadt Soest. Außerdem leitet er den Fachbereich Assistenz und Service.

Foto: BS/privat

Handlungsfelder definiert

Zur weiteren Strukturierung des Prozesses und mangels gemeinsamer Strategie wurden auf Ebene des Steuerkreises zunächst Handlungsfelder definiert, in denen Projekte entwickelt werden sollten. Das E-Government war dabei schon wegen des Auftrages durch das Land gesetzt. Hier war der weitere Projektaufbau dann auch am einfachsten. Die Kommunen in Südwestfalen verfügen mit der Südwestfalen-IT (SIT) über einen zentralen IT-Dienstleister in der Form eines Zweckverbandes. Da lag es nahe, diesen mit ins Boot zu nehmen und gemeinsam über Projektideen rund um das Serviceportal, ein Produkt der SIT, nachzudenken.

Workshops durchgeführt

Für die Definition weiterer Handlungsfelder konnte jede der beteiligten Kommunen ihre Stärken in den Prozess einbringen. Im Ergebnis wurde entschieden, Projekte in den fünf Bereichen Mobilität, Bildung, Gesundheit, attraktive Innenstadt und digitale Infrastruktur zu entwickeln. Dabei war klar, dass dies nur mit kompetenten Partnern in Stadt oder Region funktionieren konnte. Es galt also, solche potenziellen Partner zu finden. Hierfür wurden mithilfe eines externen Dienstleisters Workshops zu jedem Handlungsfeld organisiert, in denen Expertinnen und Experten aus den Kommunen und dem Konzern Stadt mit Fachleuten aus Wissenschaft und sonstigen Institutionen zusammenkamen. Wichtige Ansprechpartner waren zum Beispiel die Fachhochschule Südwestfalen, die Standorte u. a. in Soest und Iserlohn betreibt, die Fachhochschule Hamm-Lippstadt oder das Fraunhofer-Institut IOSB aus dem ostwestfälischen Lemgo.

Viele Projekte umgesetzt

Ziel der Workshops war es jeweils, neben Ideen auch konkrete Projektträger und -beteiligte zu finden und in die praktische Umsetzung zu kommen. Das Ergebnis kann sich sehen lassen: Die Modellregion hat etwa 50 konkrete Projektideen entwickelt. 25 davon wurden letztlich bewilligt und wurden bzw. werden noch umgesetzt. Dazu gehören z. B. – neben den Projekten rund um das Serviceportal – die Einrichtung eines Stadtlabors, die Weiterentwicklung unseres 3-D-Stadtmodells, die Erfassung von Klimadaten im Projekt „BürgerWOLKE“ oder die Entwicklung eines innovativen ÖPNV-Ticketsystems („Big Bird Westfalen“).

Für die Stadt Soest war das Landesprojekt Anstoß für eine Vielzahl grundsätzlicher Entwicklungen.

Zusätzlich Bundesförderung

Ermuntert durch die Erfahrungen aus der „Digitalen Modellregion“ hat sich Soest 2019 mit vier weiteren Kommunen aus Südwestfalen für das „Modellprojekt Smart Cities“ des Bundes beworben und den Zuschlag erhalten. 2021 wurden eine gemeinsame Rahmenstrategie sowie lokale Smart-City- Strategien verabschiedet. Einige schon im Landesprojekt verfolgte Projektansätze wie die einer regionalen Datenplattform oder einer City-App werden hier umgesetzt.

Aus den internen Projektstrukturen ist eine auf Dauer angelegte Organisationsstruktur geworden. Auf Ebene der Politik wurden nach der Kommunalwahl 2020 ein eigener „Ausschuss für Innovation und digitalen Wandel“ und innerhalb der Verwaltung eine neue Abteilung mit gleichlautendem Namen inklusive einem zentralen Datenmanagement gebildet. Das fachübergreifende Projektteam wurde als „Team Soest Digital“ etabliert. Der Verfasser schließlich koordiniert die digitalen Aktivitäten der Stadt nunmehr als „Chief Digital Officer“ (CDO).

Die im Rahmen der „Digitalen Modellregion“ entstandenen Kontakte und Netzwerke werden sicherlich noch weit über die Laufzeit des Landesprojektes, das 2023 offiziell endet, tragen. Insgesamt sehen wir uns damit gut aufgestellt, um Soest zu einer Smart City zu machen.

// SAVE THE DATE

Die Vorbereitungen für den nächten Kongress e-nrw laufen bereits. Das Event findet am 31. Oktober in Neuss statt.

Impressum

Herausgeberin: Dr. Eva-Charlotte Proll

Redaktionelle Leitung: Malin Jacobson
Redaktion: Jonas Brandstetter, Marco Feldmann, Jörn Fieseler, Guido Gehrt, Benjamin Hilbricht, Tanja Klement, Matthias Lorenz, Tim Rotthaus, Paul Schubert
Layout: Maximilian Spuling, SpreeService- und Beratungsgesellschaft mbH

Das Jahrbuch wird verlegt von der ProPress Verlagsgesellschaft mbH (Behörden Spiegel-Gruppe),
Büro Bonn:
Friedrich-Ebert-Allee 57, 53113 Bonn
Telefon: +49(228)97097-0
Büro Berlin:
Kaskelstraße 41, 10317 Berlin
Telefon: +49(30)557412-0
E-Mail: redaktion@behoerdenspiegel.de
Internet: www.behoerdenspiegel.de
Geschäftsführer: Dr. Fabian Rusch
Druck: Köllen Druck+Verlag GmbH

Erfüllungsort und Gerichtsstand: Bonn

Namentlich gekennzeichnete Beiträge geben nicht unbedingt die Meinung der Redaktion wieder. Alle Rechte vorbehalten. Das Buch und alle in ihm enthaltenen Beiträge und Abbildungen (auch Werbeeinschaltungen) sind urheberrechtlich geschützt. Mit Ausnahme der gesetzlich zugelassenen Fälle ist eine Verwertung ohne Einwilligung des Verlages nicht statthaft und wird urheberrechtlich verfolgt.

