Hessisches Ministerium des Innern und für Sport

HESSEN

Interkommunale Zusammenarbeit (IKZ) im Bereich der Cybersicherheit

Zusammenfassung der Tagung in Wiesbaden am 13. Dezember 2022

Interkommunale Zusammenarbeit (IKZ) im Bereich der Cybersicherheit

Zusammenfassung der Veranstaltung in Wiesbaden am 13. Dezember 2022

IMPRESSUM

Herausgeber Hessisches Ministerium des Innern und für Sport
Kommunales Beratungszentrum Hessen –
Partner der Kommunen
Friedrich-Ebert-Allee 12, 65185 Wiesbaden

Redaktion Daniela Willkommen, Claus Spandau, Andreas Weuffen

Internet https://beratungszentrum.hessen.de

E-Mail beratungszentrum@hmdis.hessen.de

Gestaltung Grützmacher GmbH · Agentur für Digital- und Printmedien, Frankfurt

KOMMUNALES BERATUNGSZENTRUM HESSEN
Partner der Kommunen

VORWORT ZUR TAGUNG

Wir freuen uns, Ihnen im Nachgang zu unserer Veranstaltung am 13. Dezember 2022 die wichtigsten Inhalte und Fakten der Veranstaltung „Interkommunale Zusammenarbeit (IKZ) im Bereich der Cybersicherheit" zu präsentieren.

Wir veranstalteten erstmalig eine Hybrid-Tagung, die von rd. 140 Teilnehmern bei diesem doch schon etwas spezielleren Thema sehr gut angenommen wurde.

Die Wahl des Themas „IKZ im Bereich der Cybersicherheit" ist ganz bewusst erfolgt, weil, es ist ein besonderes Anliegen unseres Staatssekretärs, Herrn Stefan Sauer, der schon bei Beginn des Überfalls auf die Ukraine durch Russland meinte, wir müssten die Cyber-Sicherheit als Thema der IKZ verstärkt in den Blickwinkel der Kommunen stellen.

Wenn wir heute ein sehr unbürokratisches und sehr kommunalfreundliches Förderprogramm für IKZ-Kooperationen haben und wenn Hemmnisse, die der IKZ im Wege stehen wo immer möglich rasch und gründlich beseitigt werden, dann ist das dem Wirken der Hessischen Landesregierung und deren positiver Positionierung zur IKZ zu verdanken. Das IKZ-Förderprogramm wurde vor dem Hintergrund geschaffen, eine gleichermaßen kommunalfreundliche wie auch unbürokratische Förderrichtlinie zu haben und wird bei den jeweiligen Fortschreibungen ebenso strikt berücksichtigt und eingehalten.

Mit dieser Broschüre bedanken wir uns insbesondere nochmals bei den Referentinnen und Referenten der Cybersicherheitsveranstaltung. Ihnen gilt unser Dank für die sehr informativen Beiträge und die hervorragende Unterstützung für unsere hessischen Kommunen auf dem Weg zu erfolgreichen IKZ-Projekten im Bereich der Cybersicherheit.

Bei unseren Kongressen stellen wir stets einen Bereich Interkommunaler Zusammenarbeit in den Mittelpunkt einer Tagung und tragen Ihnen dazu einiges an Theorie und etliches an erfolgreichen Beispielen mit der gesamten Palette der Erfolgsfaktoren und der Stolperfallen vor.

Auch mit der Veranstaltung aus dem Dezember 2022 konnten wir für Sie erfolgreiche Beispiele vorstellen, die als modellhaft für andere Kommunen angesehen werden können, und konnten den Teilnehmer*innen Anregungen und ein grundsätzliches Handlungsmuster mit auf den Weg in ihre Kommunen und in ihre sich anschließende Arbeit bei eigenen Projekten geben.

Das Ziel unserer Veranstaltung zur IKZ im Bereich der Cybersicherheit war, Ihnen die Notwendigkeit einer Hinwendung zur Thematik der Cybersicherheit darzulegen und bei Ihnen das Interesse zu wecken, gute, nachahmensfähige, modellhafte Kooperationen kennenzulernen, aber neben den Chancen auch Risiken und Probleme bei der Umsetzung der Projekte zu benennen und fachliches Wissen durch die entsprechenden Ansprechpartner bereitzustellen und einen Austausch zwischen Handelnden zu initiieren.

Die Gefahren im digitalen Raum sind allgegenwärtig. Mit dieser Broschüre möchten wir Ihr Bewusstsein zu diesem hochsensiblen und wichtigen Thema nochmals schärfen.

Einige Kommunen haben unsere Veranstaltung bereits zum Anlass genommen, sich auf den Weg zu einer Kooperation im Bereich Cybersicherheit zu begeben – darunter auch ein kreisweites Projekt unter Beteiligung eines Landkreises.

Sprechen Sie uns gern an. Wir helfen Ihnen bei der Initiierung von IKZ-Projekten und unterstützen Sie bei der Beantragung von IKZ-Fördermitteln.

Bitte nehmen Sie die Unterstützung und Angebote der Beratungsstellen für Cybersicherheit bei Ihren Projekten in Anspruch.

Ihr
Kommunales Beratungszentrum Hessen –
Partner der Kommunen

Daniela Willkommen
Claus Spandau
Andreas Weuffen

STAATSSEKRETÄR STEFAN SAUER
HESSISCHES MINISTERIUM DES INNERN UND FÜR SPORT

GRUSSWORT

Meine sehr geehrten Damen und Herren,

es ist für die Hessische Landesregierung, insbesondere auch im Namen unseres Hessischen Ministerpräsidenten Boris Rhein, und, vor allem auch für mich als Vertreter des Hessischen Ministeriums des Inneren und für Sport erfreulich, dass die IKZ, die wir seit dem Jahre 2004 in besonderer Weise und in stetig ansteigendem Maße finanziell und ideell unterstützen, ganz offenkundig keine kurzzeitige Modeerscheinung war. Ganz im Gegenteil hat sie sehr deutlich an Bedeutung in den Kommunen gewonnen.

Bedeutung der IKZ
Aus Sicht der Hessischen Landesregierung stellt die IKZ auch für die Zukunft ein sehr wichtiges Handlungsfeld für die Kommunen wie gleichermaßen auch für unser Bundesland dar. Deshalb haben wir uns in den zurückliegenden Jahren sehr intensiv für IKZ-Projekte in den Kommunen eingesetzt und wollen dieses auch weiterhin mindestens in dem bisherigen Umfang so weiterführen.

