

Hessische Zentrale für Datenverarbeitung

HESSEN

INFORM

Magazin für die hessische Landesverwaltung



Auf dem Weg zu Wolke 7

Die Cloud-Strategie der HZD

| ab Seite 16

Auf Nummer sicher

Der HessenPC 4.0

| ab Seite 34

#stayaware Awareness-Kampagne

Der Mensch als Schlüsselement

für Informationssicherheit | ab Seite 40

HZD

Über

60

Ministerien, Landesbetriebe und nachgeordnete Dienststellen nutzen aktuell HessenDrive.

Die Datenaustausch-Plattform aus der Cloud kommt immer dann zum Einsatz, wenn ein schneller, unkomplizierter und vor allem sicherer Datenaustausch (Schutzbedarf hoch) benötigt wird. Auch größere Datenvolumina können problemlos übertragen werden – ganz egal, ob landesweit oder mit Organisationen, Unternehmen und Personen außerhalb der Landesverwaltung.

In diesem Jahr bekommt HessenDrive ein neues Gewand mit vielen Verbesserungen und neuen Features.

Wir halten Sie auf dem Laufenden.

Produktinformationsseite für Landesbeschäftigte:

<https://moss.intern.hessen.de/its/Produktinformationen-HessenDrive/>

Kontakt:

hessendrive@hzd.hessen.de

Liebe Leserin, lieber Leser,

als Full-Service-Provider des Landes muss sich die HZD konsequent in Richtung Cloud-Anbieter entwickeln. Das ist für uns die wichtigste strategische Frage und Aufgabe der nächsten Jahre, die ich gemeinsam mit Thomas Kaspar zur Chefsache erklärt habe. Zum einen entsprechen wir damit Ihren Erwartungen und dem gestiegenen Anspruch an digitale Liefergegenstände, zum anderen aber auch der Notwendigkeit, den gestiegenen Anforderungen an den Betrieb von IT-Systemen und der flexiblen Bereitstellung von Services Rechnung zu tragen.

Die HZD wird ihre Rechenzentren sukzessive um ein attraktives Private-Cloud-Angebot erweitern, das offene Standards unterstützt, eine Einbindung in Community-Clouds wie die föderale Verwaltung-cloud des IT-Planungsrats ermöglicht und auch hybride Cloud-Lösungen nicht ausschließt. Um dies zu erreichen, müssen wir gezielt Beratungskompetenz aufbauen, agile Projekte durchführen und vor allem für die bestehenden Systeme und neuen Anforderungen das jeweils passende Cloud-Angebot finden – sicher, datenschutzkonform und klimaneutral.

In dem Cloud-Ökosystem, das wir schaffen wollen, spielen Innovation, Schnelligkeit und Agilität eine entscheidende Rolle. Die Cloud-Transformation umfasst also Infrastruktur und Organisation. Im Themenschwerpunkt dieser Ausgabe zeigen wir Ihnen, wie unser Weg zu „Wolke 7“ aussieht.



Zurück am Boden: Ralf Stettner, Abteilungsleiter VII im Innenministerium, leitet einen Sonderstab, der die IT-Ausstattung der Impfzentren in Hessen verantwortet. Die HZD unterstützt dabei. Im INFORM-Interview spricht er über die Komplexität der Aufgabe, notwendige Kompetenzen und über Krisen. Ferner finden Sie in dieser Ausgabe: Auf Nummer sicher gehen mit dem HessenPC 4.0, Awareness für die IT-Sicherheit schaffen und neue Features der FISBOX®.

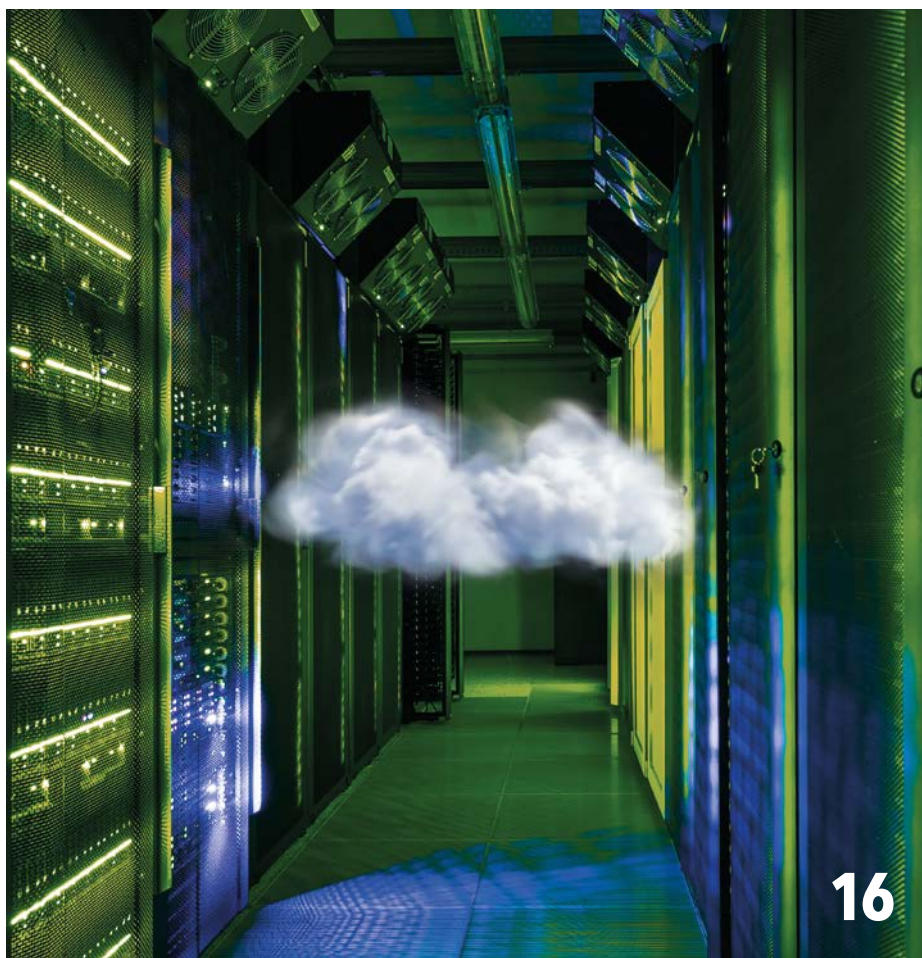
Bleiben Sie zuversichtlich.

Ihr

Joachim Kaiser

Direktor der HZD

Inhalt



Ständige Rubriken

- 8 Notizen**
- 10 Impressum**
- 11 Kommentar**
Kristina Sinemus über ... die Fortschreibung der Digitalstrategie Hessen

Interview

- 12 Ralf Stettner**
Leiter Abteilung VII im Hessischen Innenministerium, CISO und Leiter des Sonderstabs ImpfVII

16 Themenschwerpunkt: Die Cloud-Strategie der HZD

IT-Services, die den klassischen Behördengang weitestgehend ersetzen, sind von Bürgerinnen und Bürgern gefragt, von Gesetzes wegen und auf strategischer Seite gefordert. Die Nutzung von modularen, skalierbaren, hochverfügbaren Cloud-Services ist eine Lösung dafür. Die HZD wird deshalb in den nächsten Jahren ihr Cloud-Angebot ausbauen.

20 Verfahrenscloud Hessen – auf dem Weg zur Multi-Cloud

23 Die Deutsche Verwaltungscloud-Strategie nimmt Form an

24 Containerhafen für die HZD

26 Technische Digitalisierungsplattform – Microservices für die digitale Transformation

28 Continuous Integration und Continuous Delivery am Beispiel von e²P und dem Wohngeldverfahren



Magazin

34 Auf Nummer sicher - der HessenPC 4.0

Der HessenPC wird noch sicherer: Mit der neuen Version wird eine deutliche Erhöhung des Sicherheitsniveaus unter Berücksichtigung der Usability erreicht.

38 Länderübergreifender Support für die Justiz

Seit Beginn des Jahres verantwortet die HZD das zentrale Betriebsmanagement im gesamtdeutschen Mammutprojekt Elektronischer Rechtsverkehr.

40 Der Mensch als Schlüsselement für Informationssicherheit

Die HZD startet unter dem Motto #stayaware eine umfassende interne Security Awareness-Kampagne.

44 FISBOX® mit neuen Features

Die FISBOX® hat ein neues Ass im Ärmel: die digitale Antragsüberführung entsprechend den Vorgaben des Onlinezugangsgesetzes und der Digitalen Modellbehörde. Bewährt hat sie sich u.a. in einer neuen Anwendung für das Sozialministerium.

46 Blacklisting bei Massen-E-Mails vermeiden

INFORM erläutert die gängigsten Blacklists privater Provider und gibt Empfehlungen, wie man ein Blacklisting für E-Mails des Landes vermeiden kann.

Ständige Rubriken

33 Web-Lounge

Und nun: das Wetter!

47 Awareness

Jackpot!

48 Tipp

Souverän mit der Statusanzeige in Hessen-Connect umgehen

50 Serie

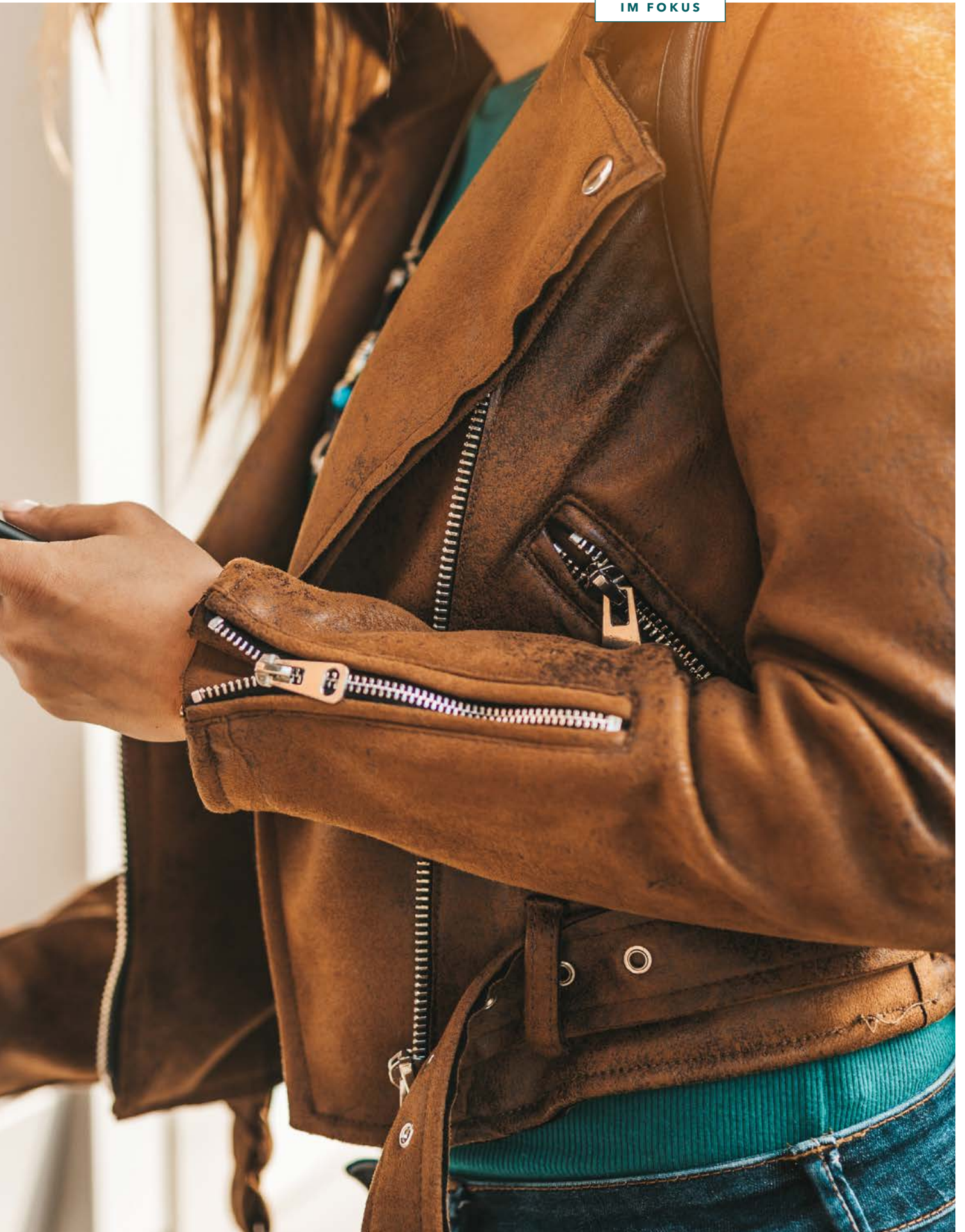
Wie digital leben wir? Digitalisierung im sozialen Umfeld

51 Vorschau INFORM 3/21



Achtsam im (digitalen) Alltag

Es gibt viele Situationen, in denen wir bewusst oder unbewusst achtsam sind. Sei es, dass wir an einer roten Ampel stehen bleiben und warten, bis sie auf grün schaltet, bevor wir weiterfahren. Sei es am Bankautomaten, wo wir darauf achten, dass keiner unsere PIN sieht – oder eben auch nicht, wie dieses Bild zeigt. In aller Regel passen wir auf, weil wir es so gelernt haben. In der digitalen Welt sind wir oft weniger vorsichtig. Die HZD hat deshalb im Rahmen einer ISO-Zertifizierung eine umfassende Awareness-Kampagne für ihre Beschäftigten gestartet. Das Motto: #stayaware. | ab Seite 40





An einem frühsommerlichen Tag spiegeln sich die Wolken in der Fassade des HZD-Neubaus. Es scheint, als ob der Himmel und die HZD miteinander verschmelzen. Während draußen die Wolken vorbeiziehen, beschäftigt sich die HZD drinnen mit dem Thema Cloud. Ob Private, Public, Hybrid oder Multi-Cloud – ähnlich wie bei ihren Namensvettern Cumulus oder Nimbostratus gibt es viele Erscheinungsformen.

Im Wandel der Zeit



50 Jahre in der Computertechnik sind in Bezug auf den technischen Fortschritt und die Weiterentwicklung eher mit einem ganzen Zeital-

ter in der Menschheitsgeschichte zu vergleichen. Das bildet sich auch eindrucksvoll in der Geschichte der HZD und in der nun vorliegenden Chronik zu 50 Jahre HZD Wiesbaden und 30 Jahre HZD Hünfeld ab. Neben der Aufarbeitung der Geschichte geben Zeitzeugnisse, Schlagzeilen und Anekdoten sowie die vielen Abbildungen ein lebendiges Bild des Wandels und der Wandelbarkeit der HZD.

➔ Werfen Sie einen Blick in die Geschichte der HZD:
<https://hzd.hessen.de/chronik>

HZD übernimmt Anwendungsmanagement für HLA

Die HZD hat das Verfahren „Digitales Magazin“ des Hessischen Landesarchivs (HLA) erfolgreich ins Rechenzentrum der HZD migriert. Im Zuge dessen wird auch das Anwendungsmanagement in der HZD aufgebaut. Das HLA hat angekündigt, noch innerhalb des Jahres 2021 ein zweites Verfahren (Arcinsys – Archivinformationssystem) in die HZD migrieren zu wollen.



Engagement für Diversität

Vielfalt am Arbeitsplatz gehört schon seit langem zum Selbstverständnis der HZD. Am Diversity Tag 2021 hat sie auch nach außen Flagge gezeigt und mit der Unterzeichnung der „Charta für Vielfalt“ ein deutliches Signal für ein buntes und gleichberechtigtes Miteinander im Berufsalltag gesetzt.



SAP-Rezertifizierung: wieder volle Punktzahl!

Das achte Mal in Folge haben das Hessische Competence Center (HCC) und die HZD Anfang April 2021 das SAP-Zertifikat „Customer Center of Expertise“ (CCoE) für das Land Hessen erhalten. Das vierte Mal in Folge mit voller Punktzahl.

SAP verleiht das Zertifikat an teilnehmende Organisationen und Unternehmen, die den Qualitätskriterien im Hinblick auf Betrieb, Support und Weiterentwicklung entsprechen. Die Rezertifizierung findet alle zwei Jahre statt.

Während das HCC fachlich für die zentralen SAP-Systeme des Landes Hessen zuständig ist, ist das T-HCC der HZD für den technischen Betrieb verantwortlich. Das Land Hessen setzt SAP zentral vor allem im Personal- und Finanzwesen ein.



Nicola Wolffgardt - neue Leiterin der Abteilung Produkte



Seit dem 6. April leitet Nicola Wolffgardt die HZD-Abteilung Produkte. Sie tritt damit die Nachfolge von Manfred Pospich an. Zu ihrem Verantwortungsbereich zählen zentrale HZD-Produkte wie der HessenPC, das Dokumentenmanagementsystem (DMS), Portale oder SAP (T-HCC). Die 50-Jährige verfügt über mehr als 18 Jahre Erfahrung im IT Service- und Produktmanagement als Full IT-Service-Provider für ein großes globales Unternehmen, wo sie zuletzt Abteilungsleiterin für „Business Solutions Finance and Data Warehouse“ war.

OASIS bleibt in hessischer Obhut

Die Zuständigkeit für das Spielersperrsystem OASIS verbleibt dauerhaft in Hessen und geht nicht auf die geplante gemeinsame Glücksspielbehörde in Halle über. Dies haben die Chefinnen und Chefs der Staats- und Senatskanzleien in ihrer Sitzung im Februar 2021 beschlossen. Das von der HZD betriebene und auch entwickelte Spielersperrsystem OASIS ist seit 2013 bundesweit in Spielbanken, Lotteriegesellschaften und bei Sport- bzw. Pferdewettanbietern sowie seit Mitte 2014 in hessischen Spielhallen im Einsatz. Anfang 2021 schlossen sich auch die rheinland-pfälzischen Spielhallen an OASIS an. Es schützt suchtgefährdete Spielerinnen und Spieler.

Aktuell wird die Anwendung auf Basis des neuen Glücksspielstaatsvertrags 2021, der am 1. Juli 2021 in Kraft treten soll, umgestellt. Demnach müssen ab Mitte des Jahres alle bundesweiten Veranstalter von Glücksspielen, auch Gaststätten mit Glücksspielautomaten sowie Online-Sportwetten und Online-Casinos, bei OASIS abfragen, ob die spielwillige Person gesperrt ist, bevor sie ggf. zum Spiel zugelassen wird.

Digitale Städte - Digitale Regionen

Der Kongress „Digitale Städte - Digitale Regionen“ ist die Leitveranstaltung des Landes Hessen für die Digitalisierung in Kommunen und Regionen. Vertreter*innen aus Politik und Verwaltung, Wirtschaft, Wissenschaft und Gesellschaft bietet er ein Forum, um sich über „Smart City“- und „Smart Region“-Themen passgenau zu informieren und zu vernetzen.

Treffpunkt der Smart City-Community ist in diesem Jahr am 08.09.2021

➔ Weitere Informationen: <https://www.smart-region-hessen.de/kongress/>



Barrierefrei - von der Corona-Warn App über hessenWarn bis hin zur Feuerwehr

Ab dem 23. Juni 2021 sind alle öffentlichen Stellen in Bund, Ländern und Kommunen verpflichtet, ihre mobilen Anwendungen (Apps) barrierefrei zu gestalten. Vorgeschrieben war dies bisher nur für die Webseiten öffentlicher Stellen. Jetzt gilt das auch für alle Apps. Zusätzlich sind die öffentlichen Stellen dazu verpflichtet, eine Erklärung zur Barrierefreiheit in ihrer mobilen Anwendung zur Verfügung zu stellen. Eine Vorlage hierzu ist im Landeskompetenzzentrum barrierefreie IT in der Durchsetzungs- und Überwachungsstelle mit Sitz im Regierungspräsidium Gießen erhältlich.

Rechtliche Grundlage dieser Regelungen ist die EU-Richtlinie für die Umsetzung digitaler Barrierefreiheit (EU) 2016/2102. „Alle Menschen, unabhängig ihrer Einschränkungen wie etwa eine Seh- oder Hörbeeinträchtigung oder ihrer technischen Möglichkeiten, aber auch ältere Menschen, Technik-Laien und ab Juni dieses Jahres auch die Anwenderinnen und Anwender mobiler Endgeräte profitieren von der barrierefreien IT und den neuen Regelungen“, betont die Landesbeauf-

tragte für barrierefreie IT, Professor Dr. Meyer zu Bexten. Gemäß der EU-Richtlinie ist das Land verpflichtet, Webseiten und Dokumente von öffentlichen Stellen zu überprüfen. Für die regelmäßige Überprüfung ist die Durchsetzungs- und Überwachungsstelle des Landes Hessen zuständig.

Zu den verpflichteten öffentlichen Stellen in Bund und Ländern gehören Ministerien, Sozialversicherungsträger oder Bürgerämter, aber auch Einrichtungen der Daseinsvorsorge wie kommunale Nahverkehrsunternehmen oder die Feuerwehren zählen dazu.