ISBN 978-3-934401-72-3
© 2023 ProPress Verlagsgesellschaft mbH (Behörden Spiegel-Gruppe)

Digitale Verwaltung

Top-Events 2023

8. März

HEssenDIGITAL

Bad Homburg
www.hedigital.de

25.–26. April

DIGITALER STAAT

Berlin
www.digitaler-staat.org

28. Juni

IT-Sicherheitstag Sachsen

Dresden
www.sicherheitstag-sachsen.de

29. Juni

BADEN-WÜRTTEMBERG 4.0

Stuttgart
www.bw-4-0.de

21.–22. September

PITS
Public-IT-Security

Berlin
www.public-it-security.de

12. Oktober

NORDL@NDERDIGITAL

Bremen
www.nordlaender-digital.de

31. Oktober

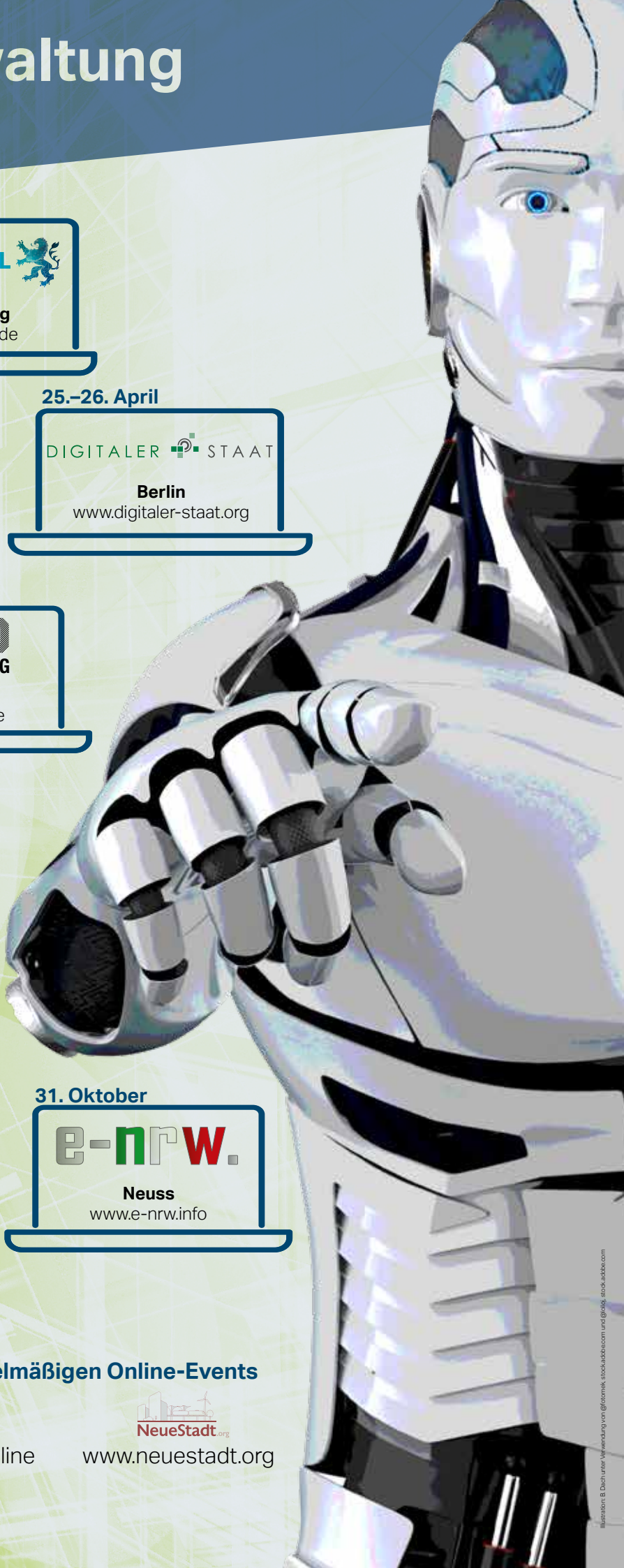
e-nrw.

Neuss
www.e-nrw.info

27. November

Digitale Verwaltung Rheinland-Pfalz 2023

Mainz
www.dv-rlp.de



Plattformen mit regelmäßigen Online-Events

DIGITALER STAAT ONLINE
www.digitaler-staat.online

NeueStadt.org
www.neuestadt.org

Behörden Spiegel

Illustration: B. Dach unter Verwendung von @fotomek, stockadobe.com und @vlds, stockadobe.com

LizenzDirekt
SOFTWARE FOR YOUR BUSINESS

NEUE PERSPEKTIVE.

GRÜN GEHT EINFACH. MIT GEBRAUCHTEN SOFTWARE-LIZENZEN.

Aktuell, nachhaltig und digital souverän.

Gebrauchte Software-Lizenzen sind Ihr Beitrag zum Digital Green Deal. Bringen Sie Nachhaltigkeit in Ihre IT und sparen dabei auch noch bis zu 70 Prozent*.

lizenzdirekt.com

Digital Green Deal. Jetzt.

#digitalgreendeal

* Maximal mögliche Ersparnis durch Kauf eines Gebraucht-Produktes von LIZENZDIREKT (im Vergleich zum vom Hersteller empfohlenen Neuverkaufspreis).