Leistungsbilanz der IKZ
Dabei ist es in erster Linie natürlich die Zukunft der IKZ, die wir im Auge haben. Aber wir haben auch bereits heute eine beeindruckende **Leistungsbilanz** bei der IKZ vorzuweisen.

So hat die Landesregierung bereits im Jahre 2004 mit einem aus heutiger Sicht kleinen Förderprogramm begonnen, den Kommunen die Wichtigkeit der IKZ deutlich zu machen. Wir haben in den Folgejahren das Förderprogramm der IKZ stetig ausgebaut. Wir haben die möglichen Förderzwecke wie auch den Kreis der antragsberechtigten Kommunen stetig erweitert. Heute sind alle Gemeinden, Städte und Landkreise und seit einigen Jahren auch kommunale Zweckverbände antragsberechtigt. Und wir haben die IKZ-Förderung auf nahezu alle Bereiche kommunalen Handelns ausgeweitet.

Kreisweite Kooperationen
Auf eine Änderung möchte ich dabei besonders eingehen. Kreisweite Kooperationen unter Beteiligung der Landkreise können nun stärker gefördert werden. So können kreisweite Kooperationen, an denen sich die überwiegende Zahl der kreisangehörigen Gemeinden beteiligt, eine über die Regelzuwendung von 100.000 € hinausgehende Förderung erhalten. Die Hessische Landesregierung hat diese Förderung bewusst erhöht, denn sie sieht gerade in der interkommunalen Zusammenarbeit zwischen Landkreisen und den kreisangehörigen Gemeinden noch großes und nicht ausgeschöpftes Potenzial.

Gründung der Beratungsstelle im Jahre 2009 – Zuständigkeit
Wir haben gemeinsam mit den kommunalen Spitzenverbänden im Jahre 2009 eine Beratungsstelle für die Kommunen zur Interkommunalen Zusammenarbeit geschaffen. In diesem Beratungszentrum sind neben der IKZ-Beratung auch die Beratung von Kommunen in Fragen der Haushalts- und Finanzpolitik sowie der sog. Förderlotse angesiedelt. Der Förderlotse berät Kommunen, Privatpersonen und Vereine auf deren Anfrage hin über bestehende Förderprogramme von EU, Bund, Land und sonstigen Stellen und die jeweils sachlich zuständigen Mitarbeiterinnen und Mitarbeiter bzw. Fachstellen.

Förderumfang bis heute
Und unser Einsatz für die IKZ zeigt sehr erfreuliche Ergebnisse. So ist – statistisch gesehen – seit dem Jahre 2009 fast jede der 443 hessischen Kommunen an nahezu fünf IKZ-Projekten beteiligt. Unsere gemeinsame erfolgreiche Arbeit in Hessen lässt sich zusammenfassen in dem Satz

„STARKE KOMMUNEN – STARKES LAND".

Die hessische Landesregierung will die Kommunen stärken. Das machen wir mit der IKZ, aber das haben wir auch bereits gemacht mit finanziell wesentlich aufwendigeren Maßnahmen wie dem Kommunalen Schutzschirm, der Hessenkasse oder einem gut ausgestatteten Kommunalen Finanzausgleich.

Thema heute: Cybersicherheit
Wir wollen Ihnen das auch in den Kommunen immer drängendere Feld der Cybersicherheit näherbringen. Wir wollen Sie für dieses wichtige Thema sensibilisieren und dazu beitragen, dass Sie ihr Augenmerk verstärkt auf Lösungen zu diesem Aspekt der Digitalisierung legen.

Dazu haben wir Ihnen in dieser Broschüre die Vorträge einiger kommunalen IKZ-Projekte und Fachvorträge zum Thema der verbesserten Cybersicherheit zusammengefasst.

HESSEN

Der Grad der Digitalisierung ist heute bereits einer der zentralsten Standortfaktoren. Alle Kommunen stehen vor ähnlichen Herausforderungen und Aufgaben im Bereich der Verwaltungsdigitalisierung.

Bürger und Unternehmen erwarten von einer modernen Verwaltung eine Erreichbarkeit rund um die Uhr. Unsere Dienste müssen so selbstverständlich wie andere Online-Dienste verfügbar sein.

Mit der Umsetzung des Online-Zugangsgesetz (OZG) sind wir genau auf diesem richtigen, zukunftsweisenden Weg. Und gleichzeitig sind die OZG-Leistungen dabei nur ein Baustein der Digitalisierung.

Einen weiteren Digitalisierungsschub lösen zweifelsohne „SMART-Cities" aus. Die SMART-City ist die intelligente Steuerung vielfältiger kommunaler Aufgaben über vernetzte Sensoren und Aktoren. Dies reicht von der städtischen Grünanlagen-Bewässerung über das Auslösen von Alarmen bei kritischen Pegelständen bis zu einer intelligenten Parkraumbewirtschaftung und vielem mehr. Die SMART-City hat großes Potential, auch für die interkommunale Zusammenarbeit.

Allerdings ist die Umsetzung der Digitalisierung leichter gesagt als getan, wie Sie alle wissen. Die IT-Technik ist komplex und die fachlichen Prozesse oft nicht auf eine Digitalisierung vorbereitet. Gerade auch wir als Verwaltung haben hier einen hohen Investitionsbedarf.

Und jetzt kommen noch die Risiken im Cyberraum hinzu.

Allenthalben nutzen Kriminelle und zunehmend fremde Staaten von faktisch überall auf der Welt die IT und speziell das Internet für ihre Angriffe. Der Schaden allein der deutschen Wirtschaft belief sich in 2021 nach Schätzungen auf ca. 200 Milliarden Euro.

Auch die Verwaltung ist massiv betroffen. Nie gab es so viele Ransomware-Angriffe, also Erpressungen durch Datenverschlüsselungen. Denken Sie nur an den allseits bekannten Fall der Landkreisverwaltung in Sachsen-Anhalt: Erstmals wurde wegen eines Cyber-Angriffs der Katastrophenfall ausgerufen. Bürgernahe Dienstleistungen waren über 200 Tage lang nicht oder nur eingeschränkt verfügbar.