Was aber heißt das konkret? Wenn etwas in einer mobilen Anwendung oder einem Webauftreten nicht barrierefrei nutzbar ist, muss in der Erklärung zur Barrierefreiheit dargelegt werden, welche wichtigen Gründe es dafür gibt und ob alternative Zugänge zu den Inhalten angeboten werden.

➔ Fragen beantwortet Ihnen das Landeskompetenzzentrum für barrierefreie IT in der Durchsetzungs- und Überwachungsstelle: LBIT@rpgi.hessen.de

INFORM

erscheint viermal jährlich (48. Jahrgang)

Herausgeber

Hessische Zentrale für Datenverarbeitung
Mainzer Straße 29, 65185 Wiesbaden
Telefon: 0611 340-0
pressestelle@hzd.hessen.de, www.hzd.hessen.de

Chefredaktion

Birgit Lehr

Redaktion

Birgit Lehr, Simone Schütz

Fachbeirat

Dr. Markus Beckmann, Markus Brückner, Janina Einsele, Dr. Bernhard Fussel, Markus Kantowski, Horst Kiehl, Susanne Mehl, Dr. Klaus-Dieter Niebling, Sabine Spang, Tülün Syha, Martin Swiderek, Kristof Uhlig, Anna-Lena Wiegand

Grafisches Konzept

Agentur 42 oHG | Konzept & Design
www.agentur42.de

Druck

AC medienhaus GmbH,
www.acmedienhaus.de

Hinweis: Bei der Gestaltung des Cloud-Themenswerpunkts haben wir uns von dem niederländischen Künstler Berndnaud Smilde inspirieren lassen.

Fotos

©Parrish Fremann-unsplash, Titel; ©Tomasz Woziak stock.adobe.com, comicsans stock.adobe.com, S. 4, S. 16-17, Collage: Agentur42; ©Alex stock.adobe.com, S. 5, S. 34; engel.ac stock.adobe.com, S. 5, S. 40, S. 42-43; beatrice préve Fotolia, S. 5; ©hedgehog94 stock.adobe.com, S. 6-7; ©Ilona Baha Fotolia, S. 9; ©Brett Jordan unsplash, S. 10; ©Ingo Boddenberg, comicsans stock.adobe.com, Collage: Agentur42, S. 19, S. 27, S. 29; ©AndSus stock.adobe.com, S. 36-37; ©everythingpossible stock.adobe.com, S. 39; ©Sashkin stock.adobe.com, S. 45; © Alle Fotos privat S. 50; Alle anderen © HZD

Grafiken

© Agentur 42 oHG: S. 9, S. 11, S. 23, S. 25, S. 28, S. 30, S. 32, S. 40, S. 42-43, S. 45, S. 51

Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Nachdruck, auch auszugsweise, nur mit schriftlicher Genehmigung der HZD.

Sie möchten zum Thema IT im Land auf dem Laufenden bleiben? Dann besuchen Sie uns online oder abonnieren unseren Newsletter INFORM|DIREKT unter www.hzd.hessen.de. Wenn Sie die INFORM regelmäßig erhalten möchten, schreiben Sie uns: informaerial@hzd.hessen.de oder rufen Sie uns an: Tel. 0611 340-3118

Gender-Hinweis

Die Vermeidung von Diskriminierung ist ein erklärtes Ziel der hessischen Landesverwaltung. Die Nennung aller Geschlechter drückt die Gleichbehandlung aller hessischen Beschäftigten als demokratisches Prinzip aus und zeigt Wertschätzung gegenüber allen Menschen – unabhängig ihres Geschlechts. Die sprachliche Gleichbehandlung ist für eine erfolgreiche Gleichstellung daher unerlässlich.

Noch gibt es keine bindenden sprachlichen Regelungen bezüglich der dritten Option bzw. geschlechtlicher Vielfalt. Die INFORM-Redaktion hat deshalb entschieden, je nach Kontext verschiedene sprachliche Ausdrucksformen anzuwenden. Wird die verkürzte Sprachform verwendet, hat dies nur redaktionelle Gründe und beinhaltet keine Wertung.





Kristina Sinemus über ... **die Fortschreibung der Digitalstrategie Hessen**

Professor Kristina Sinemus,
Staatsministerin für Digitale Strategie und Entwicklung

Wie wird unser Leben 2030 aussehen? Das kann niemand mit Sicherheit voraussagen. Aber klar ist, dass unser Leben deutlich digitaler sein wird als heute. Um die zunehmende Digitalisierung in allen Lebensbereichen zu gestalten und teilweise auch deutlich voranzutreiben und zu beschleunigen, will die Hessische Landesregierung mit der Fortschreibung der 2016 erstellten Digitalstrategie Hessen die Potenziale aktiv heben, die mit dem digitalen Wandel verbunden sind. Mit der Schaffung eines eigenen Bereichs für Digitale Strategie und Entwicklung und der gebündelten Steuerung der Digitalpolitik des Landes Hessen wurde eine wichtige Basis für ein konzertiertes Vorgehen und ein Forcieren der Digitalisierung – über Ressortgrenzen und Handlungsfelder hinweg – geschaffen. Die Strategiefortschreibung mit einem zeitlichen Horizont bis 2030 ist ebenso übergreifend angelegt – mit zwei Grundlagen: die Schaffung einer leistungsfähigen, flächendeckenden digitalen Infrastruktur sowie digitale Spielregeln für ein sicheres und faires Miteinander in der virtuellen Welt.

Grundlage aller Überlegungen ist der Nutzen für die Bürgerinnen und Bürger. Die Technik muss dem Menschen dienen und nicht umgekehrt. Ebenso wollen wir die Digitalisierung für alle Menschen und nicht nur für die besonders agilen und technologisch versierten zu einem Erfolg führen. Daher sind in der Strategie auch sechs zentrale Handlungsfelder definiert worden, in denen Digitalisierung gelingen muss.

Digitale Innovation: Wissenschaft und Forschung mit Verantwortung;

Wirtschaft und Arbeit 4.0: mit digitaler Transformation erfolgreich und leistungsstark;

Digitale Bildung: Kompetenzen stärken, Neues entdecken;

Digitale Gesellschaft: Gesundheit fördern, Teilhabe ermöglichen, Kultur öffnen;

Smarte Region: intelligente Lösungen für Stadt und Land;

Digitale Verwaltung: bürgernah, kundenfreundlich und sicher.

Bei allen tollen Möglichkeiten, die neue Technologien bieten, ist es wichtig, dass auch die Sorgen und Vorbehalte, die durch Risiken, Fehlentwicklungen oder Überforderung auftreten können, wahr- und ernstgenommen werden. Deshalb braucht es eine verantwortungsbewusste Digitalisierung, mit dazu passenden Kenntnissen und Fertigkeiten, Zugang zu Geräten und Internet sowie Regeln und Leitplanken, von unausgesprochenen Vereinbarungen bis hin zu bindenden Gesetzen.

Die Zukunft der Digitalisierung wird einen erheblichen Einfluss auf unser Leben entfalten und birgt dabei enorme Potenziale für Erfolg, Lebensqualität und Zusammenhalt in Hessen. Politik muss sich dieser bedeutsamen Herausforderung der Gegenwart verantwortlich stellen. Mit der Fortschreibung der Strategie „Digitales Hessen – Wo Zukunft zuhause ist“ wollen wir daher schon heute die Potenziale von morgen im Blick haben und die Weichen für diese stellen.



➔ Die komplette Digitalstrategie zum Nachlesen gibt es unter www.digitale-zukunft-hessen.de



„Wir arbeiten direkt unter dem Brennglas der Öffentlichkeit“

Interview mit Ralf Stettner, Hessisches Innenministerium, Leiter Abteilung VII (Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung), CISO (zentraler Informationssicherheitsbeauftragter der hessischen Landesverwaltung) und Leiter Sonderstab ImpfVII

Im November wurde von der Politik eine weitere Mammutaufgabe zur Bewältigung der Corona-Pandemie beschlossen: Innerhalb von nur wenigen Wochen sollten alle Bundesländer Impfzentren für Corona-Massenimpfungen aufbauen. Für ganz Deutschland ist das ein Hoffnungsschimmer. Für Hessen ist es die größte Impfkation in der Geschichte. Damit betraut sind das Sozial- und Innenministerium. Ralf Stettner leitet den Sonderstab ImpfVII und ist verantwortlich für die IT-Ausstattung der 28 Impfzentren in Hessen. INFORM sprach mit ihm über die Komplexität der Aufgabe, notwendige Kompetenzen und über Krisen.

INFORM: Herr Stettner, 2016 standen Sie INFORM schon einmal für ein Interview zur Verfügung. Damals haben Sie die Leitung der Hessischen Erstaufnahmeeinrichtungen für Flüchtlinge übernommen. Jetzt leiten Sie einen Sonderstab, der die gesamte IT in den 28 Impfzentren sicherstellt. Sind Sie der Mann für die Bewältigung akuter Krisen?

Stettner: Das weiß ich nicht. Aber zumindest ist es ganz gut, eine Kompetenz in Krisenorganisation zu haben. Stäbe sind aus dem Nichts sofort aufzubauen. Wir brauchen ad hoc die richtigen Personen, die bestimmte Stabsstrukturen wie Logistik, IT, Sicherheit, Organisation

und Presse abdecken können. Das Team muss als Ganzes funktionieren. Und jemand muss diese Personen, mit Motivation und vielleicht auch als Vorbild, führen können und wollen, sodass sie in der Lage sind, in kurzer Zeit schnelle und umsetzungsfähige Entscheidungen zu treffen, anders zu handeln als in normalem Verwaltungshandeln. Das ist von großer Bedeutung. Und genau da, glaube ich, kann ich mich und meine Kompetenz einbringen. Ich habe das einmal im großen Stil gemacht, das war 2015/2016 bei den Erstaufnahmeeinrichtungen - grundsätzlich ist es fast egal, um welche Krise es sich handelt.



Ralf Stettner - kurz und knapp

Mein Berufswunsch als Kind war ... weiß ich nicht mehr. Ich würde sagen Ritter.

Ich habe Geschichte studiert, weil ... ich glaube, dass man das Jetzige und Zukünftige besser beurteilen kann, wenn man weiß, was das Frühere war.

Ich bin schließlich Leiter der Abteilung Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung im Innenministerium geworden, weil ... ich hier aufbauen und gestalten sowie meinen Beitrag dazu leisten kann, Demokratie und Freiheit zu verteidigen.

Ein absolut unverzichtbares „Arbeitsgerät“ für mich ... ist die Frankfurter Allgemeine Zeitung, die analoge Ausgabe.

Um mal auf ganz andere Gedanken zu kommen, ... gehe ich wandern, am liebsten im Wald oder auf Bergen.

Mein Lieblingsbuch ist ... „Ich nicht“ von Joachim Fest.

Ich hätte gerne mehr Zeit für ... Familie, Großfamilie und Freunde.

INFORM: *Wie erging es Ihnen in den letzten Monaten?*

Stettner: November bis Mitte Februar waren hart. Wir haben Weihnachten durchgearbeitet, die einzige Ausnahme war an Heiligabend.

INFORM: *Was treibt Sie an?*

Stettner: Gestalten, Aufbauen, Führen. Die Handlungsfähigkeit des Staates und damit Demokratie und Freiheit erhalten.

INFORM: *Haben Sie sofort ja gesagt, als Innenminister Beuth Sie fragte, ob Sie den Sonderstab ImpfvII leiten würden?*

Stettner: Sonderstäbe sind dafür da, aus einer Notlage heraus der Bevölkerung, dem Staat und dem Land zu dienen. Deshalb war es für mich keine Frage, dass ich mich wieder zur Verfügung stelle.

INFORM: *Was ist die genaue Aufgabe des Sonderstabs ImpfvII?*

Stettner: Der Sonderstab hat die Aufgabe, die gesamte IT in den 28 Impfzentren in Hessen sicherzustellen. Zunächst ging es darum, Hardware zu beschaffen und Software auszuwählen, zu testen und aufzuspielen, aber auch die IT-Chefs der 28 Impfzentren „anzudocken“. Das war schon durchaus komplex und die Marktlage der IT zudem schwierig.

Daneben gilt es, zu kommunizieren und zu koordinieren, was wir überhaupt tun. Bürgerinnen und Bürger sind unmittelbar betroffen, sie wollen geimpft werden und sind sehr

sensibel – somit ist die ganze Gesellschaft sehr sensibel. Wir arbeiten direkt unter dem Brennglas der Öffentlichkeit. Das ist ein ganz großer Unterschied und eine neue Herausforderung im Gegensatz zur Leitung der Erstaufnahmeeinrichtungen oder der von mir ebenfalls geführten Taskforce Beschaffung und Verteilung Persönlicher Schutzausrüstung.

INFORM: *Die Vereinbarung von Impfterminen und die Impfkoordination werden heute in der Hauptsache digital abgewickelt. Als am 12. Januar die ersten Impftermine telefonisch und online vereinbart werden konnten, lief nicht alles auf Anhieb glatt. Ein Thema, das die Presse breitgetreten hat. Wie komplex sind der Aufbau und der reibungslose Ablauf der Impfzentren aus IT-Sicht?*

Stettner: Aus IT-Sicht war es eine große Herausforderung, die richtige Software zu beschaffen. Diese muss in der Lage sein, jeden einzelnen Schritt im gesamten Ablauf der Impfzentren abzubilden. Hier geht es beispielsweise um die Aufnahme, das Anamnesegespräch, die Auswahl und Verfüllung des Impfstoffs, die Impfung selbst und natürlich die Dokumentation des Ganzen. Aufgrund der Verarbeitung von Gesundheitsdaten ergeben sich hohe Anforderungen an die IT-Sicherheit und den Datenschutz. Zusätzlich kommt eine Software für die Impfterminvergabe zum Einsatz. Bei der Terminvergabe gibt es viele Parameter in Bezug auf den Termin und den Ort der Impfung, aber auch die zu impfenden Personen wie Alter, Vorerkrankung, Sondergruppen. Das di-

gitale Prozedere und der analoge Ablauf müssen zusammengehen. 6,3 Millionen mögliche Impfungen in 28 Impfzentren in Hessen sind betroffen.

INFORM: *Wer sitzt mit Ihnen im Boot?*

Stettner: Es sind viele Akteure beteiligt. An erster Stelle die beiden verantwortlichen Ministerien, also Sozial- und Innenministerium, mit der übergeordneten Taskforce Impfkoordination und meinem Sonderstab ImpfvII, und natürlich die 28 Impfzentren, die von den Landkreisen und kreisfreien Städten betrieben werden. Weiterhin sind der Hessische Datenschutzbeauftragte und die Landesbeauftragte für barrierefreie IT eng eingebunden.

Ganz wichtig aus IT-Sicht sind unsere technischen Partner, die HZD und die ekom21, sowie die beiden Firmen, die uns die Software zur Verfügung stellen. Bei allen Reibungen, die es in einer Krisenlage gibt, ist das ein sehr gutes und enges Miteinander. Alle wissen, dass es eine wichtige gemeinsame Aufgabe ist, bei der es gilt, seine Rolle zu erfüllen.

INFORM: *Die HZD hat eine eigene Taskforce unter der Leitung des Technischen Direktors Thomas Kaspar aufgestellt. Ihr primäres Anliegen ist es, schnell und professionell auf die Anforderungen der Impfzentren reagieren zu können und bei Hardware, Software, dem sicheren Betrieb sowie beim Personal zu beraten und zu unterstützen. Inwiefern trägt das Know-how der HZD zum Gelingen der Mammutaufgabe bei?*



Eines von 28 Impfzentren in Hessen, hier in der Landeshauptstadt Wiesbaden

Stettner: Da kann ich gleich mehrere Punkte nennen. Zum einen die Landing Page der HZD, die zur Seite mit der Impfterminvergabe weiterleitet. Diese muss permanent hochperformant sein, häufig aktualisiert und nachgesteuert werden. Der zweite wirklich wichtige Punkt ist, dass die HZD meinen Sonderstab ImpfvII beratend und personell unterstützt, nämlich mit fünf Spezialisten in verschiedenen Aufgaben und das jetzt seit Monaten. Auf Leitungsebene, mit Herrn Dr. Ornik, der bei der HZD die operative Leitung der Taskforce übernommen hat, und mit der HZD-Hausspitze, Herrn Kaiser und Herrn Kaspar, pflege ich eine sehr gute Zusammenarbeit und schnelle Lösungsfindung, wenn es mal hakt.

INFORM: *Am 19. Januar öffneten die ersten sechs Impfzentren, Anfang Februar waren alle 28 in Hessen startklar. Wie bewerten Sie die aktuelle IT-Lage in den Impfzentren?*

Stettner: Gut. Die Impfzentren arbeiten mit unserer IT-Ausstattung, daneben haben sie eigene Hard- und Software für die Anbindung ans örtliche Netz und zu ihren kommunalen

IT-Infrastrukturen. Wir haben seit vielen Wochen keine Hardware- und keine Strukturprobleme. Es gibt Nacharbeiten an der Software, zum Beispiel die Anpassung der Impfstoffe oder bestimmter Priorisierungsgruppen. Die Grundstruktur steht völlig stabil, das „Nachschrauben“ ist die Herausforderung.

INFORM: *Mangels Impfstoff laufen die Impfzentren noch immer nicht auf Vollast. War die Schonzeit gut für die IT-Ausstattung?*

Stettner: Es ist immer gut, zumindest ein paar Tage zu haben, um sich warmzulaufen und die Infrastruktur zu überprüfen. Krisenmanagement zeichnet sich dadurch aus, dass es ein atmendes System ist. Das habe ich bei den Erstaufnahmeeinrichtungen auch schon gesagt. Das System darf nicht aus Zement gegossen sein. Insofern ist es gut, wenn man sich ausprobieren und Lehren ziehen kann. Und das war in der Tat im Dezember und Januar so. Aber jetzt ist es sehr wichtig, dass die Impfzentren auf Vollast fahren können. Wir haben unseren Beitrag geleistet, dass sie es können. Ich hoffe sehr,

dass der Impfstoff bald in großer Masse kommt.

INFORM: *Seit mehr als einem Jahr hat Corona die Welt im Griff. Testen und Impfen sind die großen Hoffnungsschimmer, um in ein „normales“ Leben zurückkehren zu können. Was glauben Sie, wie lange werden Sie, die Verantwortlichen und Zuständigen, aber auch die Bürgerinnen und Bürger, die Impfzentren noch begleiten?*

Stettner: Seit dem 7. April kann man sich in Hausarztpraxen impfen lassen. Es fängt langsam an, weil nicht viel Impfstoff da ist. Die Arbeits-, Betriebs- und Privatärzte sollen nachgeschaltet werden. Das wird ein wesentlicher Pfeiler werden. Das Ziel ist die Regelversorgung durch die Ärzteschaft. Ich schließe nicht aus, dass es eine Übergangsphase von ein paar Monaten geben wird, mit den Impfzentren als stabilem Faktor, der da ist.

INFORM: *Herr Stettner, besten Dank für das Gespräch.*

Hinweis: Das Gespräch haben wir am 8. April 2021 geführt.





AUF DEM WEG ZU WOLKE 7

IT-Services, die den klassischen Behörden-gang weitestgehend ersetzen, sind von Bürgerinnen und Bürgern gefragt, von Gesetzes wegen und auf strategischer Seite gefordert. Ob Onlinezugangsgesetz auf Bundesebene oder „Strategie Digitale Verwaltung Hessen“, die Umsetzung dieser und vieler weiterer Vorgaben erfordert IT-Services, die am besten jederzeit verfügbar, bei Bedarf änderbar und automatisiert erweiterbar sind. Die Nutzung von modularen, skalierbaren, hochverfügbaren Cloud-Services ist eine Lösung dafür. Die HZD als Full-Service-Provider der hessischen Landesverwaltung wird deshalb in den nächsten Jahren ihr Cloud-Angebot ausbauen.

Cloud-basierte Ökosysteme bieten die Chance, Daten verschiedener Quellen auf neue, kreative Weise miteinander zu verknüpfen, Innovationen zu beschleunigen und neue Wertschöpfungsmodelle zu entwickeln. Ohne die Möglichkeit, in solchen Daten-Ökosystemen zu agieren, verlieren die HZD und das Land Hessen als Treiber von Innovation und Modernisierung den Anschluss und die Digitalisierungsziele geraten außer Reichweite.

Um die digitale Transformation des Landes Hessen unterstützen zu können, will die HZD gemeinsam mit ihren Kunden sowohl für die bestehenden Systeme als auch für neue Anforderungen das passende Cloud-Angebot finden. Dafür baut die HZD neben der Infrastruktur gezielt Cloud-Beratungskompetenz auf, nimmt die Rolle des Cloud-Beraters und -Vermittlers ein und entwickelt sich zum Cloud-Service-Entwickler. All das geht mit einem kulturellen und organisatorischen Wandel einher.

Wesentliche Aspekte beim Auf- und Ausbau des Cloud-Angebotes sind neben den genannten Ausführungen auch allgemeine Cloud-Paradigmen: insbesondere die Gewährleistung von Informationssicherheit und Datenschutz durch Implementierung von speziellen Sicherheitsprinzipien (z.B. Zero Trust) sowie die Zertifizierung der Cloud-Infrastruktur (gemäß BSI C-5) oder die Stärkung der digitalen Souveränität durch Interoperabilität und Nutzung von offenen Standards.