Viele Angriffe werden dabei gar nicht gemeldet. Häufig werden die zuständigen staatlichen Stellen nicht oder nur sehr zögerlich informiert und genutzt. Ein wichtiger und richtiger Schritt in diese Richtung ist das IT-Sicherheitsgesetz des Bundes. Mit dem Gesetz sind die Betreiber kritischer Infrastrukturen zur Einhaltung von Mindeststandards und zur Meldung bedeutender Angriffe auf ihre IT verpflichtet. Das IT-Sicherheitsgesetz 2.0 ist seit Mai 2021 in Kraft und erweitert die deutsche KRITIS-Regulierung von 2015 deutlich.

Unterstützung des HMDIS für die Kommunen – Cybersicherheit

Wir bieten den hessischen KRITIS-Betreibern zusätzlich vielfältige Unterstützungen. Die Ansprechstelle in Hessen ist das **CERT** in meinem Haus. Sie erreichen das CERT-Hessen rund um die Uhr. Das CERT-Hessen ist „zentrale Stelle" für hessische KRITIS-Betreiber.

Besser noch, Sie schützen Ihre Kommune präventiv, bevor der Angriff erfolgreich wird. Nutzen Sie die **Beratungsangebote des kommunalen Dienstleistungszentrums Cybersicherheit,** des sog. kDLZ CS. Wir fördern das kDLZ, damit die Beratungsleistungen für unsere hessischen Kommunen kostenfrei bleiben.

Immer mehr greift die Einsicht und Bereitschaft Cybersicherheit nicht als ungeliebten Eingriff in die freie Nutzung der IT, als übertriebene Panikmache, als Last, sondern als absolut notwendigen Schutz für einen freien und sicheren Cyberraum zu begreifen.

Cybersicherheit ist eine der wichtigsten Voraussetzungen der Digitalisierung. Cybersicherheit ist eine notwendige Bedingung für ein freies Internet.

Nehmen Sie die **Angebote des Hessen3C**, die bereits angesprochene Förderung des kommunalen Dienstleistungszentrums Cybersicherheit (kDLZ) und selbstverständlich die IKZ-Förderung in Anspruch und aktiv an.

Übergabe des IKZ-Förderbescheides an die Vertreter des Landkreises Gießen (v.l.n.r. Thorsten Becker, Abt. Sicherheit; David Pöhlmann, IT-Sicherheitsbeauftragter; Christopher Lipp, Erster Kreisbeigeordneter, alle Landkreis Gießen und Staatssekretär Stefan Sauer, HMdIS).

Dem Kreisausschuss des Landkreises Gießen wird für das Projekt „Cybersicherheit in öffentlichen Verwaltungen" eine Zuwendung in Höhe von 150.000 € gewährt.

Die Kooperation des Landkreises Gießen mit allen 18 kreisangehörigen Städten und Gemeinden, einschließlich der Universitätsstadt Gießen, belegt einmal mehr, dass interkommunale Zusammenarbeit zukunftsweisende Spielräume und besondere Chancen bietet, große Herausforderungen erfolgreich anzugehen.

CYBERSICHERHEIT

CYBERCOMPETENCECENTER – ANGEBOTE DES HESSEN3C FÜR KOMMUNEN

Markus Wiegand, Leiter Cybersecurity / Stellv. Referatsleiter Hessen3C,
Hessisches Ministerium des Innern und für Sport

CYBER COMPETENCE CENTER HESSEN

Hessisches Ministerium des Innern und für Sport

Wer bin ich?

- „vom Großrechner bis zur Cloud“
- 15 Jahre Betriebserfahrung
- 7 Jahre Leitung von Infrastruktur- und Konsolidierungsgroßprojekten
- seit 2011 ausschließlich IT-/Cyber-Security in der Landesverwaltung
  - Mitglied der Arbeitsgruppe Informationssicherheit des IT-Planungsrates
  - ehem. Mitglied des Fachbeirats des nationalen Cybersicherheitsrates

Hessisches Ministerium des Innern und für Sport

Was ist das CyberCompetenceCenter?

- Eines von drei Referaten mit Cyber-/IT-Sicherheitsschwerpunkt im hessischen Innenministerium
- ca. 50 Personen
- Betrieb des Landes-CERT für Hessen
- Meldestelle „HessenGegenHetze“
- Bündelung von Expertise
- Gemeinsames Cyber-Lagebild
- Austauschplattform für die Cybersicherheitsspezialisten des Innenressorts (insbesondere Polizei, Verfassungsschutz)

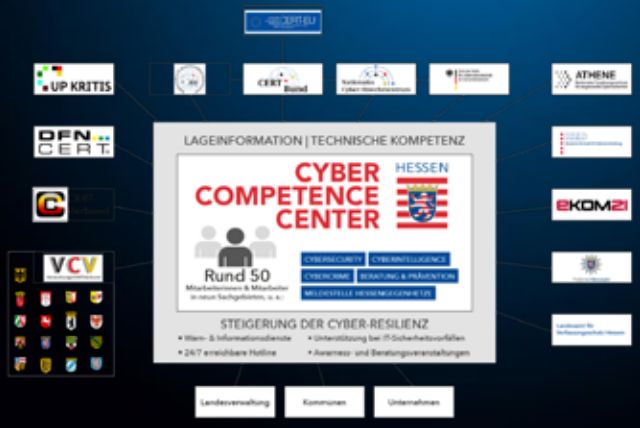
Hessisches Ministerium des Innern und für Sport

Unsere Zielgruppen:

- Landesverwaltung
- Kommunen
- KRITIS-Einrichtungen
- Kleine und mittlere Unternehmen
- Bürgerinnen und Bürger

Hessisches Ministerium des Innern und für Sport

Hessen3C auf einen Blick



Hessisches Ministerium des Innern und für Sport

Angebote des Hessen3C für Kommunen

- **Beratung**
  - hersteller- und produktneutrale Beratung zu allen Fragen der IT- und Cyber-Sicherheit
  - IT-Sicherheits-Architektur- und IT-Sicherheits-Prozess-Beratung

CYBER COMPETENCE CENTER HESSEN

Hessisches Ministerium des Innern und für Sport

Angebote des Hessen3C für Kommunen

- Warn- und Informationsdienst
  - Täglicher Schwachstellenbericht
    Informationen zu Schwachstellen, nach dem Motto:
    „Um was wir uns zuerst kümmern sollten“.
  - Warnmeldungen des CERT-Hessen und des BSI
    Informationen zu besonderen Gefährdungslagen, nach dem Motto:
    „Um was wir uns sofort kümmern müssen“.

Hessisches Ministerium des Innern und für Sport

Angebote des Hessen3C für Kommunen

Incident Response

- Unterstützung beim IT-Krisenmanagement
  - Organisation und Prozesse
  - Kommunikation intern/extern
  - Analyse von Logdaten und Artefakten
  - forensische Datensicherungen / Analysen
  - Abgleich mit nicht-öffentlichen Quellen, Verbindung zu anderen Behörden

Hessisches Ministerium des Innern und für Sport

Angebote des Hessen3C für Kommunen

Kommunales Dienstleistungszentrum – Cybersicherheit (KDLZ-CS)

- Unterstützung auf dem Weg zum Informationssicherheitsmanagement
  - Neutrales Assessment der IT
  - Priorisierte Handlungsempfehlungen
  - eLearning
  - Unterstützung von IT-Sicherheitsprojekten

Hessisches Ministerium des Innern und für Sport

Angebote des Hessen3C für Kommunen

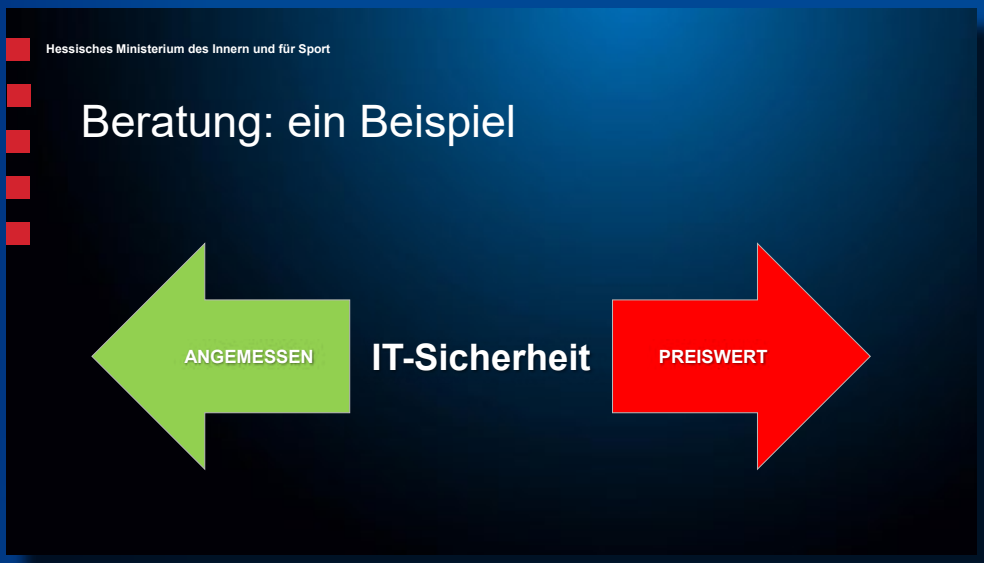
- Hessen Cyberabwehr-Ausbildungszentrum
  - Unterstützung bei der Aus- und Fortbildung der (IT-) Mitarbeiter
  - 3-tägige, ortsnahe Business-Continuity-Management-Schulungen

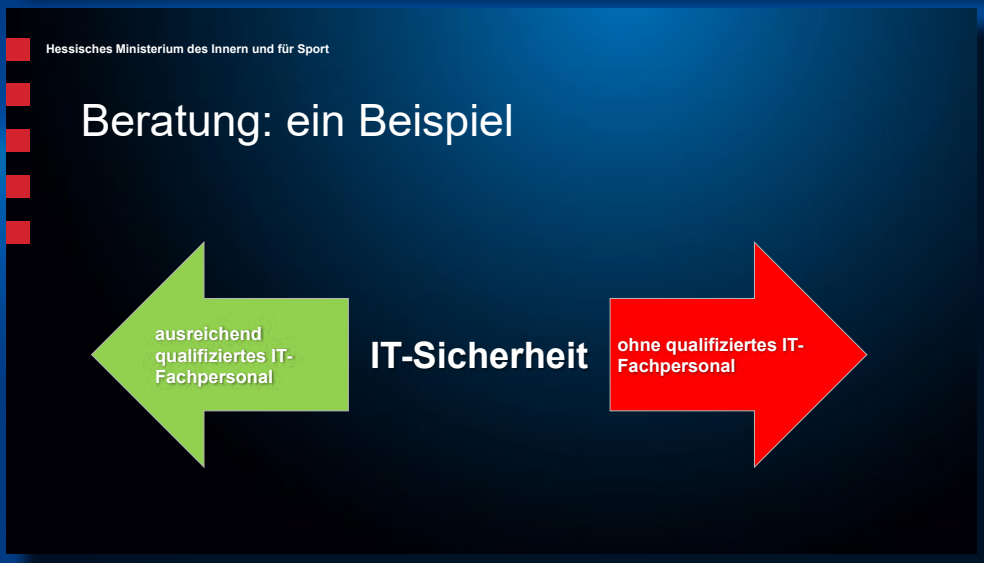
Hessisches Ministerium des Innern und für Sport