Bei der Entwicklung neuer Cloud-Services werden veränderte Architekturmuster wie Microservices, Bereitstellungsformen wie Container (ab S. 24) und agile Vorgehensweisen wie Continuous Integration und Continuous Delivery (ab S. 28) eingesetzt, um im Sinne des DevOps-Modells¹ die notwendige Flexibilität und eine Erhöhung der Geschwindigkeit in der Softwareentwicklung und in deren Bereitstellung zu erreichen. Wie die Beispiele in diesem Themenschwerpunkt zeigen, finden diese bereits an vielen Stellen in der HZD Anwendung.

Überhaupt: Schon vor fast zehn Jahren hat die HZD begonnen, sich intensiv mit der Cloudisierung zu beschäftigen – damals scheinbar noch ein „Modethema“, das 2014 zu ersten Lösungen wie der Test- und Entwicklungsplattform führte, mit der die Cloud in der HZD pilotiert wurde. Diese erste Private-Cloud-Lösung der HZD schnürt Rechenzentrumsdienste zu handlichen Paketen und liefert sie per Knopfdruck schnell und bedarfsgerecht. Nutzer*innen sind die Entwickler*innen in den Anwendungsbereichen der HZD, die bis heute im Self-Service virtuelle Serversysteme quasi im Handumdrehen erzeugen können. HessenConnect (Skype for Business) war 2016 die erste Anwendung der HZD, die nicht im eigenen Rechen-



Die Cloud-Vision der HZD

Bis 2025 wird die HZD in Hessen und darüber hinaus anerkannter und geschätzter Partner für die Bereitstellung von Cloud-Services sein und ihre Kunden als solcher mit höchsten Sicherheitsstandards und kompetenter Cloud-Beratung überzeugen.

Die Cloud-Produkte der HZD werden auf die Landesverwaltung zugeschnitten sein, um die Bedürfnisse ihrer Kunden bestmöglich abzudecken.

Agile Vorgehensweisen werden der HZD in der Umsetzung der Kundenwünsche nach Innovation die notwendige Flexibilität und Geschwindigkeit geben.

Das macht die HZD zu einem noch attraktiveren Arbeitgeber, der nachhaltig und verantwortungsvoll mit Ressourcen umgeht.

¹ Der Kunstbegriff DevOps ist ein Synonym für ein Paradigma bei der Bereitstellung von IT-Diensten. Er beschreibt die Zusammenführung von Entwicklung (Development - Dev) und Betrieb (Operations - Ops).



zentrum betrieben wird, sondern in einer sogenannten Managed Public Cloud.

Im Zuge der digitalen Transformation führt heute an einem breiteren, ganzheitlichen Aufbau von Cloud-Angeboten kein Weg mehr vorbei. Mit der Cloud-Strategie hat die HZD die theoretische Grundlage aller weiteren Schritte geschaffen. „Eckpfeiler“ für die Erweiterung des Portfolios sowie die Transformation von Verfahren in die Cloud sind fünf übergreifende Prinzipien:

- höchste Priorität bei Sicherheit und Datenschutz
- Schnelligkeit bei Konzeption, Ausführung und Lieferung
- Fokussierung auf den Kunden in allen Phasen der Leistungserbringung
- Fokussierung auf Interoperabilität, Portabilität und offene Standards für Digitale Souveränität und Zusammenarbeit
- CO₂-Neutralität

In der Praxis schafft die HZD seit 2020 mit der VerfahrenscLOUD Hessen (ab S. 20) in ihren Rechenzentren eine Cloud-Infrastruktur als so genannte Private Cloud. Die Infrastruktur ist so gestaltet, dass bedarfsgerecht Cloud-Angebote Dritter (Öffentliche Dienstleister oder

externe Cloud-Anbieter) angebunden werden können und so das Produktportfolio der VerfahrenscLOUD Hessen zu einem Multi-Cloud-Angebot erweitert werden kann. Die HZD möchte mit der VerfahrenscLOUD Hessen ein Angebot schaffen, mit dem sie anforderungsgerecht für ihre Kunden den jeweils passenden Mix aus Cloud-Services orchestrieren kann. Da die VerfahrenscLOUD Hessen perspektivisch Teil einer föderalen Deutschen VerwaltungscLOUD und damit u.a. das Fundament des Plattformsystems zur Umsetzung des Onlinezugangsgesetzes in Hessen werden soll, werden bereits bei der Implementierung die Anforderungen der „Deutschen VerwaltungscLOUD-Strategie“ und die im IT-Planungsrat abgestimmten Blaupausen für die Implementierung berücksichtigt (s. S. 23).



Janina Einsele
Enterprise Architektin der HZD

janina.einsele@hzd.hessen.de



Peter Lacher
Technischer Programmleiter 24/7 -
Hochverfügbarkeit

peter.lacher@hzd.hessen.de

AUF DEM WEG ZU **WOLKE** **7**

„Das Thema Cloud ist das bahnbrechende Thema in der IT der letzten 40 Jahre. Im Prinzip beschäftigen sich alle IT-Dienstleister damit. Auch wir müssen uns intensiv damit beschäftigen. Und zwar jetzt. Wir sprechen hier nicht von einer Dringlichkeit, die irgendwann kommen wird, sondern einer bereits existierenden Dringlichkeit.“

Als Full-Service-Provider des Landes ist es unsere urreigene Aufgabe, technisch auf der Höhe der Zeit zu sein und ein attraktives Cloud-Angebot zu schaffen.“

Thomas Kaspar
Technischer Direktor der HZD

Auf dem Weg zur Multi-Cloud



Was ist Cloud?

Der Begriff „Cloud Computing“ ist ein feststehender, quasi-standardisierter Begriff. Durch die internationale Gleichbedeutung des Begriffs ist sichergestellt, dass in allen Regionen der Welt dasselbe Verständnis vorherrscht, was „Cloud“ ist und was die reine Technologie leistet. Hinter diesem Begriff steckt eine Vielfalt von Techniken und Standards, die im Zusammenspiel mit allgemein anerkannten Prinzipien eine große Menge an unterschiedlichen Diensten bereitstellt.

Nüchtern betrachtet wird die Cloud definiert als ein Portfolio aus standardisierten Produkten einer IT-Infrastruktur, das über dedizierte Schnittstellen in formal uneingeschränkter technischer Verfügbarkeit über Rechnernetzwerke ad-hoc bereitgestellt wird, aus Speicherplatz, Rechenleistung und Anwendungssoftware besteht und nutzungsabhängig vergütet wird.



Seit dem vergangenen Jahr nutzen die ersten Kunden der HZD die Vorteile der Verfahrenscloud Hessen (VCH) ganz nach dem Prinzip „Infrastructure as a Service“. Um langfristig alle IT-Services auf die Verfahrenscloud Hessen übernehmen zu können, treibt die HZD deren Ausbau mit neuen Tools und flankierenden Projekten voran.

2019 startete die HZD die Produktentwicklung der Verfahrenscloud Hessen (VCH). Dabei handelt es sich um eine logische Plattform, die vollständig gemäß den Definitionen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum Cloud Computing arbeitet. Die VCH ist der technische Ausgangspunkt für eine komplette Cloud-Strategie, an der sich die Cloud-Transformation der HZD ausrichten wird: vom Nischenprodukt in der Cloud zum Cloud-Anbieter, der nur noch wenige Verfahren ohne Cloud-Anbindung betreiben wird. Alle IT-Services der HZD und ihrer Kunden sollen demnach (sofern technisch möglich und sinnvoll) mittelfristig sukzessive auf die VCH übernommen werden. Dabei wird die HZD eine hochverfügbare und über zwei Standorte abgesicherte Private-Cloud-Infrastruktur bereitstellen. Vorkonfigurierte Cloud-Ressourcen sollen aus dem Hessennetz heraus bedarfsgerecht jederzeit abrufbar sein. Der Zugang zu den Diensten wird unkompliziert mit Hilfe von Standardbrowsern über ein Selfservice-Portal erfolgen und die Nutzung anschließend nach Verbrauch abgerechnet werden.

Plattform as a Service

Die ersten großen Schritte auf dem Weg zum Cloud-Service-Provider ist die HZD bereits im vergangenen Jahr gegangen. Seit dem 1. Juli 2020 steht HZD-Kunden die Verfahrenscloud Hes-

sen zur Verfügung. Damit können virtuelle Server (als Hülle und zunächst ohne Betriebssystem) bereitgestellt werden. Und zwar nicht mehr auf klassischem Weg, sondern auf der Basis einer hyperkonvergenten Infrastruktur. Diese „Infrastructure as a Service“ (IaaS) wird in der Folge konsequent weiter zu einer IaaS plus und zu einer PaaS (Plattform as a Service) ausgebaut werden. Ein zentrales Element ist hierbei der Aufbau einer Cloud-Management-Plattform mit einem Portal für Themen wie Selfservice, Monitoring, Reporting, Automatisierung usw. Aber auch Themen wie Software-defined Networking, Plattfordienste für Virtual Desktop Infrastructure (VDI) und Container usw. werden hierbei betrachtet.

Erste Migrationen

Das Hessische Statistische Landesamt (HSL) wurde als erster Kunde der HZD mit einem beträchtlichen Teil seiner Infrastruktur aus dem eigenen Rechenzentrum bereits auf eine Vorversion der Verfahrenscloud Hessen migriert. Der Abschluss der dreistufigen Migration von rund 100 virtuellen Maschinen erfolgte zum 31. März 2020. Seitdem läuft der Betrieb störungsfrei.

Seit 2020 nutzen weitere Kunden die Services der Verfahrenscloud Hessen. Am prominentesten wäre hier die Polizei mit der Verfahrensfamilie POLAS zu nennen, die bis Oktober 2020 vollständig auf die VCH migriert wurde. Des Weiteren die Justiz mit dem umfangrei-

chen Programm eJustice, das nach ausführlichen Tests 2021 in der zweiten Jahreshälfte 2020 produktiv gesetzt werden konnte.

Mehr Raum für IT-Kernaufgaben

Der Nutzen für das HSL wie auch für weitere Kunden, die von eigenen Rechenzentrumsinfrastrukturen auf die VCH im Rechenzentrum der HZD migrieren, liegt derzeit vor allem darin, an den höheren Sicherheitsstandards der HZD-Rechenzentren zu partizipieren und von den spezifischen Kosten und Risiken bei der Bereitstellung der Infrastruktur entlastet zu werden. Außerdem kann sich das eigene IT-Personal verstärkt auf die IT-Kernaufgaben des Kunden konzentrieren. Mit dem weiteren Ausbau der VCH kommen neue Tools und flankierende Projekte hinzu, die zusätzliche cloudspezifische Vorteile bieten.

Portal-, Container- und SDN-Lösungen

Mit Morpheus wird gegenwärtig ein Tool evaluiert, das die Verwaltung der Cloud-Umgebung vereinfacht und einen Kundenzugriff zu Bestellung, Reporting und Selfservice möglich machen wird. Hierbei werden auch Schnittstellen zum neuen Tool für Prozessmanagement, zu Containern und zum Software-defined Networking (SDN) entwickelt. Dies ist insofern relevant, als dass für die VCH eine stabile, wartbare und flexible Infrastruktur aufgebaut werden soll, in der auch Container von einem Entwicklungsteam oder Fachverfahren betrieben werden können. Die VCH muss als Plattform sicherstellen, dass die in der Umgebung zu betreibenden Container den Ansprüchen von HZD und BSI an Sicherheit, Monitoring, Logging und Skalierung genügen. Im Rahmen einer Pilotierung soll in der zweiten Jahreshälfte eine erste Umgebung bereitgestellt werden. Auch SDN ist von zentraler Bedeutung für die VCH, weil es eine intelligente, zentrale Steuerung von Netzen mithilfe von Softwareapplikationen ermöglicht

und damit einen wesentlichen Beitrag zum Erreichen der Ziele im Hinblick auf eine Private- und Multi-Cloud-Strategie leistet. Derzeit wird im Rahmen eines Vorprojekts analysiert und geprüft, inwieweit dies im Kontext der VCH umsetzbar ist.

Mit virtuellem Arbeitsplatz und hochverfügbarem Administrationszugang

Eine weitere Frage, die die Entwickler*innen der VCH umtreibt: Wie kann ein virtueller Arbeitsplatz auf der VCH bereitgestellt werden, also eine Virtual Desktop Infrastructure (VDI) geschaffen werden? Hierbei wird der komplette HessenPC als Client virtuell zur Verfügung gestellt und zentral betrieben. Das bedeutet, dass alle Funktionen und Softwarepakete über ein Netzwerk bereitgestellt werden und der Arbeitsspeicher sowie Speicherplatz nicht mehr lokal vorgehalten werden. Eine produktive Bereitstellung dieser Ausbaustufe ist für Ende August 2021 geplant.

Zusätzlich kommt mit der MAOAM-Zone (Management, Automation, Orchestrierung, Analyse, Monitoring) beim Ausbau der VCH eine konsolidierte, standardisierte und redundante Plattform ins Spiel, die administrative Infrastrukturen für Systeme, Netze, Firewalls etc. bereitstellt – also einen einheitlichen, sicheren und hochverfügbaren Administrationszugang schafft. Während Systeme der VCH von vorneherein und ausschließlich über die MAOAM administriert werden, befinden sich Legacy-Systeme (Altsysteme) noch überwiegend außerhalb, werden jedoch nach und nach ebenfalls in die MAOAM überführt.



Dr. Martin Scheuermann
Bereichsleiter RZ Management und Prozesse

martin.scheuermann@hzd.hessen.de

Es gibt verschiedene Initiativen und Arbeitsgruppen, die eine Bundes-Cloud mit möglichst digitaler Souveränität im Blick haben, darunter die des IT-Planungsrats. Das zentrale Gremium für die föderale Zusammenarbeit in der Informationstechnik hat nun den über 100 Teilnehmer*innen der AG „Cloud Computing und Digitale Souveränität“ und der UAG „Technik & Betrieb“ (s. auch INFORM 1/21) einen Beschluss zur Schaffung von Standards und Schnittstellen für föderale Cloud-Lösungen übergeben. Das heißt: Die nächsten Schritte werden angegangen und umgesetzt. Das erklärte Ziel ist, bis Ende des Jahres ein gemeinsames Architekturkonzept der deutschen Verwaltungscoud zu erstellen. Mitten auf diesem Weg möchten wir einen kleinen Einblick in die gemeinsamen Überlegungen bieten.

Es wird ein verteilter Betrieb der föderalen Cloud-Lösung in Rechenzentren des Bundes, der Länder und Kommunen angestrebt. Die IT-Dienstleister der öffentlichen Verwaltungen sollen diese dezentrale Cloud-Infrastruktur hosten und betreiben. Private Anbieter und Drittanbieter sollten dabei nicht grundsätzlich ausgeschlossen werden.

Alle Organisationen aus Bund, Ländern und Kommunen sollen die angebotenen Lösungen der föderalen Cloud nutzen können. Entstehende Erweiterungen und Anpassungen



HZD-weiter Austausch

Bei ihrer internen Fachtagung Ende März rückte die HZD einen ihrer zentralen Arbeitsschwerpunkte in den Fokus: Unter dem Motto „Auf dem Weg zu Wolke 7“ wurde das Thema Cloud-Transformation aus verschiedenen Blickwinkeln beleuchtet.

Den Auftakt der vom Enterprise Architekturmanagement organisierten 7. Auflage bildete eine Bestandsaufnahme von Ist-Situation und kommenden Herausforderungen. In seiner Keynote skizzierte Thomas Kaspar, Technischer Direktor der HZD, Vision und Mission für die nächste Phase des anspruchsvollen Vorhabens. Das Enterprise Architekturmanagement erstellte mit dem Input der Tagungsteilnehmer*innen eine Standortermittlung hinsichtlich der anstehenden Aufgaben vor.

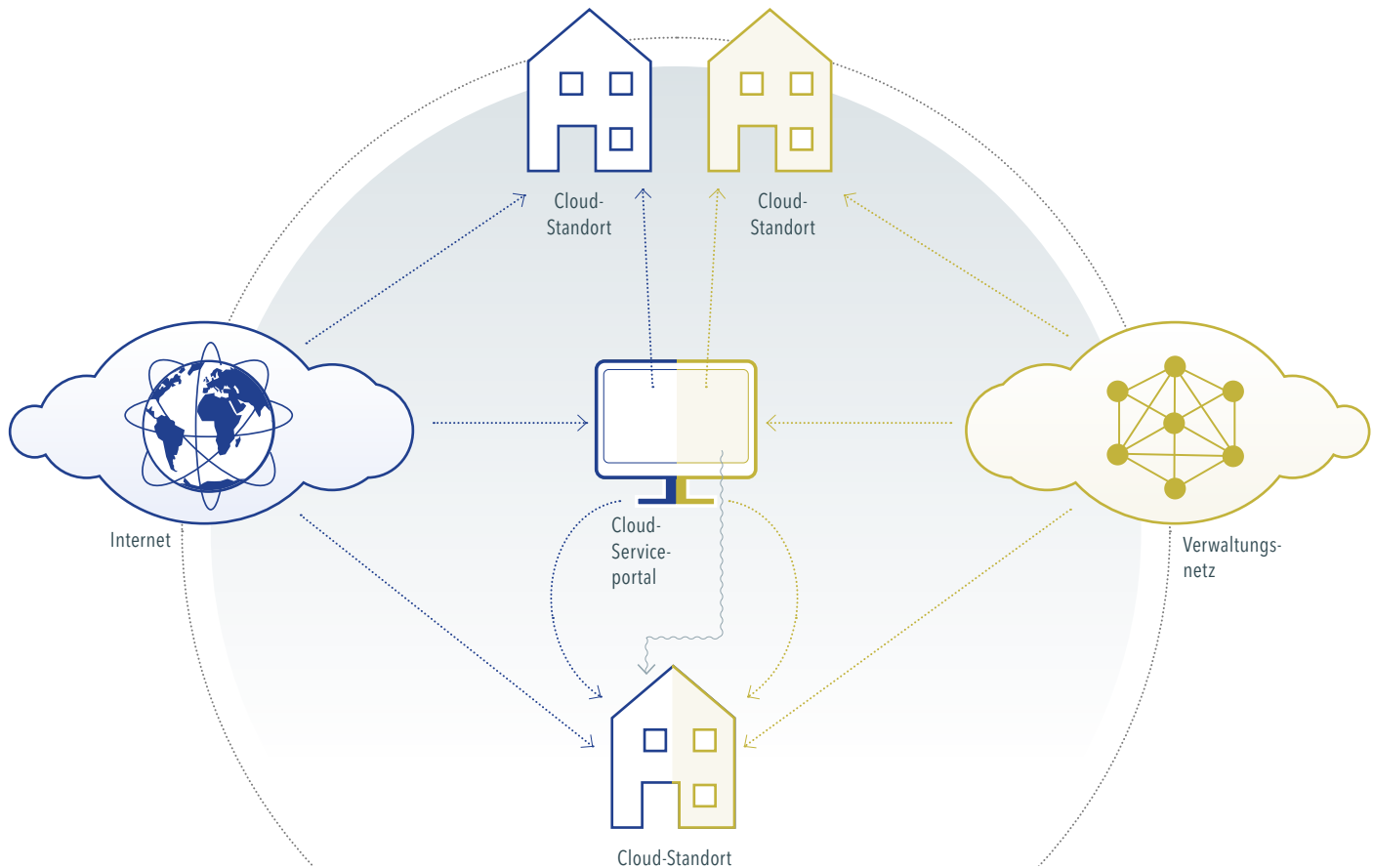
Aktive Mitarbeit war auch bei „Neulich in der Public Cloud“ gefragt. Der Workshop des HZD-Innovationsmanagements lud ein, Erfahrungen mit öffentlichen Cloud-Services auszutauschen und daraus mögliche Schlüsselgedanken für die künftige Arbeit abzuleiten.

Die Erfahrungsberichte und Fachvorträge zu den Cloud-Aktivitäten in der HZD waren für die Teilnehmer*innen in doppelter Hinsicht lohnend. Zum Teil zeigten sie einen Querschnitt der Projekte, die in Sachen Cloud-Transformation bei der HZD in Arbeit sind oder bereits realisiert wurden. Andere eröffneten den sprichwörtlichen Blick über den Tellerrand und skizzierten die Cloud-Strategien von Akteuren aus Wirtschaft und Gesellschaft.

Die Fachtagung im Überblick

Vorträge	Workshop	Erfahrungsberichte	Cloud-Aktivitäten in der HZD
<ul style="list-style-type: none"> ■ Vision & Mission, Ableitung von Handlungsfeldern und Maßnahmen ■ Gastbeitrag: Vorstellung der Cloud-Transformation beim BWI – Lessons Learned 	<ul style="list-style-type: none"> ■ Neulich in der „Public Cloud“: Erfahrungen mit Public Cloud-Services und was wir daraus lernen können 	<ul style="list-style-type: none"> ■ Übergeordnete Cloud-Aktivitäten auf Bundesebene: <ul style="list-style-type: none"> – AG Cloud und digitale Souveränität, UAG Technik und Betrieb, IG Container ■ Cloud bei IKEA IT – ein Erfahrungsbericht und Austausch zu den Dimensionen der Cloud-Transformation 	<ul style="list-style-type: none"> ■ Projektstatus Verfahrenscloud Hessen und Cloud-Management-Plattform ■ Informationssicherheit: Bausteine und Richtlinie zu Cloud und Container ■ Technische Digitalisierungsplattform ■ Softwarearchitektur für die Cloud: Independent System Architecture (ISA) ■ Umgang mit Cloud-Strategien am Beispiel Office ■ Continuous Delivery-Prozesse in der HZD ■ Aktivitäten in den bundesweiten Verfahren e-Justice und KONSENS

Die Deutsche Verwaltungscloud- Strategie nimmt Form an



einer Lösung sollen für andere Teilnehmer*innen nachgenutzt werden können.