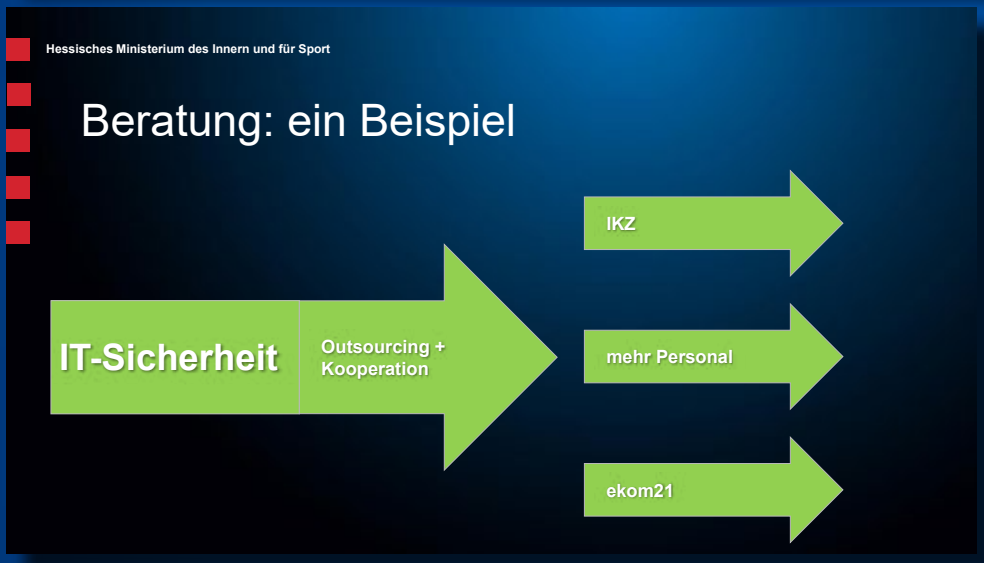
Angebote des Hessen3C für Kommunen

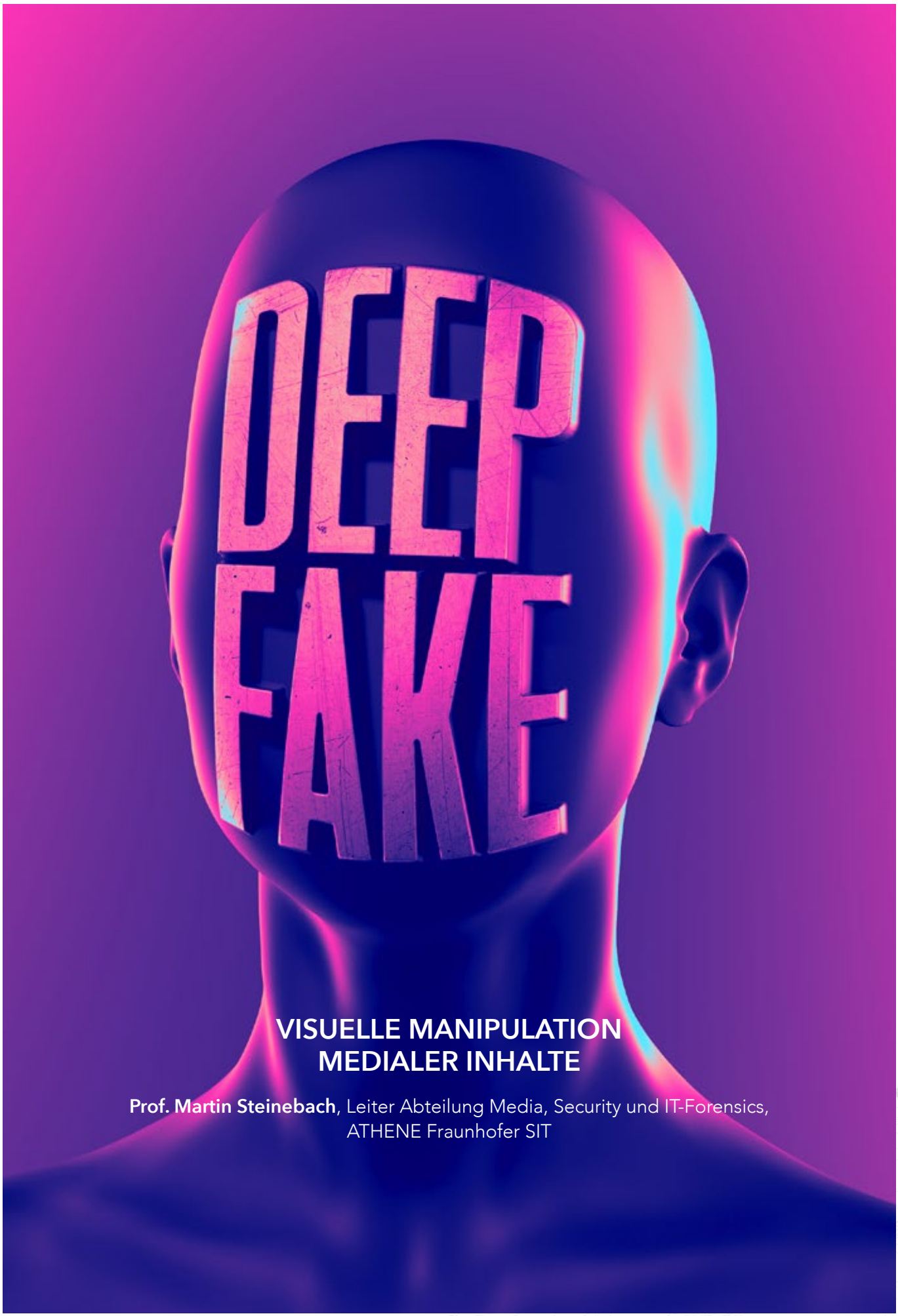
- Hessen Data Leak Checker
  - Möglichkeit zum kostenfreien und DSGVO-konformen Abgleich Ihrer Domains mit den Data-Leak-Datenbanken des Hasso Plattner Instituts.

CYBER COMPETENCE CENTER HESSEN









VISUELLE MANIPULATION MEDIALER INHALTE

Prof. Martin Steinebach, Leiter Abteilung Media, Security und IT-Forensics, ATHENE Fraunhofer SIT

Videokonferenzen sind heute zu einem Standard der Kommunikation geworden, insbesondere auch im beruflichen Alltag. Immer häufiger finden Besprechungen online oder zumindest hybrid statt. Dadurch hat auch die Möglichkeit, Videokonferenzen zu manipulieren an Bedeutung gewonnen. Deepfake Verfahren wie DeepFaceLive[1] sind in der Lage, aus einem dreiminütigen Video, welches eine Person zeigt, deren Mimik innerhalb eines Tages Rechenzeit auf einem handelsüblichen, für Computerspiele geeigneten PC so zu erlernen, dass das Gesicht der Person dann in Echtzeit über ein Kamerabild gelegt wird, das danach in eine Videokonferenz eingespeist wird. Allgemein kann das Vertrauen, welches in eine bekannte Person gesetzt wird, durch die Übernahme ihres Gesichts missbraucht werden. So kann ein Angreifer Videokonferenzen mit vorgetäuschten Identitäten besuchen, um beispielsweise CEO Fraud zu betreiben oder Desinformationen zu verbreiten.