Open Source-Software wird als probates Mittel für den Aufbau der Cloud angesehen. Betriebene Anwendungen in der Verwaltungscloud müssen allerdings nicht Open Source sein. Es sollte aber ein „Vendor Lock-in“ verhindert werden. Die Beauftragung, Anpassung und Löschung von Services erfolgt über ein zentrales Cloud-Serviceportal. Die angebotenen Services werden in

einem standardisierten Servicekatalog verwaltet. Endnutzer*innen können direkt am Cloud-Standort ohne die Nutzung des Cloud-Serviceportals darauf zugreifen.

Neben grundsätzlichen Überlegungen und einem gemeinsamen Glossar wurden bereits über 100 Use Cases mit Akzeptanzkriterien beschrieben, die mit dem Zielkonzept abgebildet werden sollten.

- ➔ Die Federführung der am stärksten besetzten UAG „Technik und Betrieb“ liegt beim Ministerium für Energiewen-

de, Landwirtschaft, Umwelt, Natur und Digitalisierung in Schleswig-Holstein und beim Datenverarbeitungszentrum Mecklenburg-Vorpommern. Hauptansprechpartner in der HZD sind Markus Kantowski sowie die beiden weiteren beteiligten Kolleg*innen Janina Einsele und Peter Müller.



Markus Kantowski
Stellvertretender Leiter
Enterprise Architektur-
management HZD
Architektur-B@hzd.hessen.de

Container- hafen

für die HZD



Private Cloud

Cloud-Produkte und -Dienste werden dediziert für eine Institution (Landesverwaltung) betrieben. Sie können von der Institution selbst oder einem Dritten organisiert und geführt werden und können dabei im Rechenzentrum der eigenen Institution oder eines Dritten gehostet werden.

Community Cloud

Produkte werden von mehreren Institutionen (z.B. Landesverwaltungen) geteilt, die ähnliche Interessen haben. Eine solche Cloud kann von einer dieser Institutionen und per Inter-Cloud-Connection gemeinsam mit Dritten betrieben werden.

Public Cloud

Produkte werden der Allgemeinheit oder einer großen Gruppe, beispielsweise einer ganzen Industriebranche, zur Verfügung gestellt.

Hybrid Cloud

Mehrere Cloud-Infrastrukturen, die für sich selbst eigenständig sind, werden über standardisierte Schnittstellen gemeinsam genutzt.

Container stehen bei Digitalisierungsstrategien mit Fokus auf IT-Architekturen weit oben auf der Agenda. Containerisierung gilt als der bedeutendste Umbruch in der IT-Welt seit Einführung der Hardware-Virtualisierung mit virtuellen Maschinen (VMs). Dabei erhielt diese neue Variante der Virtualisierung ihren Aufschwung mit dem Trend hin zu sogenannten Microservices und weg von monolithischen Applikationen.

Ähnlich wie VMs sind Container eine Art Behälter für Anwendungen, in dem diese laufen können. Während VMs eine ganze Computer-Umgebung abbilden, enthalten die Container lediglich die wichtigen Daten, die für die Ausführung der Applikation benötigt werden. Dazu gehören Betriebssystem-Komponenten wie Libraries und Binaries. Dies ermöglicht eine leichtgewichtige Form der Virtualisierung. Die wohl bekannteste Container-Technologie ist Docker, weswegen der Begriff „Docker Container“ in aller Munde ist.

Docker Container stellen abgekapselte Einheiten dar, die unabhängig voneinander ausgeführt werden können, ganz egal, wo sie sich gerade befinden. Vergleichen wir sie mit Frachtcontainern, in denen ein oder mehrere Männchen sitzen und arbeiten. Diese Männchen sind in unserem Fall Applikationen, beispielsweise php, mysql und Apache. Sie sitzen gemeinsam in einem Container. Für die Männchen macht es keinen Unterschied, ob der Frachtcontainer nun in Hamburg, New York oder Sydney steht. Von innen sehen die Container alle gleich aus und es herrschen dieselben Bedingungen. Dasselbe gilt

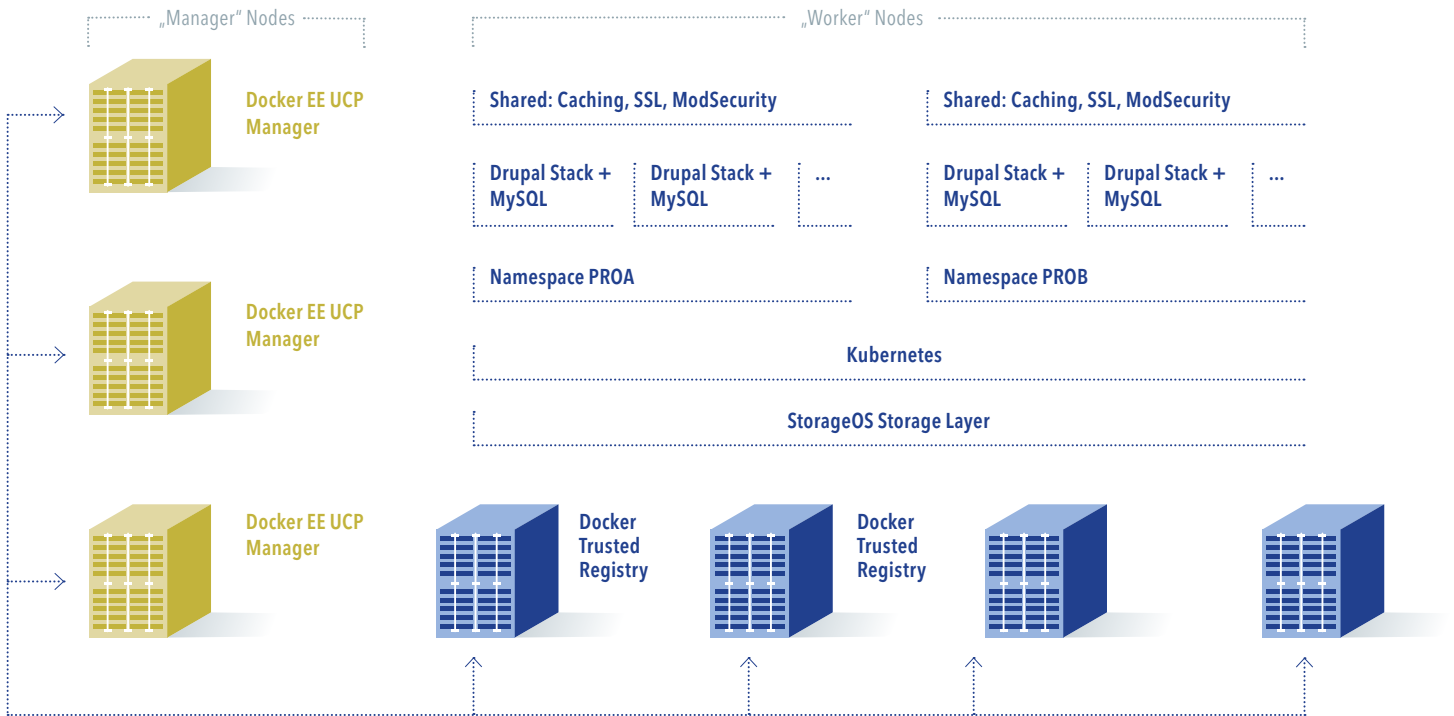
auch für die Applikationen im Software-Container.

Im Sommer 2018 hat das Portal-Betriebsteam begonnen, einen Proof of Concept (PoC) für eine Docker-basierte Infrastruktur durchzuführen. Ziel einer möglichen Docker-basierten Infrastruktur war es, neben den Verfahren im eigenen Bereich auch Verfahren aus anderen Bereichen betreiben zu können, um so eine entsprechende Optimierung der Auslastung der Ressourcen/Hardware zu erreichen.

Die folgenden Anforderungen wurden an die Docker-basierte Infrastruktur gestellt:

1. Optimierung der Ressourcen
2. Autoscaling, also die Möglichkeit individuelle Workloads nach Bedarf automatisch skalieren zu lassen
3. Flexibles Deployment
4. Updatefähigkeit der eingesetzten Komponenten

Für den Aufbau der entsprechenden Basisinfrastruktur haben wir neben Docker EE (Docker Enterprise) auch Kubernetes (EFK Stack Elasticsearch/Fluentbit/Kibana), Grafana, Ansible, StorageOS, NGINX+ usw. eingesetzt.



Architekturbild für Docker-basierte Infrastruktur
 bestehend aus Basisinfrastruktur und zusätzlichen Komponenten

Ende 2019 haben wir den PoC beendet. Als Gesamtergebnis lässt sich festhalten: Der PoC war erfolgreich, trotz der hohen Komplexität und teilweise mangelnder Produktionsstabilität einiger Softwarekomponenten. Auch die Bestätigung des architektonischen Ansatzes im PoC führt zu diesem positiven Ergebnis.

Ziehen wir noch einmal die genannten Anforderungen heran, zeigt sich ganz klar der Erfolg:

1. Optimierung der Ressourcen
 - Die Anzahl der Worker-Maschinen ergibt sich aus der Last bzw. der Nachfrage, die angestrebte Auslastung liegt bei rund 80 Prozent.
2. Autoscaling, also die Möglichkeit individuelle Workloads nach Bedarf automatisch skalieren zu lassen
 - Wurde durch Kubernetes (Auto-) Scaling und Ressource-Management-Mechanismen erreicht.
3. Flexibles Deployment
 - Wurde durch Automatisierung der Auslieferung CI/CD-Pipeline (Jenkins) erreicht.
4. Updatefähigkeit der eingesetzten Komponenten

– Alle eingesetzten Komponenten sind updatefähig und die Updates werden von den Herstellern regelmäßig zur Verfügung gestellt.

Der PoC hat nicht nur die Anforderungen erfüllt, er hat auch noch weitere Ergebnisse geliefert. Wir haben zum einen ein Betriebshandbuch und Sicherheitskonzept erstellt, zum anderen Last- & Performancetests sowie einen Penetrationstest erfolgreich durchgeführt. Und: Von den gewonnenen Erkenntnissen und Ergebnissen profitieren nicht nur wir als Portal-Betriebsteam, sie fließen auch in den Aufbau der Technischen Digitalisierungsplattform ein (s. S. 26).

AUF DEM WEG ZU
WOLKE 7



Thomas Schlander
 Gesamtbetriebsleiter Portale

thomas.schlander@hzd.hessen.de

Microservices für die digitale Transformation

Gute Aussichten: Die Technische Digitalisierungsplattform in der Cloud

Mit der Technischen Digitalisierungsplattform (TDP) die digitale Transformation der Verwaltung meistern, das ist der Anspruch des gleichnamigen Projekts, das in der INFORM 01/21 vorgestellt wurde.



(Cloud)-Transformation -

Punkt für Punkt umgesetzt mit der Checkliste IT-Architektur

Die „Checkliste IT-Architektur“ des Enterprise Architekturmanagements (EAM) der HZD kommt schon seit mehr als zehn Jahren bei der Entwicklung von Soll-Konzepten in IT-Projekten zum Einsatz. Und sie hat schon oft geholfen, selbst bei großen Vorhaben wie der Freiräumung von Rechenzentrumsräumen.

Inhalt der Checkliste sind vielfältige Fragestellungen, die in einem IT-Projekt früher oder später beantwortet werden müssen – darunter eben auch Fragen zum Thema Cloud-Transformation. Von der Funktionalität des IT-Services in einem Geschäftsprozess und der potenziellen Nutzergruppe führen diese durch die verschiedenen Ebenen der IT-Architektur bis hin zur konkreten technischen Umsetzung und zur Einführung des neuen IT-Services in den dauerhaften Betrieb. Unabhängig von einem Beratungsgespräch gibt die Checkliste samt Leitfaden den Projektleiter*innen, Verfahrensverantwortlichen und Änderungswilligen Anhaltspunkte und hilfreiche Hinweise zu Vorgaben/Vorschriften der Landesverwaltung.

Das Thema Cloud-Readiness spielt dabei eine immer größere Rolle. Die Ansprechpartner*innen kommen so bereits frühzeitig mit Fragestellungen rund um das Thema Cloud-Transformation in Berührung. Dabei kann das Thema von einer breiten und diversen Nutzergruppe mitbedacht und bei anstehenden Veränderungen mitberücksichtigt werden.

Ändern sich Vorgaben oder rücken zukünftige Änderungen in den Blickwinkel der dezentralen Projektleiter*innen, Verfahrensverantwortlichen und IT-Architekt*innen, ist dies einfach mit einer Ergänzung oder Erweiterung der Checkliste IT-Architektur möglich.

Perspektivisch plant das EAM der HZD, die Fragestellungen der Checkliste in einem IT-Service mit zentraler Datenbank abzubilden, sodass die Ergebnisse in ein zentrales Repository fließen, das übergreifend und mit anderen Projektdaten korreliert ausgewertet werden kann.

Die Antwort auf die Frage, wie die technischen Anforderungen zur Verwaltungsdigitalisierung erfüllt werden können, liefert die TDP-Integrationsplattform, ein TDP-Teilprojekt und ihr technischer Kern. Ihre Aufgabe ist es, durch einen modularen Aufbau der Digitalisierungsplattform ein nahtloses Zusammenspiel einzelner Komponenten zu ermöglichen und eine schnelle Entwicklung und Bereitstellung von Services zu unterstützen. Dynamische Skalierbarkeit und Ausfallsicherheit sind weitere Merkmale der Integrationsplattform.

Der Schlüssel zum Erfolg liegt im Einsatz geeigneter Werkzeuge und Technologien. Hier setzt die TDP-Integrationsplattform auf eine Microservice-Architektur auf Basis von Containern unter Nutzung von Cloud-Infrastruktur.

Die Vorteile dieses Ansatzes liegen auf der Hand: Die Microservice-Architektur bietet die Möglichkeit von agilen Entwicklungsprozessen. Anwendungen werden in kleine, in sich geschlossene Dienste aufgeteilt, sodass die Funktionen einer Anwendung flexibel erstellt und aktualisiert werden können. Dies

reduziert die Abhängigkeit zwischen Softwarekomponenten. Module können leicht ausgetauscht oder ergänzt werden, sobald sich Prozesse ändern oder Anwendungen hinzukommen, ohne dass das gesamte System geändert werden muss.

Container verbessern die Bereitstellungszeit und die Effizienz von Anwendungen in einer Microservice-Architektur. Sie unterstützen Microservices auch nach einem Ausfall bei der erneuten Bereitstellung. Die Containerplattform erlaubt es, containerisierte Software-Komponenten auszutauschen und unkompliziert über generische Schnittstellen anzubinden. Die technisch einheitlichen Schnittstellen, die die TDP-Integrationsplattform anbieten wird, sind für die Kommunikation in einer verteilten Architektur unerlässlich, in der Lösungsbausteine oder Verfahren außerhalb der Digitalisierungsplattform mit den Microservices der Plattform kommunizieren. Sie sind gekennzeichnet durch standardisierte Technologie, Autorisierungs- und Authentifizierungsfunktionalität sowie standardisierte Fehlerbehandlung. Auf diese Weise bleiben die Microservices selbst leichtgewichtig.

Die Cloud-Infrastruktur schließlich ermöglicht ein flexibles Ressourcenmanagement, denn die Services sind dynamisch skalierbar und leicht anzusprechen. Mögliche Lastspitzen werden in der Cloud-Umgebung automatisch abgedeckt und verarbeitet. Als Cloud-Infrastruktur nutzt die TDP-Integrationsplattform als Plattform as a Service (PaaS) die Verfahrenscloud Hessen (VCH). Das Herzstück der Digitalisierungsplattform bilden die Microservices und generischen Schnittstellen, die von der TDP-Integrationsplattform bereitgestellt werden.

Mit diesem Technologiestack wird die TDP-Integrationsplattform zum Werkzeugkasten der digitalen Transformation, aus dem sich die Digitalisierungsprojekte bedienen, um eine Vielzahl an Verwaltungsleistungen digital umzuset-



zen. Sie reduziert die Komplexität für diese Digitalisierungsprojekte und versetzt sie in die Lage, Online-Services so zu entwickeln, dass die Geschäftsprozesse durchgängig elektronisch abgewickelt werden können. Einmal implementierte digitale Verwaltungsleistungen lassen sich einfach weiterentwickeln, ihre Administration und ihr Betrieb werden vereinfacht und optimiert.

So steht über die Digitalisierungsplattform bald nicht nur eine große Anzahl neuer Verwaltungsverfahren und digitaler Bürger-Services zur Verfügung, sondern diese auch rund um die Uhr.

AUF DEM
WEG ZU
WOLKE
7



Dr. Petra Förg
Kunden-, Projekt- und Architektur-
management
petra.foerg@hzd.hessen.de

Abläufe automatisieren, **Software- Qualität** steigern

Continuous Integration (CI) und Continuous Delivery (CD) werden immer häufiger im Bereich Testing und Cloud-Technologien eingesetzt. Auch im Mehr-Länder-Verfahren der Justiz e²P baut die HZD auf die moderne Technologie; genauso im Wohngeldverfahren, das die HZD seit 1978 betreibt und stets weiterentwickelt.

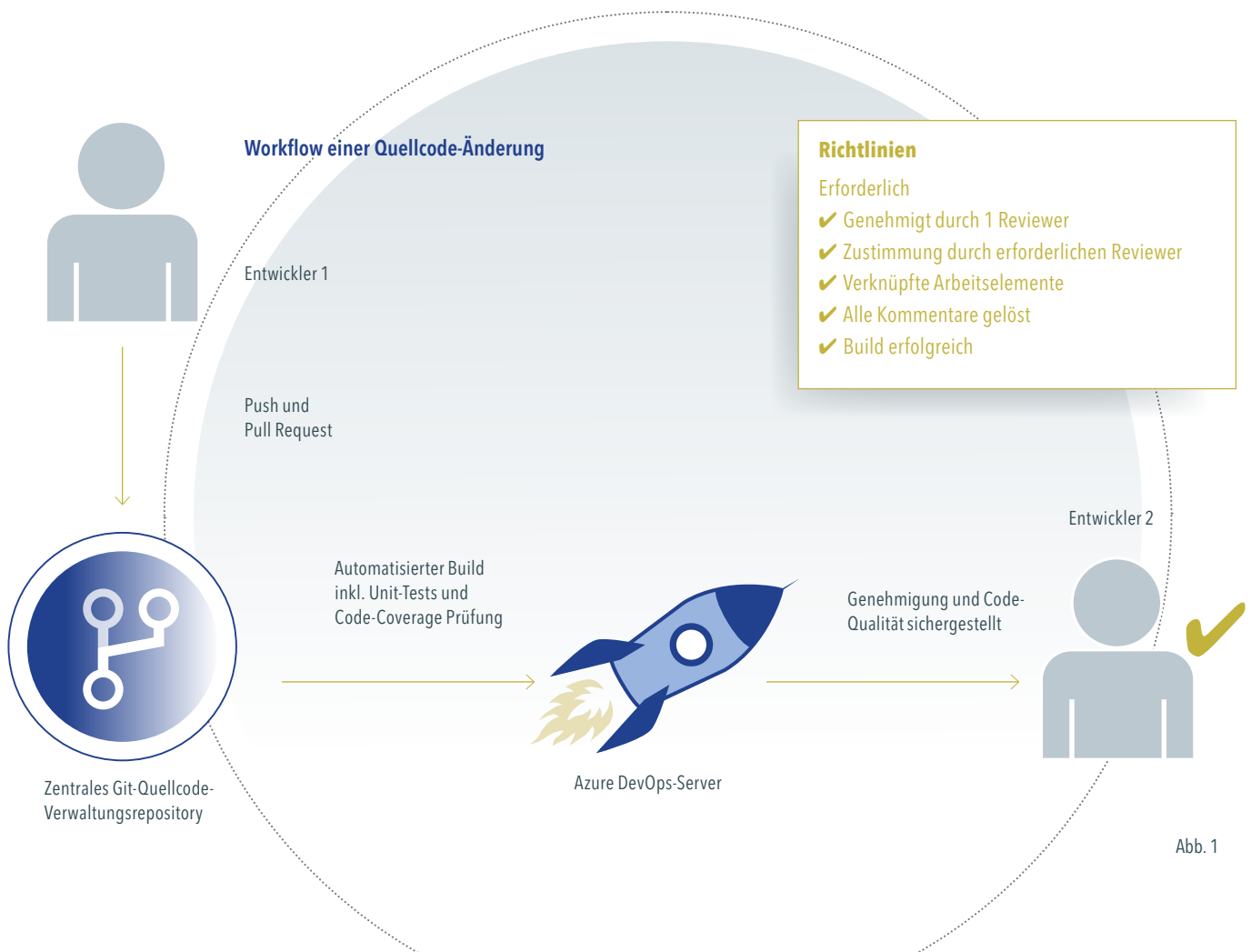


Abb. 1



Das Justizverfahren e²P ist eine im e²-Verbund entwickelte Software. Daraus ergibt sich, dass die Software-Komponenten nicht automatisiert in die produktiven Umgebungen ausgeliefert werden können. Die Software-Architektur entspricht hier einer serviceorientierten Architektur (SOA), die derzeit nicht auf Container-Technologien aufbaut. Mit dem Aufbau einer CI/CD-Pipeline will die HZD die folgenden drei Ziele erreichen:

- Sicherstellung der Code-Qualität
- Schnelle Integration
- Aufwände minimieren und Fehlervermeidung durch automatisiertes Deployment

Als Tooling haben wir den Azure Dev-Ops-Server und die Software ReadyAPI für Integrationstests gewählt.

Beispielhaft stellen wir den Workflow für eine Quellcode-Änderung einer Komponente vor (siehe Abb. 1). Ein Entwickler überträgt seine Änderungen an die zentrale Git-Quellcodeverwaltung (push) und beantragt die Übernahme in den allgemeinen Entwicklungsstrang (Pull Request). Im Hintergrund läuft ein automatisierter Build an, der die Softwarekomponente baut,



Continuous Integration ist ein Prozess in der Software-Entwicklung, der das fortlaufende Zusammenfügen und Testen einer Software mit ihren Komponenten beschreibt. Im Zeitalter von Cloud-Technologien und sogenannten Microservices stehen Entwickler*innen vor der Herausforderung, das Zusammenspiel einzelner Komponenten sicherzustellen. Denn: Es kann durchaus vorkommen, dass einzelne Komponenten für sich betrachtet sehr gut funktionieren, aber mit den anderen Komponenten der Software nicht zusammenarbeiten. Durch eine sogenannte CI-Pipeline versucht man, diese Integration sehr früh im Entwicklungsstadium zu testen und ggf. auftretende Fehler zu beheben.

Continuous Delivery ist eine Sammlung von Techniken bzw. Werkzeugen und Prozessen, die zum Ziel hat, den Softwareauslieferungsprozess zu verbessern. Software, die kontinuierlich weiterentwickelt wird, ist besonders davon betroffen, da hier immer wieder neue Versionen erzeugt werden. Die Qualität der Software wird permanent überprüft. Dabei helfen automatisierte Tests und automatisierte Reports, die Aussagen über die unterschiedlichen Qualitätsaspekte der Software abzubilden.

In Abgrenzung zum Begriff Continuous Deployment wird die Continuous-Delivery-Pipeline nur bis zu den vorproduktiven Systemen aufgebaut. Auf die produktiven Systeme wird die Software manuell ausgeliefert.

**Automatisiertes Deployment
der Komponenten**

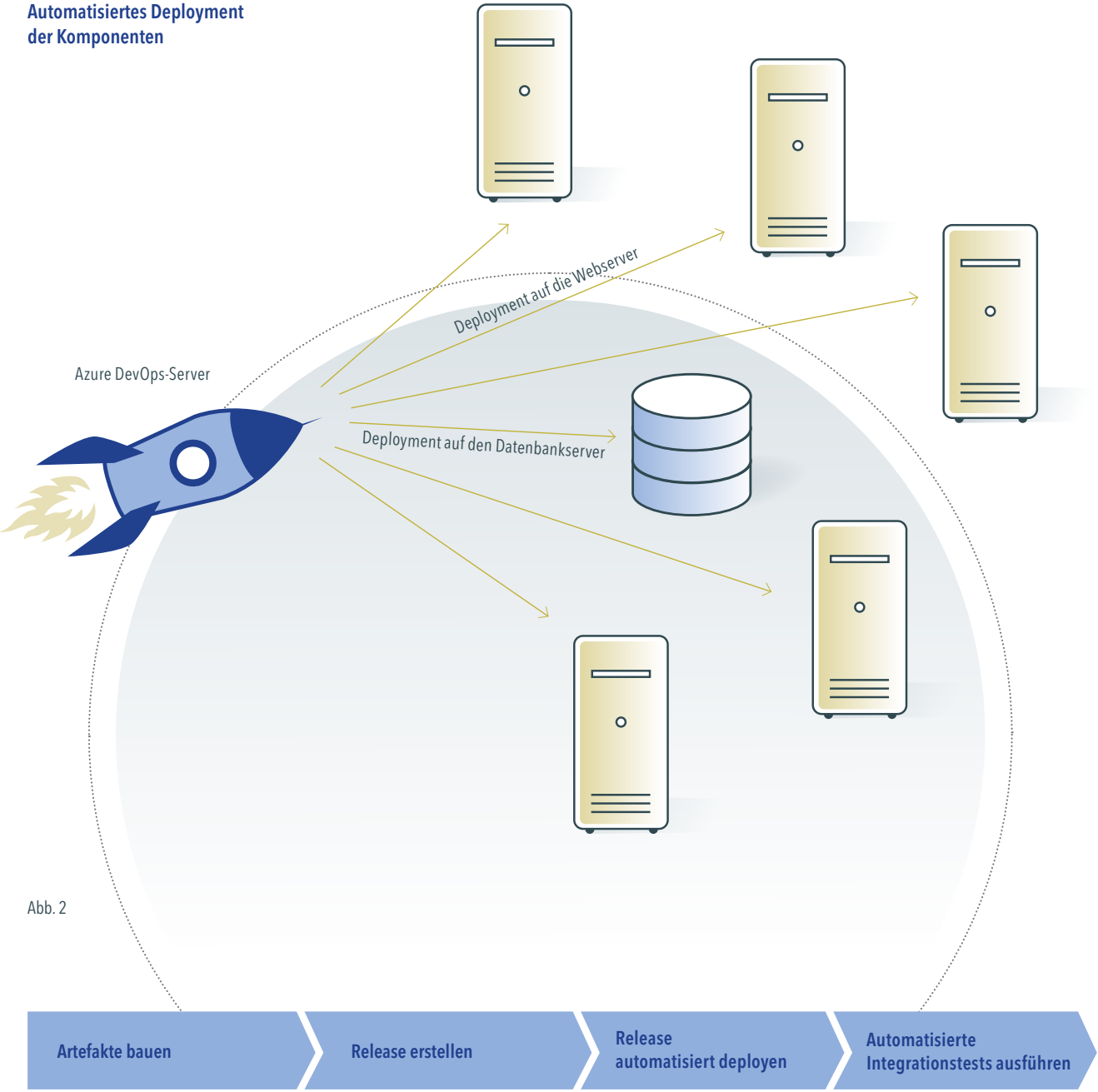


Abb. 2

die Unit-Tests ausführt und die Code-Abdeckung durch Unit-Tests prüft. Ist dieser durchgelaufen, schaut sich ein anderer Entwickler die Code-Änderungen an und kann diese genehmigen oder ablehnen. Dadurch ist der erste Punkt der definierten Ziele abgedeckt.

Im Anschluss werden die einzelnen Softwareartefakte gebaut, ein Release erstellt und die einzelnen Komponenten automatisiert auf die Server deployed (vgl. Abb. 2). Jeden Abend laufen dann die Integrationstests mit der Software ReadyAPI, die das Zusammenspiel der Komponenten testen. Dadurch sind die Punkte zwei und drei der Ziele abgedeckt.

Im Verfahren e²P haben wir die folgenden Erkenntnisse beim Aufbau einer CI/CD-Pipeline gewonnen:

- Der Initialaufwand für das Erstellen der Pipeline inklusive der benötigten Skripte ist relativ hoch.
- Der Nutzen – deutliche Zeitersparnis (mehrere Deployments täglich) und Reduzierung von Fehlerquellen – relativiert allerdings den anfänglichen Aufwand.
- Die Code-Qualität konnte durch die Automatisierung der Tests und der Qualitätssicherung anderer Entwickler deutlich gesteigert werden.

Die Automatisierungsskripte müssen genauso wie die Software gepflegt und weiterentwickelt werden. Dennoch lautet die klare Empfehlung aus dem Projekt, so viel wie möglich zu automatisieren. Der anfängliche Aufwand zahlt sich sehr schnell aus.

AUF DEM WEG ZU WOLKE 7

„Es entstehen immer mehr Cloud-Ökosysteme wie die deutsche Verwaltungscloud, GAIA-X, oder hybrides Government. Daten verschiedener Quellen werden auf neue, kreative Weise miteinander verknüpft werden. Ohne die Möglichkeit, in solchen Daten-Ökosystemen zu agieren, verlieren wir Bedeutung als Treiber von Innovation und Modernisierung in Hessen. Gerade die Kollaboration der Wirtschaft mit der öffentlichen Verwaltung erlangt im Rahmen des hybriden Governments immer mehr Bedeutung.“

Nur ein Beispiel: Bei der Buchung meiner Urlaubsreise wird mir mitgeteilt, dass mein Ausweis abgelaufen ist. Es wäre noch besser, wenn ich die Verlängerung des Ausweises gleich durchführen könnte.

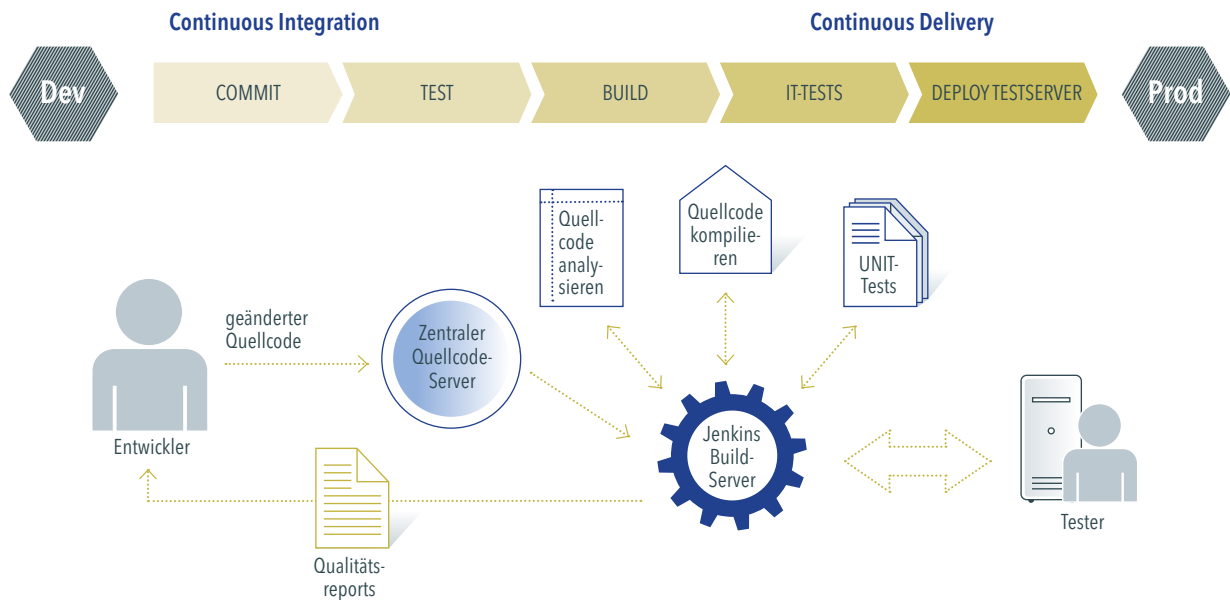
Sicherlich sind das große Herausforderungen an die IT-Sicherheit und den Datenschutz, aber ohne Cloud-Strategien wäre das alles nur theoretisch möglich.“

Thomas Kaspar
Technischer Direktor der HZD



Pascal Meister
IT-Entwicklungsleiter e²P

pascal.meister@hzd.hessen.de



Wohngeld - vom Großrechner in die Cloud

Einkommensschwächere Haushalte können einen Antrag auf Wohngeld stellen. Der Zuschuss zu den Wohnkosten soll dabei helfen, einen angemessenen und familiengerechten Wohnraum finanzieren zu können.

In Hessen liefen die Berechnungen bis 2009 auf dem Großrechner im Rechenzentrum der HZD. 2010 hat die HZD das Verfahren auf ein Web-Verfahren umgestellt. Ergebnis war HeWoG-Web, eine Java-basierte Webanwendung, die neben der Wohngeldberechnung eine anwenderfreundliche Plausibilisierung der Antragsdaten, umfangreiche Auskunfts- und Ausgabefunktionen und verschiedene Schnittstellen zu anderen Verfahren besitzt. Mittlerweile wird das hessische Verfahren auch in Thüringen und Brandenburg eingesetzt. Die drei Länder bilden einen Entwicklerverbund. Für das Jahr 2022 ist der Einsatz in Rheinland-Pfalz vorgesehen.

Die HZD hat das Wohngeldverfahren einst entwickelt und entwickelt es kontinuierlich weiter. Genau in solchen Fällen kommt die Technologie Continuous Delivery und damit die permanente Überprüfung der Qualität der Software und der verbesserte Auslieferungsprozess besonders zum Tragen. Im Wohngeldverfahren bauen wir seit Jahren auf Continuous Delivery.

In der Abbildung oben ist dieser Prozess dargestellt: Als Entwickler speichere ich meine Quellcode-Änderungen im zentralen Quellcode-Server. Im Anschluss daran wird der Quellcode kompiliert, eine statische Code-Analyse durchgeführt und danach laufen die UNIT-Tests. Die Ergebnisse werden jede Nacht zu Qualitäts-Reports zusammengefasst.

Nach den erfolgreichen UNIT-Tests werden die Artefakte gebaut, die installiert werden sollen. Im Wohngeldverfahren sind das die Web-

Anwendung und mehrere Batch-Anwendungen. Mit der Web-Anwendung werden automatisierte Integrationstests durchgeführt, d.h. Benutzereingaben gegen die Web-Oberfläche werden automatisiert ausgeführt. Sind alle diese automatisierten Tests positiv, führe ich noch manuelle Tests durch. Dazu wird die zu testende Web-Anwendung automatisch auf dem Entwicklungsserver installiert, auf dem die manuellen Tests stattfinden. Die Zeit vom Einchecken bis zum Testergebnis beträgt im besten Fall nur noch rund 15 Minuten.

Die Technologien und Werkzeuge in diesem Prozess des Wohngeldverfahrens sollen in den nächsten Jahren in die Cloud verlagert werden.



Hans Heinrich Napp
Entwicklungsleiter Java-Anwendungen

HansHeinrich.Napp@hzd.hessen.de



Und nun: **das Wetter!**

Berndnaut Smilde ist ein niederländischer Künstler. Auch wenn sein Name nicht sehr geläufig sein dürfte, haben viele von uns wohl schon einmal Bilder von seinen Kunstwerken gesehen: Wolken, die in Räumen schweben – in einem Gewölbekeller, einer Kirche, in einem mit Kronleuchtern dekorierten Saal oder einer verlassenen Fabrikhalle. Smilde betrachtet seine Wolken als temporäre Skulpturen aus fast nichts, die aussehen, als könne man sie greifen, und die doch zerfallen, wenn man es versucht.

Die Cloud, die uns alle möglichen IT-Dienste anbietet, hat mit den Wolken am Himmel – oder in Räumen – einiges gemeinsam: Wir kennen die einzelnen Bestandteile, wir verstehen die Grundprinzipien und Rahmenbedingungen der „Wolkenbildung“ und doch ist es nicht einfach, etwas zu machen, das den Namen Wolke verdient. Auch „die Cloud“ hat ganz verschiedene Erscheinungsformen: Die Größe, die Komplexität, die Elastizität können stark variieren. Während man bei Infrastructure as a Service (IaaS) die virtualisierte Technik noch erahnen kann, bekommt man das bei Anwendungen aus der Cloud (SaaS) nicht unbedingt mit: „Diese Wolke sieht aus wie ... eine Anwendung!“

Berndnaut Smilde liefert seine Wolken – in der IT-Sprache – „on premises“. Ist das sinnvoll? Draußen gibt es doch genug Wolken. Aber so, wie wir über das Wetter schimpfen, wird schnell deutlich, dass es oft „die falschen Wolken“ sind: zu viel, zu wenig, zu dunkel, zu nass ... Zudem lassen sich im Innenraum die Rahmenbedingungen kontrollieren. Das schafft mehr Klarheit und Berechenbarkeit, und auch mehr Arbeit: Wir sind selber für die Rahmenbedingungen verantwortlich und können uns nicht einfach an Vorhandenem erfreuen. Doch das können wir „draußen“ auch nicht unbedingt, denn die Rahmenbedingun-

gen der Cloud-Nutzung werden von vielen Faktoren beeinflusst. Das sind zum einen die großen Strömungen wie etwa die technische Entwicklung oder die rechtlichen Vorgaben wie die DSGVO. Es können zum anderen aber auch vergleichsweise kleine Einflüsse sein, wie die Verfügbarkeit eines einzelnen Dienstes oder spezieller Teilfunktionen, weil der Anbieter diese ändert.

Das Selbermachen hat neben der Kontrolle über die Rahmenbedingungen noch einen weiteren Vorteil. Wer sich mit den inneren Zusammenhängen befasst, lernt, die richtigen Fragen zu stellen. Es geht gar nicht darum, alles selber machen zu müssen. Und Fragen wirft die Beschäftigung mit Cloud-Technologien massenhaft auf, denn „Cloud“ ist mehr als etwas Technik und ein bisschen Self-Service. Schon fünf grobe Handlungsebenen der Cloud-Transformation lassen die Dimension erahnen. Da gesellen sich zur Infrastruktur noch die Architektur, die Organisationsstruktur, die (Unternehmens-)Kultur und die Prozesse. Eine Frage, die all diese Handlungsebenen überspannt, ist die, wie wir einen guten Service für unsere Kunden gestalten können. Neben den Erfahrungen des Selbermachens helfen uns dabei auch Erfahrungen des Selbernutzens von dem, was „draußen“ schon da ist. So können Dienste der „public“ und der „private cloud“ evtl. zu einem Gesamtangebot verschmelzen. Bei den echten Kunst-Wolken dürfte diese Verschmelzung von Drinnen und Draußen um einiges schwieriger sein.



Dr. Markus Beckmann
Architektur, Produkte und Standards,
Verfasser des Trendberichts der HZD
markus.beckmann@hzd.hessen.de

Auf Nummer sicher – der HessenPC 4.0

Der HessenPC wird noch sicherer: Mit dem HessenPC 4.0 wird eine deutliche Erhöhung des Sicherheitsniveaus unter Berücksichtigung der Usability erreicht. Dafür hat die Hessische Ministerin für Digitale Strategie und Entwicklung gemeinsam mit der HZD ein Gesamtpaket für die Mitarbeiter*innen der Landesverwaltung zusammengestellt, das den HessenPC um verschiedene zusätzliche Bausteine der IT-Sicherheit wie das Schnittstellenmanagement oder eine Erweiterung des Virenschutzes ergänzt.

Egal ob Wirtschaft oder Verwaltung – überall dort, wo Entscheidungen agieren und online präsent sind, finden sich Angriffsziele für Cyberattacken. Die Gefährdungen durch Ransomware, Malware, Spionage, Phishing und das Ausspähen von Computer-Netzwerken sind immer stärker auftretende Bedrohungsszenarien in der IT. Das zeigen die Emotet-Angriffswellen im letzten Jahr, die auch die IT-Systeme der hessischen Landesverwaltung betroffen hatten und dazu führten, dass über Monate bestimmte Anwendungen nur eingeschränkt nutzbar waren. Es gibt allerdings kein perfektes Sicherheitsprodukt, mit dem ein vollständiger Schutz für IT-Systeme erreicht werden kann. Deshalb müssen ganzheitliche Sicherheitskonzeptionen

unter Nutzung verschiedenartiger Bausteine der IT-Sicherheit entworfen werden, die – miteinander verzahnt – diesem Schutz möglichst nahekommen.