Derzeit ergeben sich für den Angreifer dabei noch zwei Herausforderungen: Zum einen wird die Stimme häufig mit technischen Methoden noch nicht so überzeugend verändert wie das Aussehen, entsprechende Verfahren hinken des visuellen Deepfakes hinterher. Demensprechend muss die Stimme vom Angreifer nachgeahmt werden. Zum anderen erfordern die so nutzbaren Deepfakes eine gewisse Ähnlichkeit mit den ausgetauschten Personen, da nur die Gesichtsregion verändert wird. Haare und Körperbau müssen also vom Angreifer, soweit möglich, kosmetisch imitiert werden.

Wünschenswert ist als Konsequenz ein automatisches technisches Erkennen von Deepfakes. Ansätze hierfür sind von der Forschung bereits zahlreich vorgestellt worden. Sie basieren auf bildforensischen Methoden, die durch den Deepfake entstehende Anomalien in den Bildeigenschaften erkennen oder auch auf maschinellem Lernen, wobei ein Netz durch echte Videos und Deepfakes trainiert wird und danach selbständig zwischen beiden Kategorien unterscheiden kann.

Allerdings sind hier noch Fehlerraten zu erwarten, die einen Einsatz beispielsweise als Plugin für einen Browser entgegenstehen. Je nach Ansatz und Qualität der Deepfakes sind hier Erkennungsraten zwischen 60 und 90 Prozent zu erwarten. Die größere Herausforderung ist aber die häufig nicht erwähnte Wahrscheinlichkeit für Fehlalarme, die bei einer größeren Videokonferenz schnell zu massiven Problemen führen, wenn mit einer hohen Wahrscheinlichkeit mindestens ein Teilnehmer als Deepfake fehlerkannt wird. Zusätzlich ist es derzeit noch möglich, die Erkennung von Deepfakes durch Verschleierungen wie Weichzeichner, Helligkeitsanpassung oder Quantisierung der Bilder zu erschweren oder ganz zu verhindern. Aktuelle Forschungsergebnisse zeigen aber, dass auch hier Gegenmaßnahmen möglich sind. Die Verschleierungen werden dann erkannt und ein Verfahren, welches Deepfakes in Kombination mit der entsprechenden Verschleierung aufdecken kann, wird ausgewählt.

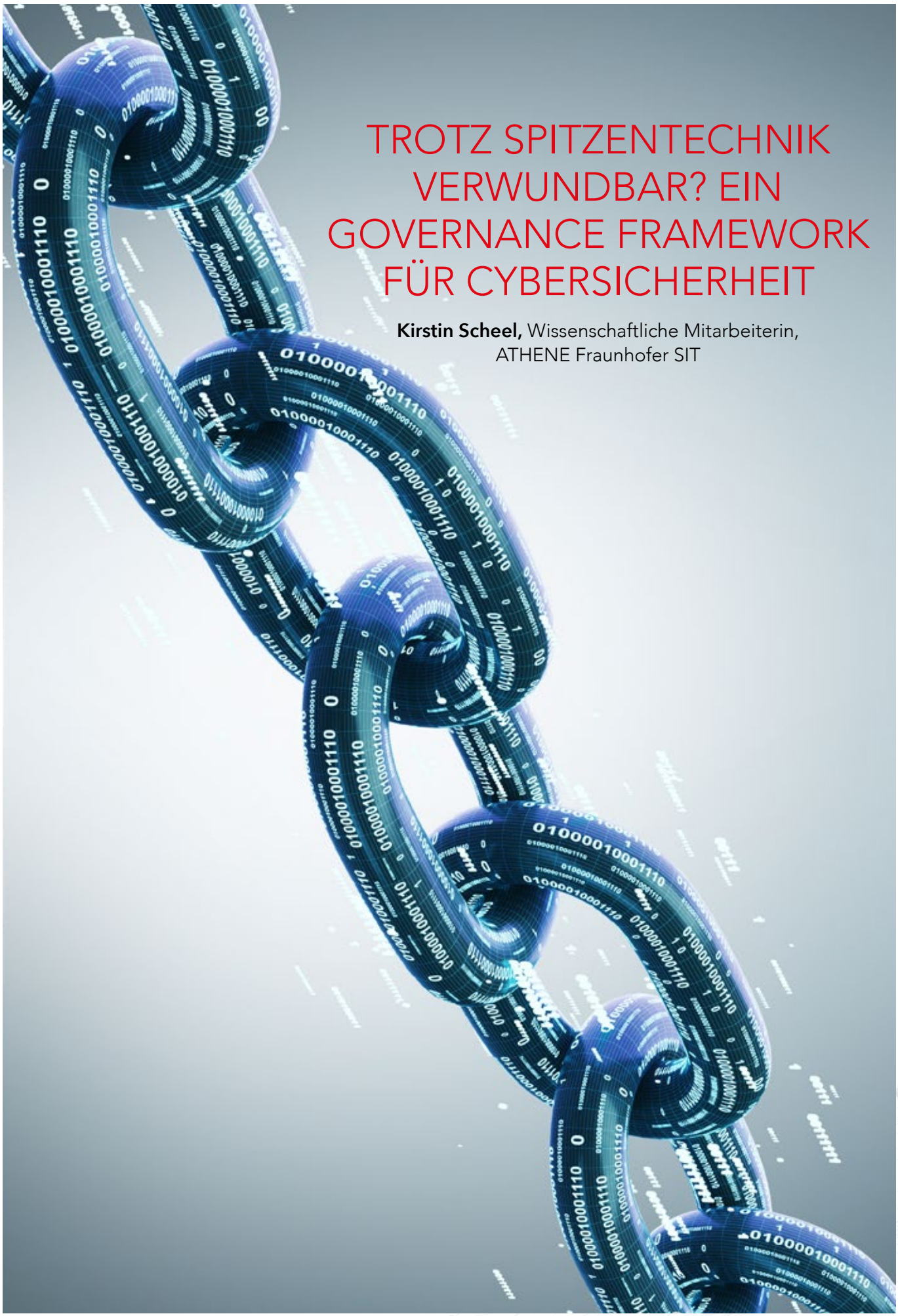
Neben Deepfakes sind aber seit Mitte 2022 auch die text-to-image Verfahren wie DALL-E und stable diffusion[2] zu einer Herausforderung für das Vertrauen geworden, welches in Bilder gesetzt werden kann. Mit diesen, teilweise frei als Open Source verfügbaren Lösungen können Bilder anhand einer kurzen Textbeschreibung entweder völlig neu erstellt oder entsprechend den Vorgaben im Text manipuliert werden. Soll eine Desinformation durch ein „Beweisfoto" verstärkt werden, kann nun beispielsweise ein geheimes Treffen zweier Personen einfach synthetisiert werden. Dazu genügt es, dass das zugrundeliegende System die Person kennt, also ausreichend viele Bilder von ihr im Training gezeigt bekommen hat, was bei Personen des öffentlichen Lebens so gut wie immer der Fall ist. Aber auch die Möglichkeit, ein vorhandenes Foto beliebig per Texteingabe zu verändern, kann missbräuchlich genutzt werden. Einer Person, die auf einem Foto ein Smartphone hält, kann stattdessen beispielsweise ein Messer in die Hand gesetzt werden. Ebenso kann Kleidung von Personen verändert oder entfernt werden.