Neues Sicherheitspaket

Zur Absicherung des HessenPC kommen seit der Version 2.0 die Produkte des Zentralen Virenschutzes zum Einsatz. Durch sie können auffällige Ereignisse gemeldet oder aktiv unterbunden werden. Daneben werden Elemente wie Firewalls oder Paketfilter zum Schutz der IT-Netze und -Systeme der Landesverwaltung genutzt. Für Angriffsszenarien wie das Eindringen in IT-Systeme durch die Ausführung von noch unbekannter Malware gibt es jedoch aktuell noch keine Standardlösung. Angesichts der gestiegenen



Anforderungen und der sich ständig ändernden Angriffsszenarien arbeitet die HZD gemeinsam mit dem HMinD daran, den Schutz des HessenPC deutlich auszubauen. Dazu wird der HessenPC um verschiedene zusätzliche Bausteine der IT-Sicherheit ergänzt, die im Zusammenspiel für eine deutliche Erhöhung des Sicherheitsniveaus des HessenPC ohne Einschränkung der Usability sorgen können. Der geplante HessenPC 4.0 umfasst verschiedene Sicherheitsfeatures, die nun in einem sinnvollen Maßnahmenpaket gebündelt wurden. Diese Bündelung erleichtert die fachliche Abstimmung sowie die Klärung der Finanzierung. Die geplante Erweiterung des Sicherheitspaketes für den HessenPC wird bei einer Realisierung folgende Features umfassen:

- HP Sure Click (ehemals Bromium)
- Erweiterung des Zentralen Virenschutzes
- HessenPortControl (ehemals Schnittstellenmanagement)
- Aktualisierung von Sicherheitspatches bei B2-Paketen ohne Kundenauftrag
- Einführung von Microsoft Edge

HP Sure Click

Einer der neuen Sicherheitsbausteine des HessenPC 4.0 ist „Bromium Advanced Endpoint Security“ des Herstellers HP Sure Click Enterprise. HP Sure Click ist ein Sicherheitsverfahren, welches es ermöglicht, Anwendungen in einem abgesicherten Modus zu starten. Jeder Prozess kann somit unabhängig und losgelöst laufen. Durch diese Microvir-



tualisierung auf den Arbeitsplatzsystemen wird eine Infektion des Clients verhindert. Folglich wird eine Ausbreitung von Schadsoftware auf das Netzwerk unterbunden. HP Sure Click bietet einen komplementären Schutz vor Ransomware und Advanced Malware und soll vor Bedrohungen schützen, für die es noch keine spezifischen Gegenmaßnahmen gibt. Die Endpoint-Security-Lösung setzt nicht auf Erkennung, sondern auf Isolation. E-Mail-Attachments, Webseiten und Dateien aus unsicheren Quellen werden auf dem PC in einer abgesicherten Umgebung ausgeführt. Damit ist beispielsweise ein Schutz vor Zero-Day Exploits in Anwendungen (MS Office, Adobe Reader usw.) gegeben.

Erweiterung des Zentralen Virenschutzes

Auf dem aktuell ausgerollten HessenPC 3.0 ist mit dem Zentralen Virenschutz (ZVS) ein Standard-Virenschutz auf Basis der McAfee Endpoint Security Platform implementiert. Ergänzt wird diese Lösung durch die zentrale Managementlösung ePolicy Orchestrator. Die neuen Angriffsvektoren können jedoch nur durch neue Schutzmechanismen wie Verhaltensanalyse und lernfähige Schutzsysteme wirksam bekämpft werden, um auch in Zukunft einen wirkungsvollen Schutz zu gewährleisten. Daher gilt es, den bestehenden Virenschutz um Reputations- sowie Analysetechniken zu ergänzen, welche die Lücken zwischen bekannten und unbekanntem Angriffsvektoren soweit wie möglich reduzieren. Dies wird es ermöglichen, Dateien und Programme auf den Arbeitsplatzrechnern vor Schadsoftware zu schützen, selbst wenn diese noch gar nicht bekannt ist. Dafür soll der ZVS um folgende Werkzeuge ergänzt werden:

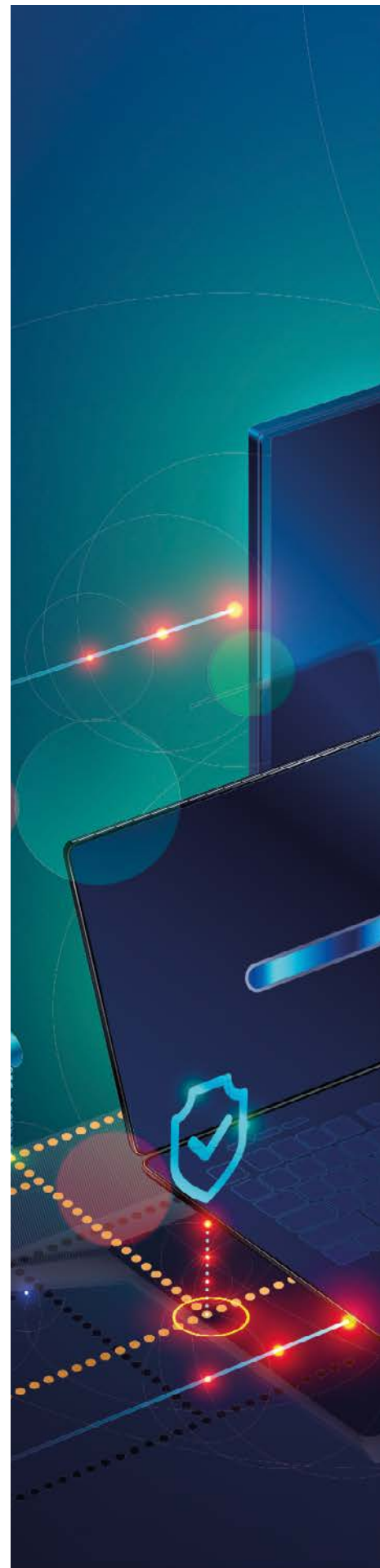
- **Adaptiv Threat Protection** analysiert Dateien und Prozesse, um auf der Basis von Datei-Reputation, Regeln

und Reputationsschwellenwerten zu entscheiden, welche Aktion lokal durchgeführt wird.

- **Threat Intelligence Exchange**; auf dem TIE-Server erfolgt eine weitere Prüfung über die Reputationsdatenbank und - sofern konfiguriert - eine Prüfung via VirusTotal. Neue Erkennungen können den Systemen der Landesverwaltung global bereitgestellt werden.
- **Advanced Threat Defense** kombiniert statische Code-Überprüfung mit dynamischer Analyse und Machine Learning und erstellt innerhalb weniger Minuten eine automatisierte Bewertung anhand einer tiefgreifenden Analyse.
- **Data Exchange Layer** ermöglicht eine Echtzeitkommunikation zwischen Clients und zentralen Schutzkomponenten.

HessenPortControl

Ein weiterer Sicherheitsbaustein ist HessenPortControl für ein zentrales Schnittstellenmanagement auf Basis des Produktes DriveLock. Es ersetzt damit Device Control von McAfee DLP für Endpoint Security. Im ersten Rollout liegt das Augenmerk auf USB-Schnittstellen sowie SD-Slots und CD-/DVD-Laufwerken. Grundsätzlich kann HessenPortControl extern an den Arbeitsplatzrechnern unbefugt angeschlossene Geräte blockieren. Darüber hinaus werden die Daten auf Wechseldatenträgern verschlüsselt. Durch diese Verschlüsselung bietet HessenPortControl Schutz vor unerwünschten Zugriffen und dem Verlust vertraulicher Daten. Zudem erlaubt das Produkt die Protokollierung von Datenübertragungen, sodass bei einem Sicherheitsvorfall oder Verdachtsfall der Abfluss von Daten nachvollzogen werden kann.





Aktualisierung von B-Paketen

Derzeit erfolgt die Bereitstellung und Aktualisierung von Software-Paketen der Kategorie B2 des HessenPC erst nach Beauftragung. Bis dahin besteht über einen längeren Zeitraum das Risiko, dass durch den Einsatz nicht gepatchter Software auf dem HessenPC bekannte, aber nicht geschlossene Sicherheitslücken ausgenutzt werden und erheblicher Schaden entstehen kann.

An die HZD wurde daher die Anforderung formuliert, Aktualisierungen und Patches dieser Software-Kategorie künftig auch ohne direkten Kundenauftrag bereitzustellen. Da Sicherheitspatches zunehmend in Kombination mit Fehlerbehebungen ausgerollt werden, kann die Unterscheidung dieser beiden entfallen und durch ein einheitliches Vorgehen abgelöst werden. Mit einem zentralen Patch-Management und einer regelmäßigen Aktualisierung der B-Pakete kann die HZD Lücken in der Informationssicherheit schließen und das Risiko von Angriffen signifikant reduzieren.

Microsoft Edge

Microsoft hat mit dem aktuellen Major-Release den Browser Microsoft Edge als festen Bestandteil von Windows 10 eingeführt. Dieser neue, Microsoft-eigene Browser nutzt die gleiche Basis-Engine wie Google Chrome und bietet weitere Vorteile, wie z. B. die Möglichkeit, andere Sicherheitsfeatures von Windows 10, etwa die Out-of-the-box-Virtualisierung Application Guard, zu nutzen.

Derzeit wird im HessenPC eine 3-Browser-Strategie verfolgt. Die eingesetzten Browser sind Internet Explorer, Mozilla Firefox und Google Chrome. Doch schon heute gibt es Webseiten, die den Internet Explorer nicht mehr unterstützen und bei denen deshalb auf alterna-

tive Browser ausgewichen werden muss. Sofern Microsoft in der Zukunft den Internet Explorer abkündigt, müsste der HessenPC kurzfristig reagieren. Alle Fachverfahren der Ressorts, die auf dem Internet Explorer basieren, wären dadurch nur eingeschränkt oder gar nicht mehr verfügbar. Zudem ist zu erwarten, dass Softwareentwicklungen, die in Kooperation mit anderen Bundesländern bestehen, ihre Entwicklung zeitnah auf den neuen Browser Edge umstellen.

Ausblick

Das funktionale Gesamtpaket rund um den HessenPC 4.0 mit den neuen Sicherheitskomponenten wurde bereits den relevanten Digitalisierungsgremien (darunter AK Standards und EGOV-VR) vorgestellt. Nach der Anfang des Jahres erfolgten fachlichen Zustimmung der Ressorts zum Gesamtpaket HessenPC 4.0 muss noch die Finanzierung der Einführung, der Lizenzbeschaffung und des Betriebs sowie die geplante Aufnahme ins LEV geklärt werden. Hiernach erfolgen die Detailplanung und die kontinuierliche Abstimmung mit den Ressorts.

Damit werden die stetige Verbesserung und Weiterentwicklung des HessenPC aber nicht abgeschlossen sein. Bereits heute befasst sich die HZD mit der Evaluation weiterer Produkte, z.B. einem neuen Office-Paket, weiteren Online-Konferenz-Tools oder der verbesserten Zugangssicherheit, die das Gesamtpaket des HessenPC in naher Zukunft erweitern werden.



Berislav Kolakovic

Leiter Programmmanagement-Board
HessenPC

berislav.kolakovic@hzd.hessen.de

Länderübergreifender **Support** für die Justiz

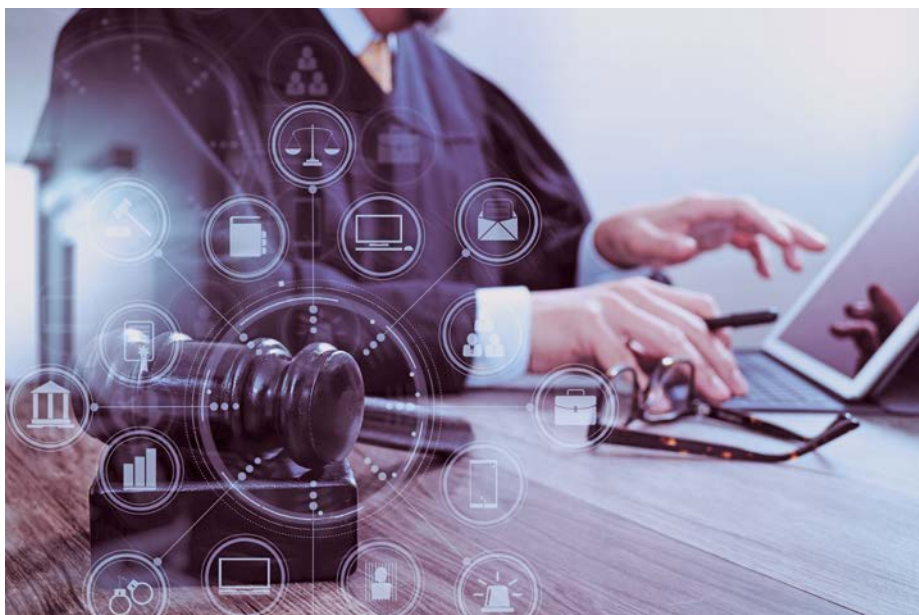
Im gesamtdeutschen Mammutprojekt Elektronischer Rechtsverkehr kommt der HZD seit Beginn des Jahres eine wichtige Rolle zu: Sie verantwortet das zentrale Betriebsmanagement, um in der Zusammenarbeit aller Bundesländer für ein reibungsloses Zusammenspiel der technischen Komponenten zu sorgen.

Damit eine vorwiegend papierlose Kommunikation der Gerichte im Rahmen des Elektronischen Rechtsverkehrs (ERV) sowie die elektronische Aktenführung (eAkte) möglich wird, erarbeiten Bund und Länder rechtskonforme und informationstechnologische Verfahren und Lösungen. Teil dieser Infrastruktur ist das elektronische Gerichts- und Verwaltungspostfach (EGVP) als Kommunikationskanal, genauso aber auch SAFE als zugrundeliegender technischer Standard für das Identity- und Access-Management sowie XJustiz als Datensatz, der den medienbruchfreien Austausch verfahrensbezogener Daten im elektronischen Rechtsverkehr ermöglicht. Um das Zusammenspiel all dieser technischen Komponenten, die zur Realisierung des ERV benötigt werden und die darüber hinaus länderübergreifend betrieben werden, bestmöglich zu planen, zu koordinieren und Testcases sowie die Pflege und den Betrieb von technischen Komponenten strategisch auszurichten, braucht es ein zentrales Betriebsmanagement. Zur Umsetzung dieses zentralen Betriebsmanagements hat die „Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz“ (BLK) am 9. September 2019 ein bundesweites Vergabe-

verfahren gestartet. Auch die HZD hatte sich an der Ausschreibung beteiligt und konnte sich am Ende erfolgreich gegen die Mitbewerbenden durchsetzen. Anschließend hat die BLK-Arbeitsgruppe „IT-Standards in der Justiz“ mit Beschluss vom 11. August 2020 die HZD damit beauftragt, das Betriebsmanagement im Rahmen des Elektronischen Rechtsverkehrs (ERV) wahrzunehmen, das bisher von einem externen Dienstleister übernommen wurde. Durch diese Beauftragung erhält die HZD eine weitere wichtige Rolle im Rahmen der länderübergreifenden Zusammenarbeit in der Justiz.

Von der Problembehandlung bis hin zur Weiterentwicklung

Das ERV-Betriebsmanagement umfasst Leistungen im länderübergreifenden Störungs-, Fehler- und Problemmanagement für die wesentlichen technischen Schlüsselkomponenten des Elektronischen Rechtsverkehrs. Das reicht von einem vergessenen Passwort über eine User-Freischaltung bis hin zur Fehlerfindung in einem System, an dem mehrere unterschiedliche Bundesländer, Verfahren und Systeme beteiligt sind. Weiterhin zählen die länderübergreifende Zusammenarbeit und Koordination sowie die Weiterentwicklung und Optimierung bestehender Prozes-



se und Tools zu den zentralen Aufgaben. Dies umfasst auch die Funktion als Clearingstelle, die über die Schlüsselkomponenten hinaus auch die im ERV eingesetzten Drittprodukte berücksichtigt. Auf diesem Weg eröffnen sich für die HZD Möglichkeiten, die bisherigen Erfahrungen und Erkenntnisse aus bereits abgeschlossenen Projekten im Kontext des Gesamtvorhabens zur Umsetzung des Elektronischen Rechtsverkehrs einzubringen. Mit bereits etablierten Tools und Prozessen aus dem Umfeld der Entwicklung und des Releasemanagements leistet die HZD einen wichtigen Beitrag, um die gesamte Handhabung zunehmend transparent und einheitlich zu gestalten.

Gemeinsam mit der Bund-Länder-Kommission

Zur Erfüllung dieser komplexen Aufgaben stellt die HZD ein fünfköpfiges Betriebsteam bereit, das sich seit Januar 2021 im Aufbau befindet und in der Außenstelle Hünfeld ansässig ist. Es nimmt die übertragenen Aufgaben in enger Zusammenarbeit mit der BLK-AG „IT-Standards“ wahr und agiert als Teil des zur AG gehörenden Projektbüros. Ansprechpartner*innen des Teams nach außen sind in erster Linie die ERV-Verantwortlichen des Bundes und der Länder, können aber – einhergehend mit

den zuvor genannten Aufgaben – bis zu den Herstellern von Fachverfahren spezifischer Software reichen. In einem ersten Schritt geht es seit Anfang 2021 darum, die Aufgaben des bisherigen Dienstleisters zu übernehmen. Bedingt durch den weiterhin schnell wachsenden ERV – beispielsweise die bevorstehende Einführung des besonderen Bürger- und Organisationenpostfachs (eBO) bis Ende des Jahres und die am 1. Januar in Kraft tretende Nutzungspflicht des besonderen elektronischen Anwaltspostfachs (beA) für Rechtsanwälte – werden im weiteren Verlauf verschiedene Anpassungen von Tools und Prozessen notwendig werden. Um dies zu erreichen und gleichzeitig die hohe Qualität der zu liefernden Services aufrechtzuerhalten und zu verbessern, werden die über Jahre gesammelten Erfahrungen aus dem e²-Verbund – also dem Zusammenschluss der Länder Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Saarland, Sachsen-Anhalt und des Bundesarbeitsgerichts – elementar sein.



Mike Dilling
Rolloutmanagement,
Betrieb dezentrale Fachverfahren
mike.dilling@hzd.hessen.de

”

Mit der Übernahme des ERV-Betriebsmanagements hat die HZD einen wichtigen Auftrag für die bundesweite Justiz übernommen. Im länderübergreifenden Vorhaben des Elektronischen Rechtsverkehrs kommt ihr bei der Problemlösung im Fehlerfall eine koordinierende Funktion zu.“

Hans-Georg Ehrhardt-Gerst

Leiter der Abteilung J sowie der HZD-Außenstelle in Hünfeld

Der Mensch als **Schlüssel-** **element** für Informationssicherheit

HZD startet unter dem Motto #stayaware eine umfassende interne Security Awareness-Kampagne

Informationssicherheit

Umfassender Begriff, da auch die Sicherheit von nicht elektronisch verarbeiteten Informationen betrachtet wird.



Cyber-sicherheit

Das Aktionsfeld der IT-Sicherheit wird auf den gesamten Cyber-Raum ausgeweitet



IT-Sicherheit

Sicherheit der IT-Systeme



Was ist Informationssicherheit und aus welchen Komponenten besteht sie?

Auch wenn die Wahrheit weh tut, ein Großteil von Computern und Netzwerken wird heute durch rücksichtsloses und kriminelles Ausnutzen von Hilfsbereitschaft, Freundlichkeit und Anteilnahme wohlmeinender Menschen kompromittiert. Ein getarnter Link in einer E-Mail, vorgeblich vertrauenswürdige Social-Media-Accounts, die zur verdeckten Installation von Malware führen, vorsätzlich betrügerische Anrufe unter Vorspiegelung falscher Tatsachen, um sich Zugangsdaten zu erschleichen – all das passiert heute täglich in deutschen Unternehmen, Institutionen und bei Privatanwender*innen.

Kaum jemand wird heute noch den Stellenwert der Automatisierung und Digitalisierung von Prozessen und Aufgaben bezweifeln. Und dass diese Entwicklungen unumkehrbar sind, haben mittlerweile auch jene verstanden, die noch vor Jahren naserümpfend auf die ersten Digitalisierungswellen geschaut haben. Beides erfasst und verändert intensiv unsere Lebenswirklichkeit, und das wird auch in exponentiellem Tempo weiter zunehmen. Mit starren und langwierigen Prozessen wird man mit der sich rapide ändernden Welt nicht mehr Schritt halten können. Ein Umdenken zu schnellen, flexiblen und agilen Prozessen, Mindsets und Geschäftsmodellen ist nötig. Die Kehrseite der Vorteile der Automatisierung und Digitalisierung, z.B. jederzeit schnell und effizient auf Informationen zugreifen zu können, sind gesteigerte Anforderungen an die Cybersicherheit und den Datenschutz.

Im Rahmen einer ISO 27001 Zertifizierung auf Basis von BSI-Grundschrift¹ hat sich rund um den Informationssicherheitsbeauftragten der HZD, Dr. Arno Domack, ein schlagkräftiges Expert*innen-Team gebildet, das sich die Erarbeitung und Durchführung von erfolgreichen Security Awareness Kampagnen auf Basis modernster Erkenntnisse von Angriffs- und Abwehrszenari-

en auf die Flagge geschrieben hat. Das Ziel dieser Kampagnen soll es sein, Mitarbeiter*innen der HZD zielgruppenspezifisch zu den wichtigen Themen der Informationssicherheit und des Datenschutzes zu informieren, zu stärken und zu sensibilisieren.

Awareness für die Awareness erzeugen

Um herauszufinden, wie gut sich die HZD-Mitarbeiter*innen bereits mit den verbundenen Themen der Informationssicherheit auskennen, hat das Spezialist*innen-Team der Awareness-Kampagne mit sorgfältig ausgewählten Fragen eine SharePoint-Umfrage durchgeführt. Anhand der Umfrageergebnisse konnten die Inhalte der Kampagne so gestaltet werden, dass sich die Mitarbeiter*innen einerseits in ihren Vorstellungen der Abwehr von Cyberangriffen bestätigt fühlen, andererseits ihre Handlungs- und Interventionsmöglichkeiten erweitern. Der richtige Einstieg bei einer solchen Kampagne ist der Schlüssel für die Akzeptanz und die gezielte Weiterentwicklung bei den Beschäftigten.