Auch hier kann damit gerechnet werden, dass in naher Zukunft Methoden zur Erkennung solcher Verfahren verfügbar werden. Erste Forschungsergebnisse sind bereits veröffentlicht. Eventuell können ähnliche Verfahren wie bei der Erkennung von Deepfakes eingesetzt werden. Aber auch statistische Algorithmen, wie sie in der Steganalyse eingesetzt werden, sind erfolgversprechend. Auch optisch weisen die künstlich erstellten Fotos heute noch Fehler auf, beispielsweise bei unterschiedlichen Augenfarben von Personen, einer falschen Anzahl von Fingern oder Unregelmäßigkeiten in der Bildschärfe.

Zusammengefasst kann festgehalten werden, dass in jüngerer Vergangenheit zahlreiche Möglichkeiten entstanden sind, die es Anwendern ohne große Investitionen und mit überschaubaren Kenntnissen erlauben, Bild- und Videosignale zu manipulieren. Der forensische Ansatz, solche Manipulationen aufzudecken, ist dabei immer nur die zweitbeste Strategie. Zuverlässiger ist es, eine Infrastruktur aufzusetzen, die es durch Signaturen oder Protokolle erlaubt, die Echtheit eines Inhalts zu belegen, ähnlich wie dies heute bei signierten Dokumenten der Fall ist.

1 https://github.com/iperov/DeepFaceLive

2 https://stability.ai/blog/stable-diffusion-public-release



TROTZ SPITZENTECHNIK VERWUNDBAR? EIN GOVERNANCE FRAMEWORK FÜR CYBERSICHERHEIT

Kirstin Scheel, Wissenschaftliche Mitarbeiterin,
ATHENE Fraunhofer SIT

Die Digitalisierung durchdringt nicht nur den Alltag aller Bürger*innen, sondern auch Behörden und administrative Infrastrukturen. Bezüglich der Cybersicherheit gibt es dabei jedoch manchmal strukturelle und organisatorische Hindernisse. Hier setzte ein vom Hessischen Ministerium des Innern und für den Sport (HMdIS) initiiertes Forschungsprojekt mit dem Fraunhofer-Institut für Sichere Informationstechnologie SIT als Mitwirkender im Forschungszentrum ATHENE an. Im Laufe des Projekts wurde ein Governance-Rahmenwerk entwickelt, welches strategisch das IT- Sicherheitsniveau von öffentlichen Stellen verbessern helfen kann.

Das 5V-Rahmenwerk für Cybersicherheit kann ein erster Schritt auf dem Weg einer Auseinandersetzung mit der IT-Sicherheit sowie ihrem Management in der öffentlichen Verwaltung sein. Letztlich sollte das Ziel eine professionell aufgestellte, idealerweise z.B. nach BSI IT-Grundschutz zertifizierte, Organisation sein – die 5V können helfen, dafür den Einstieg zu finden.

Diese basieren auf den in Abbildung 1 dargestellten Grundsätzen:

(i) Verankerung,

(ii) Verantwortlichkeiten,

(iii) Vereinheitlichung,

(iv) Vereinigung, und

(v) Verbesserung.