Zum Auftakt der Kampagne gab es zwei Basisveranstaltungen für die komplette Belegschaft, die in Zusammenarbeit und mit der Expertise der Datenschutzbeauftragten der HZD Gundula Bucsa und ihrer Vertretung Dr. Ute Hellwig entwickelt wurden. Denn auch wenn Informationssicherheit heute in aller Munde ist, übersehen viele, dass das Themengebiet des Datenschutzes über die Datensicherheit unumstößlich mit der Informationssicherheit verbun-

¹ Die BSI-Standards enthalten Methoden und Vorgehensweisen zu den unterschiedlichsten Themen aus dem Bereich der Informationssicherheit und stellen mit dem IT-Grundschrift-Kompodium einen De-Facto-Standard für die Informationssicherheit dar.



Security Awareness – was ist das überhaupt?

Awareness beschreibt in erster Linie eine Bewusstheit und ist eine Betonung der aktiven Handlung, sozusagen eine Form der Aufmerksamkeit. Security Awareness erweitert diese Definition zur notwendigen Sensibilisierung von Mitarbeiter*innen für Themen rund um Informationssicherheit und Datenschutz, um potenzielle Sicherheitsbedrohungen aufzuzeigen und zu vermeiden.

Warum funktioniert Informationssicherheit nicht ohne Datenschutz?

Informationssicherheit und Datenschutz teilen sich das Anwendungsgebiet des Schutzes persönlicher Daten. Das Anwendungsgebiet der Informationssicherheit unterscheidet hingegen nicht zwischen natürlichen und juristischen Personen.

Kennen Sie die wichtigsten Achtsamkeitshinweise?

- Sperren Sie immer Ihren PC, wenn Sie Ihren Arbeitsplatz verlassen (auch wenn es nur zwei Minuten sind).
- Ändern Sie unbedingt Ihr Bitlocker-Passwort.
- Dokumente, Unterlagen und Notizen sind immer in abschließbaren Schubladen oder Schränken aufzubewahren.

#StayAware



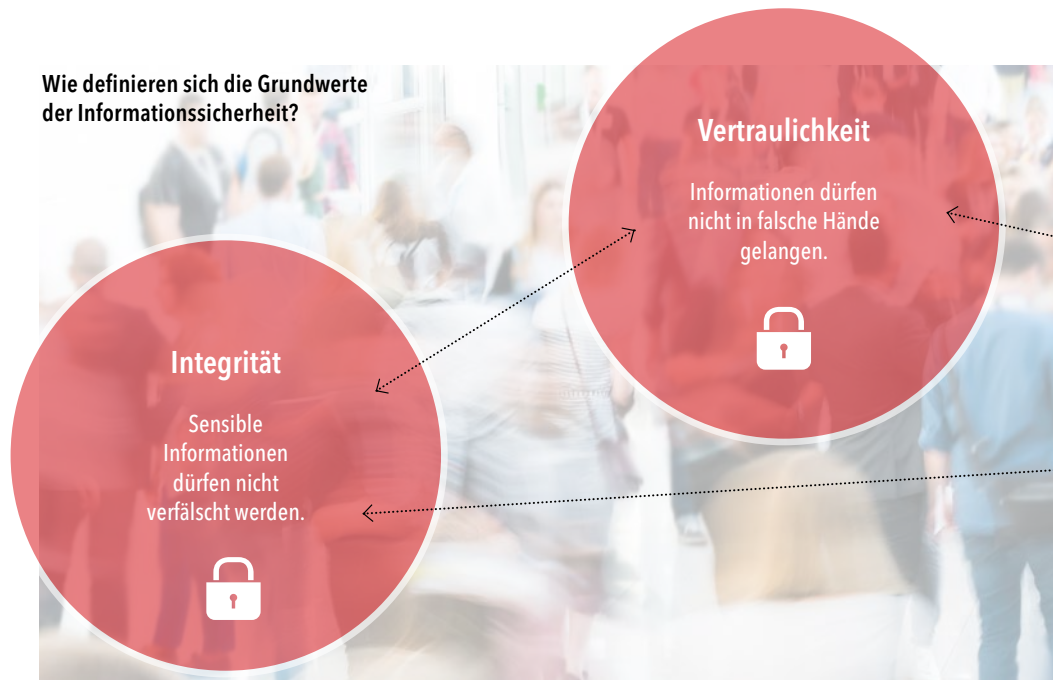
”

Langweilige Folien oder verklausulierte Schulungsunterlagen sprechen uns schon lange nicht mehr an, verfehlen mitunter sogar ihre Wirkung und lassen die Brisanz für das Thema Security Awareness übersehen oder gar vergessen. Die Awareness-Kampagne erreicht die Beschäftigten über vielfältige Kommunikationskanäle wie Web-based-Trainings, Webinare und gänzlich neue Formate.“

Lisa Reinhardt

Security Awareness Koordinatorin

Wie definieren sich die Grundwerte der Informationssicherheit?



den ist. Wussten Sie zum Beispiel, dass jeder Datenschutzvorfall auch ein Informationssicherheitsvorfall ist? Umgekehrt ist aber nicht jeder Informationssicherheitsvorfall ein Datenschutzvorfall!

Zielgruppenspezifisch und aktuell

Von Januar bis Anfang April 2021 konnte die Informationssicherheitskoordinatorin Lisa Reinhardt insgesamt ca. 1.000 Beschäftigte für die wichtigsten Aspekte der beiden Themengebiete sensibilisieren. Damit wurde der Grundstein im facettenreichen Gebiet der Security Awareness gelegt. Künftig werden zielgruppenspezifische Inhalte genauso wie aktuell relevante Themengebiete vertieft: Erkennung möglicher Angriffsszenarien, akute Gegenmaßnahmen und proaktive Verhaltensweisen, verinnerlichte Prozessabläufe, aber auch Wissensauffrischungen zu datenschutzrelevanten Themen wie die sichere Verarbeitung personenbezogener Daten oder das wichtige Themengebiet der Passwörter.

In den aktuellen Zeiten rückt das Thema Homeoffice immer weiter nach oben auf der Agenda und damit auch der Punkt, wie wir sicher zu Hause arbeiten können. Denn grundsätzlich gelten natürlich die Sicherheitsmaßnahmen, die am Arbeitsplatz vor Ort getroffen werden, auch für den heimischen Arbeitsplatz. Beispielsweise

müssen Geräte bei Nichtnutzung sicher aufbewahrt oder gesichert sein. Ebenso dürfen Außenstehende keinen Zugriff auf unternehmensrelevante Daten haben. Nicht nur im Büro, sondern auch zu Hause sind IT-Sicherheitsvorfälle denkbar.

Die HZD kümmert sich verlässlich um die technische Sicherheit und systemseitig können bereits zahlreiche Betrugsversuche abgefangen werden. Trotzdem sollte jedem bewusst sein, dass auch die beste Technik keine hundertprozentige Garantie dafür ist, arglos mit den Themen rund um Informationssicherheit umzugehen: Es gibt mittlerweile ganze kriminelle Industriezweige, die auf arglose, freundliche Mitarbeiter*innen setzen, um ihre schädlichen Ziele zu erreichen.

Social Engineering

Mit der HZD #stayaware Security Awareness-Kampagne legt die HZD einen besonderen Fokus auf die Vermittlung von Inhalten rund um die zwischenmenschliche Beeinflussung, im modernen Sprachgebrauch auch Social Engineering genannt. Während einer Awareness-Woche wurden beispielsweise täglich Videoclips im Mitarbeiterportal (MAP) veröffentlicht, die praktische Tipps und Tricks an die Hand geben, wie denn eigentlich den sogenannten „Social Engineers“ auf die

Informationssicherheit hat das Ziel, Informationen jeglicher Art und Herkunft zu schützen. Dabei können Informationen sowohl auf Papier, in Rechner-Systemen aber auch in den Köpfen der Menschen gespeichert sein.

Verfügbarkeit

Notwendige Informationen müssen abrufbar sein.



Schliche gekommen werden kann, woran eine Phishing-Mail erkennbar ist oder wie manipulierte Absender-Adressen von E-Mails ermittelt werden können. Die Resonanz zeigt, wie akut und brisant dieses Themenfeld ist.

Diese und viele weitere Themen werden während des gesamten Jahres 2021 aufbereitet und in wechselnden Formaten vermittelt. Denn die Themen rund um Awareness für Informationssicherheit müssen dauerhaft in den Unternehmensalltag integriert werden und dürfen künftig nicht außer Acht gelassen werden.

➔ Wir freuen uns sehr über das rege Interesse in der HZD, über den kritischen Austausch mit den Beschäftigten und die vielen Anfragen aus der Landesverwaltung und stehen auch für Sie, liebe Leser*innen, als Ansprechpartner*innen gerne zur Verfügung.

Lisa Reinhardt, Security Awareness Koordinatorin

Dr. Ute Hellwig, Informationssicherheitsmanagement

Vladimir Schewelew, dualer Student im kooperativen Studiengang IT-Sicherheit an der Hochschule Darmstadt

Dr. Arno Domack, Informationssicherheitsbeauftragter der HZD

➔ E-Mail: awareness@hzd.hessen.de



Beantworten Sie diese Fragen richtig?
Achtung! Es kann mehr als eine Antwort richtig sein!

1. **Was wird im Bereich der Informationssicherheit unter einem Restrisiko verstanden?**
 - a Ein nach der Bedrohung verbleibendes Risiko
 - b Ein Risiko, für das entschieden wurde, dass es akzeptiert werden kann
 - c Ein inhärentes Risiko, für das es keine Risikobehandlung gibt
 - d Ein Risiko, das im Rahmen der Risikoanalyse nicht weiter betrachtet wird
2. **Welche dieser Daten sind besondere Kategorien personenbezogener Daten?**
 - a Krankheit
 - b Religion
 - c Gewerkschaftszugehörigkeit
 - d Adresse

(Auflösung der Fragen auf Seite 50)

”

Wir setzen auf befähigte Mitarbeiterinnen und Mitarbeiter, die die kriminellen Machenschaften von Hackern kennen, erkennen und beurteilen können, die auffällige Indizien feststellen und melden, die solche Angriffsversuche frühzeitig blockieren und wie von selbst in ihre Verhaltensweisen und Prozessabläufe integrieren.“

Dr. Arno Domack

Informationssicherheitsbeauftragter der HZD

FISBOX®

mit neuen Features

Die FISBOX® ist der Trumpf der HZD für Fachinformationssysteme. Mit fast 50 Fachverfahren ist sie im Land und in den Kommunen im Einsatz. Und fast monatlich kommen neue Anwendungen oder Überführungen aus veralteten IT-Systemen hinzu. Ihr absoluter Vorteil: Die FISBOX® wird stets den Anforderungen entsprechend bedarfsgerecht ausgerichtet und schnell eingesetzt. Das HZD-Team entwickelt sie außerdem zur Komplettlösung für die Digitalisierungsstrecke vom Antrag über das Backend zur Veraktung weiter. Das neuste Ass im Ärmel: die Überführung digitaler Anträge mit HessenDante in die FISBOX® entsprechend den Vorgaben des Onlinezugangsgesetzes und der Digitalen Modellbehörde. Die neue Anwendung LAFE für das Sozialministerium zeigt, was die FISBOX® kann.

Das hessische Landesprogramm „Fachkräfteoffensive Erzieherinnen und Erzieher“ fördert im Wesentlichen den Ausbau praxisintegrierter Ausbildungsplätze sowie Anleitungsfreistellungen durch pädagogische Fachkräfte. Mögliche Antragsteller sind die mehr als 2.200 Träger der hessischen Kindertageseinrichtungen.

Die Anforderungen an ein entsprechendes Fachinformationssystem zur Bearbeitung und Dokumentation der gestellten Anträge konnte die HZD auf Basis der FISBOX®-Standards umfassend und schnell erfüllen. Durch die standardisierte Schnittstelle der FISBOX® an die Onlineantragskomponente HessenDante kann das Antragsverfahren seit Oktober 2020 vollständig online abgebildet werden. Die digitale Übernahme der Antragsdaten und notwendiger Anlagen zu den Anträgen (z.B. in Form von Nachweisen und Bestätigungen aus Webformularen) in das FISBOX®-Fachinformationssystem LAFE (Landesprogramm Fachkräfteoffensive Erzieherinnen und Erzieher) hat die HZD erfolgreich umgesetzt. Somit wer-

den die Zielvorgabe des Onlinezugangsgesetzes (Bereitstellung von Online-Services für Bürger*innen und Unternehmen) als auch die Anforderungen der Digitalen Modellbehörde erfüllt.

Während der Eingabe der Antragsdaten in das Onlineantragsformular werden u.a. antragstellende Träger und die jeweils zugehörigen Kindertagesstätten bereits mit der FISBOX® auf Gültigkeit und Plausibilität abgeglichen. So ist nicht nur die Möglichkeit der Eingabe fehlerhafter Angaben minimiert, sondern auch die Anzahl an Stammdaten, die im Rahmen einer Antragstellung eingegeben werden müssen weitestgehend reduziert worden.

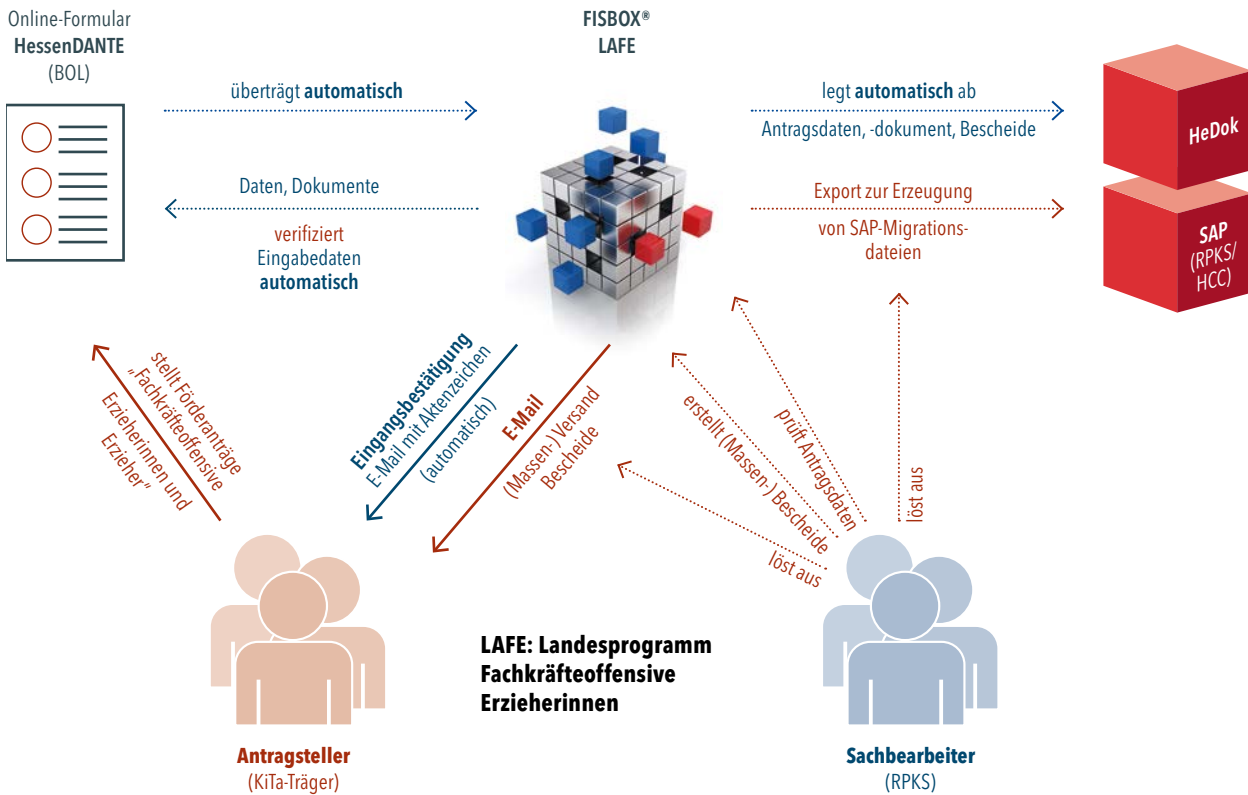
Der Antragstellende erhält nach der Eingabe der Antragsdaten aus der FISBOX® heraus eine automatisierte Bestätigung per E-Mail mit einer individuellen Referenznummer zum jeweiligen Antrag. Sobald die Förderfähigkeit durch das Regierungspräsidium Kassel festgestellt wird, erzeugt die FISBOX® auf Knopfdruck den entsprechenden Bescheid und stellt diesen dem Antragstellenden per E-Mail direkt zu. Die



Neue FISBOX®-Features für 2021 und 2022

- Speichermodul SharePoint
- Schnittstelle HessenDrive
- Schnittstelle E-Payment
- Schnittstelle Rückkanal
- Einbindung von Excel-Vorlagen in den Auswertemanager (Grafiken/Diagramme)
- Schutzbedarf hoch / sehr hoch (Schutzziel Vertraulichkeit)
- PDF-Erstellung (mit Druckstraßenkonformität)
- 2-Faktor-Authentisierung
- Maßnahmen zur Verbesserung der Barrierefreiheit
- Technische Modernisierung (Migration auf .NET 5/6)





**LAFE: Landesprogramm
Fachkräfteoffensive
Erzieherinnen**

Auszahlung der Fördermittel wird durch die Bereitstellung der Buchungs- und Auszahlungsinformationen für jeden Zahlungslauf individuell aus der FISBOX® heraus unterstützt, ebenso wie die jährlichen Rechenschaftsberichte für den Hessischen Rechnungshof nach § 44 LHO.

Aktuell geht das Sozialministerium den letzten noch verbleibenden Schritt zur Volldigitalisierung des Gesamtverfahrens: die automatisierte Anlage von Vorgängen zur Ablage der Anträge und Dokumente des Förderverfahrens in HeDok, dem Dokumentenmanagementsystem (DMS) der hessischen Landesverwaltung. Die zum Einsatz kommende HeDok-Schnittstelle der FISBOX® richtet die HZD derzeit ein.



Manfred Schehr
Produktmanager FISBOX®

manfred.schehr@hzd.hessen.de



Manuel Hoffrichter
Projektleiter FISBOX®

manuel.hoffrichter@hzd.hessen.de



Die HZD hat uns auf Basis der FISBOX® innerhalb kürzester Zeit ein Tool für die Abwicklung eines Massenförderverfahrens in Form eines vollständigen Fachinformationssystems zur Verfügung gestellt. Das Projektmanagement hat uns von Anfang an kompetent beraten und LAFE entsprechend unserer Bedarfe hin zu einem Onlineantragsverfahren weiterentwickelt. Das Besondere an LAFE ist, dass innerhalb dieser IT-Fachanwendung das komplette Förderverfahren abgebildet ist: von der Entgegennahme verifizierter Anträge aus einem Onlineformular für die Sachbearbeitung über den elektronischen Versand der Bescheide bis hin zur Unterstützung der Auszahlung der Fördersummen. Mit LAFE haben wir ein Produkt erhalten, das eine zügige Umsetzung des Förderverfahrens auf Seiten der Landesverwaltung garantiert und dessen Onlineantrag im Handling für die Antragstellenden einfach und übersichtlich ist.“

Dr. Christian Peter

Referatsleiter Jugend, Jugendhilfe im
Hessischen Ministerium für Soziales und Integration

Blacklisting

bei Massen-E-Mails vermeiden

Beim Versand von Massen-E-Mails¹ (z.B. Newsletter) können mitunter Probleme bei der Zustellung auftreten, vor allem wenn es sich um Empfänger*innen privater Provider (z.B. web.de, gmx, telekom etc.) außerhalb der Domäne hessen.de handelt. Grund dafür können sogenannte Blacklists der entsprechenden Provider sein.



1. Anzahl E-Mails

10.000 und mehr „normale“ E-Mails an die großen Provider wie web.de oder gmx sind im Tagesbetrieb durchaus üblich. Kommt zusätzlich noch ein Massen-E-Mail-Versand hinzu, kumulieren diese Zahlen. Das kann dazu führen, dass die Provider bei Überschreitung des Schwellwertes für einen vorübergehenden Zeitraum keine E-Mails von den Mail-Servern der Domäne hessen.de mehr empfangen.

Es ist daher ratsam, E-Mails an einen Verteiler mit mehreren 100 Empfänger*innen nicht in den üblichen Geschäftszeiten zu versenden, sondern bewusst auf Zeitfenster außerhalb auszuweichen. Darüber hinaus sollten keine Verteiler mit mehr als 100 Empfänger*innen einer gleichen Domäne (z.B. web.de) erstellt werden. Es ist besser, mehrere Verteiler zu nutzen und den Versand zeitverzögert zu steuern.

2. Links in E-Mails

Das Einfügen von Links in Massen-Mails führt generell dazu, dass diese als gefährlich eingestuft werden. Wenn möglich, sollte auf die Angabe von Links verzichtet werden. Insbesondere HTTPS-Links, die auf eine nicht HTTPS-fähige Webseite verweisen und Links mit mehr als 125 Zeichen, automatischen Authentifizierungsangaben oder Domänen zweifelhaften Ursprungs werden oft als gefährlich eingestuft.

3. E-Mail-Anhänge

E-Mail-Anhänge sollten bei Massen-E-Mails prinzipiell vermieden werden. Ist das nicht möglich, dann sollten die Anhänge möglichst klein sein und keine aktiven Inhalte haben. Vor allem Microsoft-Office-Dokumente (doc, docx, xls, xlsx, ppt, pptx, ...) sollten nicht angehängt werden.

4. Datenschutz

Erhalten Empfänger*innen Massen-E-Mails unangefordert oder ohne einen bereits bestehenden Kontakt zur Dienststelle, werden solche E-Mails fast immer als SPAM-Mails angesehen. Das führt eventuell zu Beschwerden, in der Regel beim Datenschutzbeauftragten. Vor dem Versand einer Massen-Mail sollten daher unbedingt die datenschutzrechtlichen Rahmenbedingungen geklärt und auf bestehende An- oder Abmeldemöglichkeiten hingewiesen werden.

5. Empfänger-Adressen

Der Verteiler sollte stets aktuell sein. Denn: Provider wie t-online.de sperren den Empfang von Massen-E-Mails auch dann, wenn ein bestimmter Anteil der Empfänger-Adressen falsch oder nicht vorhanden ist. Hierdurch sollen per Generator erstellte E-Mails unterbunden werden. Diese versuchen anhand eines Namenslexikons eigentlich unbekannte Empfänger*innen zu adressieren und scannen somit Empfängerlisten einer Domäne.

Viele Provider betreiben technische Sicherheitsmaßnahmen zum Schutz ihrer eigenen Infrastruktur und der Empfänger*innen vor ungewollten E-Mail-Zustellungen wie SPAM-Mails oder massenhaften Werbe-Mails. Die Sicherheitsmaßnahmen reagieren auf bestimmte Parameter der Mails. Die meisten Provider orientieren sich bei der Festlegung und Interpretation der Parameter an sogenannten Blacklists. Wird gegen diese verstoßen, kann es sogar vorkommen, dass eigentlich erwünschte E-Mail-Zustellungen ebenfalls abgelehnt werden. Auch E-Mails aus der Domäne hessen.de sind in jüngster Zeit wiederholt davon betroffen gewesen. INFORM erläutert deshalb die gängigsten Blacklists der Provider und gibt Empfehlungen, wie man ein Blacklisting für E-Mails des Landes vermeiden kann.

¹ Von Massen-E-Mails zu unterscheiden und hier nicht gemeint sind E-Mails, die ein E-Mail-Absender innerhalb der Domäne hessen.de an Empfänger*innen innerhalb der Domäne hessen.de versendet (z.B. Anschreiben an alle Beschäftigten des Ressorts). Aber auch hier schadet es nicht, die Empfehlungen zu beachten.



Jackpot!

Eines Nachts im August 1995 erzittern die Mauern einer Bankfiliale im verschlafenen Städtchen Saarmund, als ein LKW rückwärts in das Schaufenster der Bank fährt. Zwei Gestalten springen aus dem LKW, um den Geldautomaten zu klauen. Sie binden ein Stahlseil um das freistehende Gerät, das sie mithilfe des Lasters aus der Verankerung reißen und mitnehmen. Etwas später müssen sie mit sehr viel Bedauern feststellen, dass sie den Kontoauszugsdrucker statt des Geldautomaten erwischt haben. – Die meisten Hacker stellen sich i.d.R. deutlich geschickter an!

Beim sog. Skimming versuchen Hacker an die PIN Ihrer Bankkarte zu kommen. Früher wurde das über einen Kartenleser gemacht, der vor den Eingabeschlitz des Bankomat-Lesegeräts gebaut wurde. Heutzutage wird ein USB-Sniffer ins Gerät selbst eingesteckt. Die abgegriffenen Daten können einfach über ein handelsübliches Lese-/Schreibgerät auf eine Leerkarte übertragen werden.

Ein Geldautomat ist im Grunde simpel aufgebaut: Er besteht aus den Mensch-Maschine-Interfaces, einem Tresor mit angeschlossener Mechanik für die Geldausgabe und einem Computer als zentraler Steuereinheit. Alles wird durch eine mechanisch gesicherte Abdeckung gekapselt. Die Preise für solche Automaten rangieren zwischen 20.000 und 200.000 Euro. Leider wird bei einem günstigen Gerät gespart, wo es nur geht. Deshalb werden hier i.d.R. ganz herkömmliche Consumer-Notebooks verbaut, die den gleichen sicherheitstechnischen Problemen wie alle anderen Geräte dieser Klasse unterliegen: Sie sind schlecht gewartet und daher sehr einfach angreifbar. Der Sicherheitsspezialist Kaspersky hat 2016 eine Statistik über die Verwendung von Windows XP bei Bankautomaten-Computern erstellt und kam zwei Jahre nach Support-Ende immer noch auf eine Quote von 90 %!

Ein Hacker benötigt damit nur noch einen Zugang zum System, um hier jede Menge offener Sicherheitslücken auszunutzen. Der Zugang wird ihm entweder über Wartungs-Schnittstellen an der Rückseite des Gerätes geboten oder er nutzt einen Generalschlüssel, um die Abdeckung zu öffnen. Hier wird alles an Schnittstellen geboten, was das Hacker-Herz begehrt: USB, RJ45, etc. Den Generalschlüssel gibt es für einige tausend Dollar im Darknet zu kaufen. Das ist jedoch meist nicht notwendig. Bei www.shodan.io werden unter dem Begriff ATM¹ alle bekannten Geldausgabegeräte mit offenkundigen Systemschnittstellen gelistet. Die Angriffsmöglichkeiten sind vielfältig:

- Per ARP-Spoofing wird vorgegaukelt, selbst das Bank-Bearbeitungszentrum zu sein und Geldausgaben angewiesen werden.
- Als MITM² kann man bei fehlender TLS-Verschlüsselung Transaktionen abfangen, eine Wartungsmeldung auf dem Display lancieren, die Transaktion abschließen und das Geld kassieren, wenn der Kunde gegangen ist.
- Mit Blackboxing wird ein im Darknet erworbenes RaspberryPi-Gerät genutzt, das über USB mit dem System verbunden wird. Die hierauf verwendete Software kontrolliert die Geldkassette des Automaten. Auszahlungsanweisungen können bequem über das Handy übermittelt werden. Das Gleiche funktioniert mit per USB eingeschleuster Malware, die ebenfalls über das Darknet erworben wird.

Für diese als *Jackpotting* bezeichneten Varianten des Bankbetrugs muss man kein IT-Fachmann sein. Dabei zeigt sich wieder einmal deutlich, dass auch hier das Thema IT-Sicherheit nicht ernst genug genommen wird.

¹ Automated Teller Machine

² Man-In-The-Middle



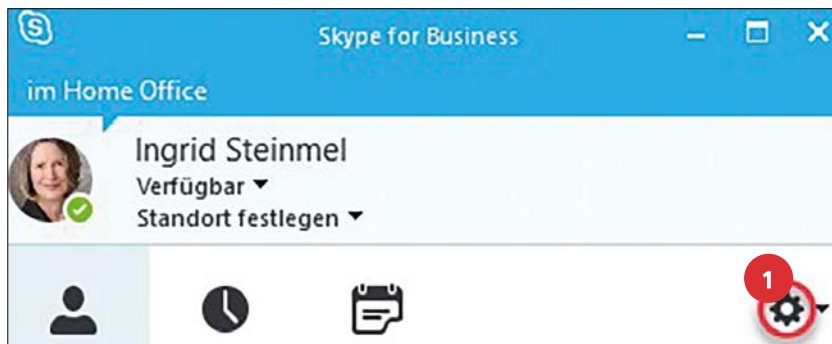
Albrecht Weiser
SecurityTest Service
Teletrust Information Security Professional (TISP)

albrecht.weiser@hzd.hessen.de

Souverän

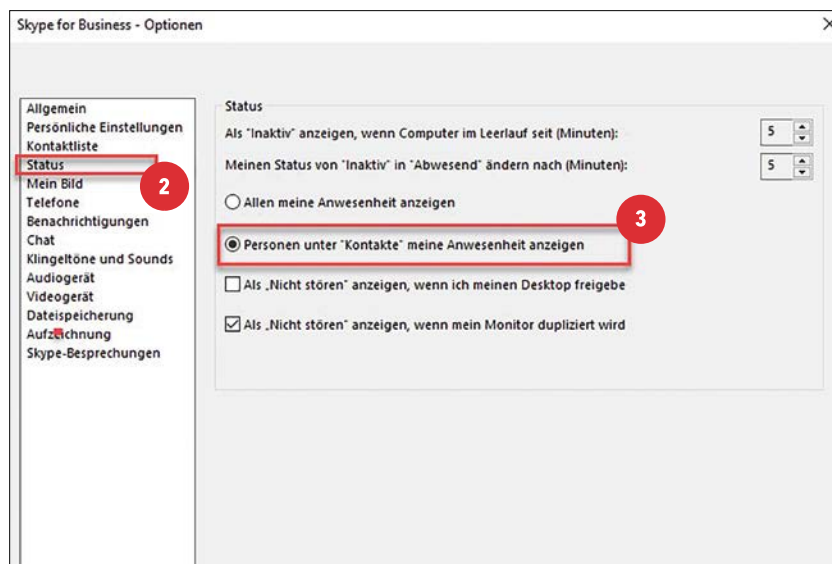
mit der Statusanzeige in HessenConnect umgehen

Jetzt, wo viele von uns zu Hause arbeiten, nutzen wir HessenConnect, um „online“ zu chatten, zu telefonieren, an Sitzungen oder auch an Seminaren teilzunehmen. Da kann es nicht schaden, sich mit dem Onlinekonferenz-Werkzeug gut auszukennen. Vielleicht haben Sie sich schon gefragt, wie die Statusmeldungen in HessenConnect zustande kommen. Unser Tipp beschäftigt sich dieses Mal genau mit dieser Frage.



Bei der Installation des Clients ist der sog. „Privacy Modus“ bereits als Default eingestellt. Das können Sie sehen, wenn Sie:

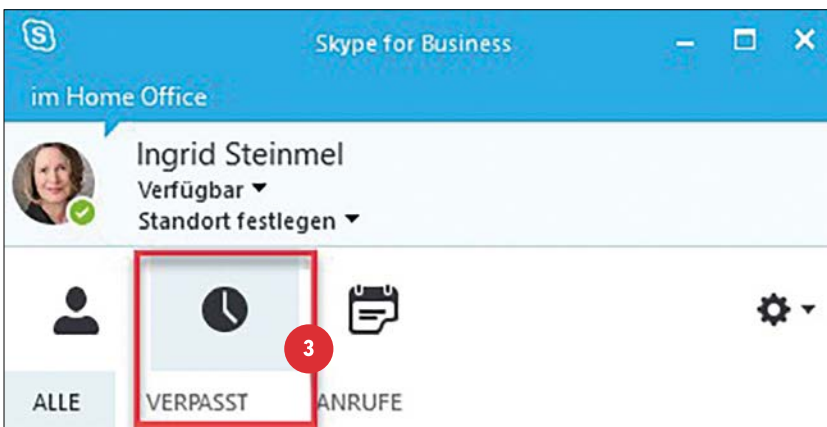
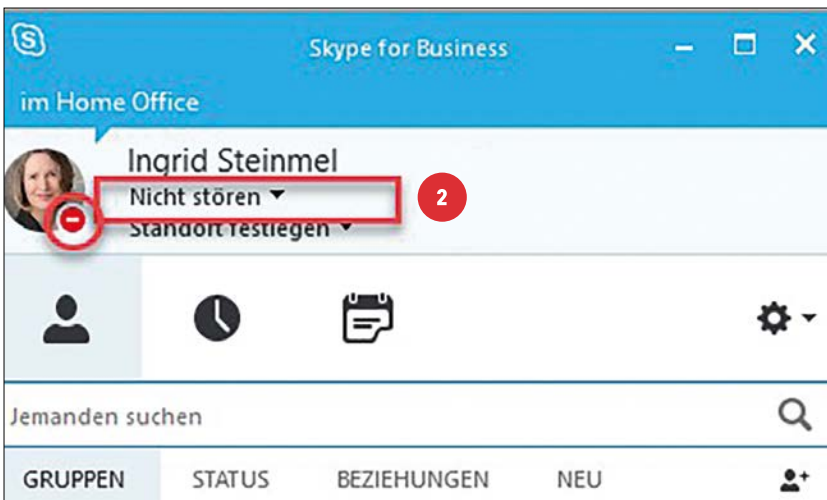
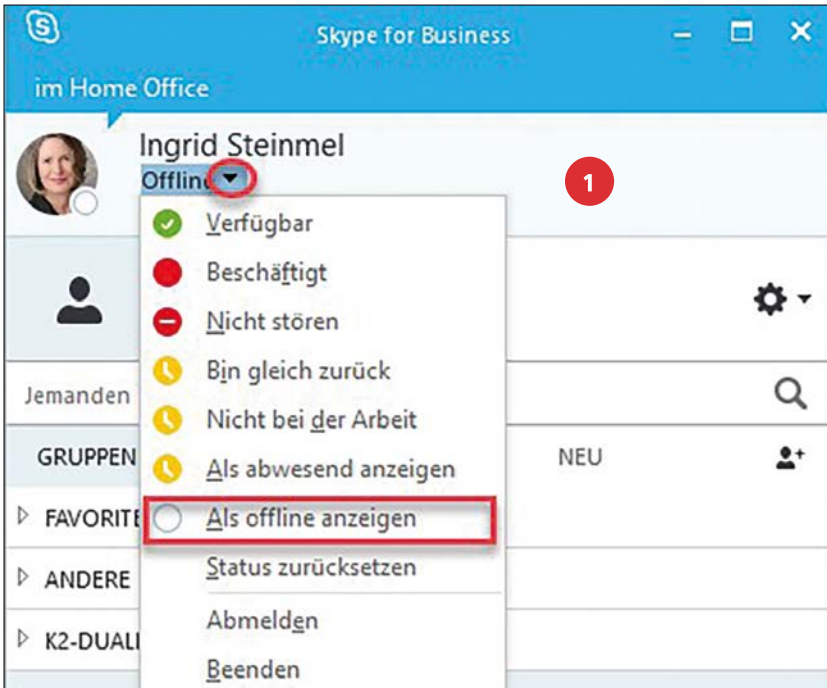
1. in der Skype for Business App das Zahnrad anklicken und danach
2. im Optionen-Fenster das Menü „Status“ öffnen.
3. Dort sollte der gezeigte Eintrag für den sog. „Privacy Modus“ ausgewählt sein.



Der Privacy Modus stellt sicher, dass nur Mitarbeiter*innen, die sich gegenseitig in HessenConnect in einer Kontaktliste führen, ihren aktuellen Status einander übermitteln.

Wenn nur eine Seite eine Kontaktperson in eine HessenConnect-Kontaktliste aufgenommen hat, bleibt die gegenseitige Statusanzeige bei „offline“.

Sie möchten gut erreichbar sein? Dann sollten Sie hier den Eintrag „Allen meine Anwesenheit anzeigen“ in der darüber liegenden Zeile auswählen. In diesem Fall können alle Mitarbeiter*innen im hessischen Landesnetz Ihren Status sehen, sofern sie in HessenConnect nach Ihnen suchen.



Die Statusmeldungen selbst werden in HessenConnect nach verschiedenen Kriterien automatisch gesetzt. Sie können jederzeit diesen automatischen Status **manuell überschreiben**, indem Sie das Drop-down Menü öffnen:

1. Hier können Sie beispielsweise „Als offline anzeigen“ auswählen. Danach werden Sie bei allen Kontakten als „Offline“ angezeigt. Trotzdem können Sie HessenConnect für Chats und Anrufe weiterhin nutzen und auch von anderen Anwender*innen erreicht werden.

2. Aber vielleicht möchten Sie sicherstellen, dass Sie während einer Präsentation nicht durch Chats und Anrufe gestört werden? Kein Problem: Sie wählen den Status „Nicht stören“ aus und bekommen dann keine Chats oder Anrufe mehr angezeigt. Übrigens: Wenn Sie in einer HessenConnect-Sitzung den Präsentationsmodus nutzen, wird dieser Status auch automatisch mit dem Text „Hält Präsentation“ eingestellt.

3. Die verpassten Anfragen können Sie anschließend sehen, wenn Sie das Uhr-Symbol und dort den Reiter „VERPASST“ anklicken.

Viel Erfolg bei der Nutzung von HessenConnect weiterhin!



Ingrid Steinmel
IT-Fortbildung

ingrid.steinmel@hzd.hessen.de

Wie digital leben wir?

Digitalisierung im sozialen Umfeld

Digitalisierung gestalten - das ist unser Job. Aber hört unser Denken und Handeln in digitalen Algorithmen an der Bürotür auf? Wie digital leben wir in unserem Alltag - und hat die Pandemie uns digitaler gemacht?

Dr. Bernhard Fussel

Bereichsleiter Betrieb Netze und Sicherheitskomponenten, HZD

Statt mich wie vor der Pandemie mit meiner Clique aus der damaligen Mainzer Szenekneipe „Krokodil“ an der Pizzeria Fortuna zu treffen, haben wir den virtuellen Tresen ins Leben gerufen: Diese Idee eines Freundes begann mit einer Dichterlesung von Schiller über Ringelnetz bis Morgenstern per Videotool. Daraus haben sich viele Abende entwickelt, an denen wir uns mal in kleiner, mal in größerer Runde austauschen - sei es über Poesie oder die Entwicklung des Menschen hin zum Homo sapiens sapiens.



Angelika Töws,

IT-Prozessmanagerin, HZD

Einige andere Trainees und ich sind inzwischen vom gemeinsamen realen Mittagstreffen in der HZD-Cafeteria auf eine „Skype-Mittags-Telko“ ausgewichen. Aufgelockert werden diese Mittags-Telkos durch digitale Montagsmalerrunden, die sehr gut ankommen und zur Erheiterung beitragen. Kürzlich ist uns dabei die Idee zu einem Netzwerk gekommen, das junge Menschen in der HZD miteinander verbindet. Wir stehen noch am Anfang der Planung, hoffen aber, dass wir uns eines Tages auch wieder mit gemeinsamen „analogen“ Aktivitäten vernetzen können.



Karim Meiborg, Softwareentwickler web 2.0, Drupal, HZD

Normalerweise proben wir einmal die Woche in einem Proberaum, zuletzt im vergangenen September. Während des ersten Shutdowns im Frühjahr 2020 haben wir versucht, mit normalen Videokonferenz-Tools zu proben. Das ging fürchterlich schief, weil die Latenzen zu groß sind und schwanken - da kann man keinen gemeinsamen Takt halten.

Um Weihnachten stieß unser Gitarrist auf die Open-Source-Software Jamulus, die speziell für das gemeinsame Musizieren entwickelt wurde. Ich habe die Server-Komponente auf einem Raspberry-Pi zuhause installiert und den Server von außen zugänglich gemacht. Jedes Bandmitglied hat zuhause ein Audio-Interface, mit dem Instrument bzw. Mikrofon und Computer miteinander verbunden sind. Die ersten Tests waren vielversprechend und bald hatte jeder sein Audio-Setup im Griff.

Im Großen und Ganzen klappt das erstaunlich gut. Hin und wieder knackt und rauscht es, das ist der Preis für die geringe Latenz. Wir proben jetzt wieder wöchentlich, hoffen allerdings, dass wir uns bald wieder in echt treffen können. Online gelingt es uns zwar, das bestehende Repertoire „warmzuhalten“, aber was Neues haben wir uns auf diesem Weg bislang nicht erarbeiten können.



Wo und wie sind Sie digitaler geworden? Die INFORM-Redaktion freut sich auf Ihre Rückmeldungen.

→ redaktion@hzd.hessen.de

Erscheinen: September 2021



OZG-Umsetzung

Im Zuge der **OZG-Umsetzung bis 2022** realisiert die HZD im Auftrag des Innenministeriums in einem eigenen Projektrahmen die Umsetzung der OZG-Leistungen des Landes mit den jeweiligen Ressorts. Die nächste Ausgabe der INFORM stellt das Umsetzungsmanagement der HZD genauer vor.



HessenWeb

Ab **Mitte des Jahres** wird das bisherige Content-Management-System für die Internetauftritte der Landesverwaltung vom HessenWeb abgelöst. Die neuen Features garantieren ein **deutliches Plus** an Gestaltungsfreiheit beim Aufbau der Seiten.

**Sie möchten zum Thema IT im Land
auf dem Laufenden bleiben?**

Dann besuchen Sie uns auch online oder
abonnieren unseren Newsletter INFORM|DIREKT unter
www.hzd.hessen.de

Die HZD im Überblick

Leistungen, Aktivitäten und Zahlen – jetzt im
Jahresbericht 2020



online: <https://hzd.hessen.de/jahresberichte>

Bestellen Sie Ihr gedrucktes Exemplar: infomaterial@hzd.hessen.de

www.hzd.hessen.de