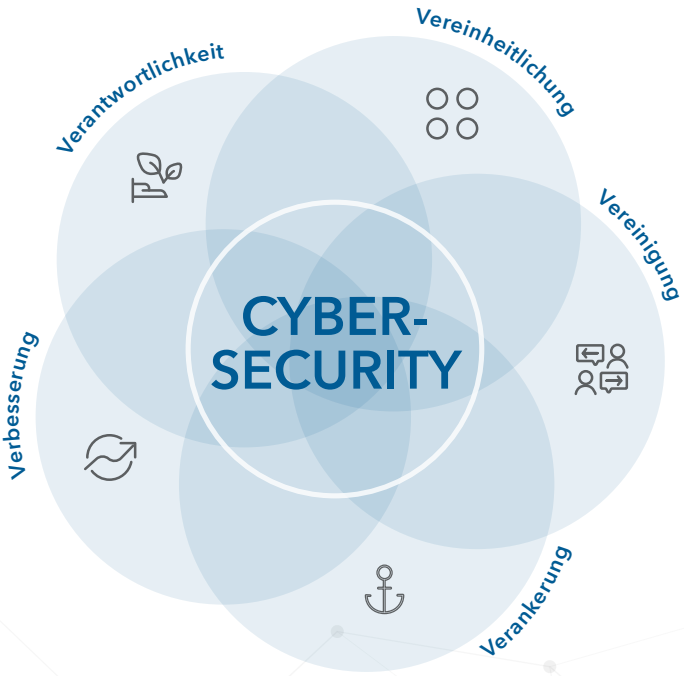


Abbildung 1: 5V

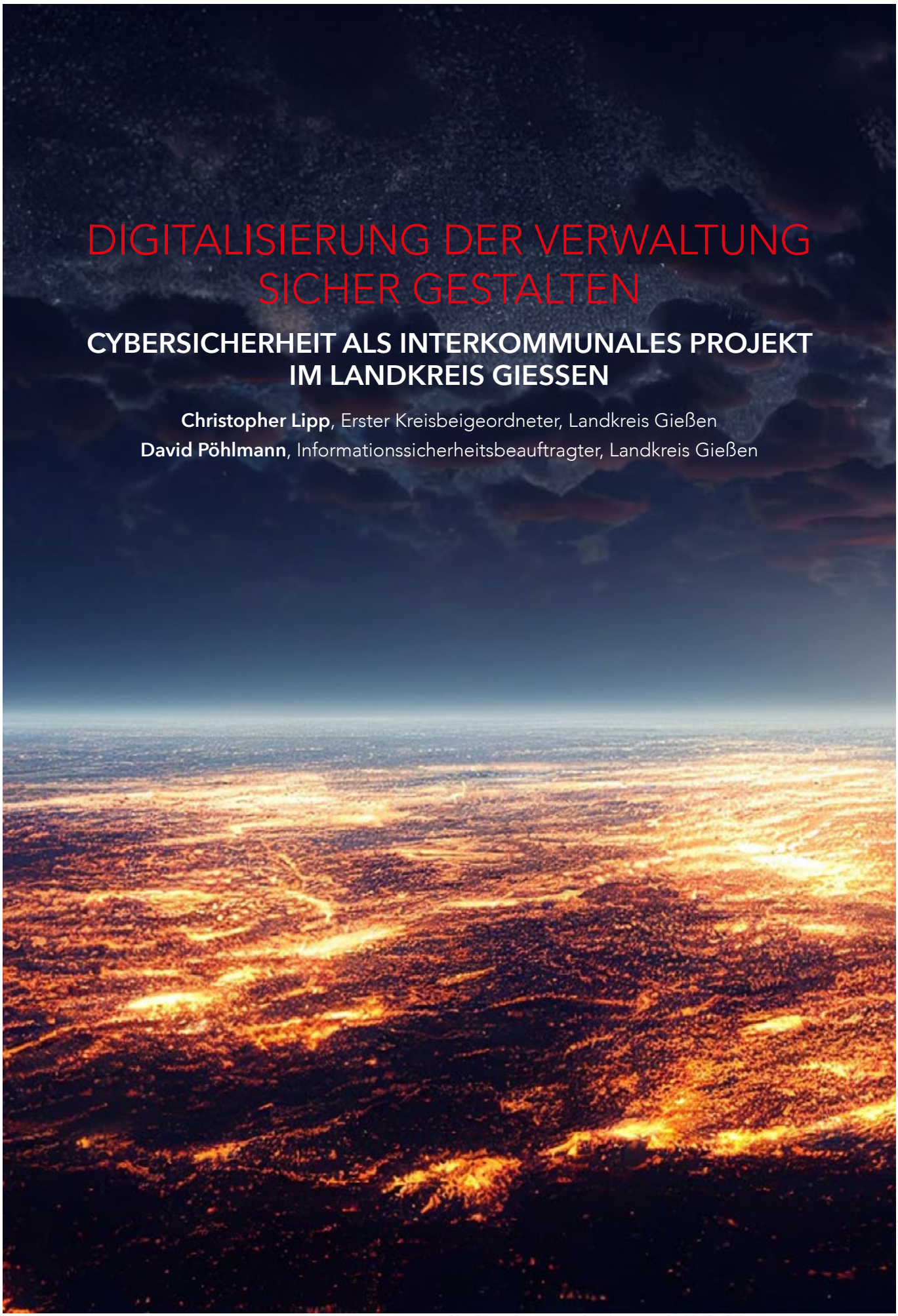
Die Cybersicherheit muss auf höchster Ebene in der Organisation **verankert** werden. Die oberste Führungsebene muss sich der Notwendigkeit von Sicherheit als Eckpfeiler aller Digitalisierungsprojekte bewusst sein.

Es müssen klare **Verantwortlichkeiten** zugewiesen werden. Darüber hinaus sind angemessene Ressourcen für die Wahrnehmung dieser Zuständigkeiten erforderlich.

Ein weiterer zentraler Gedanke ist die **Vereinheitlichung** von Systemen und Prozessen über Organisationseinheiten hinweg. Viele Fälle von Malware-Befall können sich z.B. über Systeme ausbreiten, die nicht richtig segmentiert sind.

Wichtig sind auch die betriebliche **Vereinigung** und bereichsübergreifende Kooperation, um Ressourcen effizient und effektiv einzusetzen.

Sich dynamisch verändernde Umgebungen erfordern eine kontinuierliche **Verbesserung**. Das Lernen aus internen und externen Fehlern ist unerlässlich, um mit diesen Entwicklungen Schritt zu halten.



DIGITALISIERUNG DER VERWALTUNG SICHER GESTALTEN

CYBERSICHERHEIT ALS INTERKOMMUNALES PROJEKT IM LANDKREIS GIESSEN

Christopher Lipp, Erster Kreisbeigeordneter, Landkreis Gießen
David Pöhlmann, Informationssicherheitsbeauftragter, Landkreis Gießen

Sehr geehrter Herr Staatssekretär Sauer,
sehr geehrter Herr Spandau,
sehr geehrte Damen und Herren,

zunächst möchte ich mich für das Interesse an unserer interkommunalen Zusammenarbeit auf dem Gebiet der Cybersicherheit, die wir seit dem 1. August 2022 mit allen 18 kreisangehörigen Kommunen des Landkreises Gießen – einschließlich der Universitätsstadt Gießen – durchführen, bedanken. Bedanken möchte ich mich ebenfalls ausdrücklich für die großzügige finanzielle Förderung des Landes Hessen für unser Projekt. Dies bestärkt uns darin, dass es der richtige Weg ist, die großen Herausforderungen im Zusammenhang mit der Gewährleistung der Informationssicherheit in den Kommunen im interkommunalen Verbund gemeinsam anzugehen.

Zusammen mit Herrn Pöhlmann, Informationssicherheitsbeauftragter des Landkreises Gießen, möchte ich Ihnen im Rahmen unseres Vortrages einen Einblick in unser Projekt, die ersten Schritte seit dem Projektstart sowie einen Ausblick auf die weitere Projektdurchführung geben.

Ausgangspunkt für die interkommunale Zusammenarbeit auf dem Gebiet der Cybersicherheit im Landkreis Gießen war die feste Überzeugung aller Projektpartner, dass die Digitalisierung der Verwaltung und dabei insbesondere die Digitalisierung staatlicher Leistungen ein Prozess ist, der nur dann erfolgreich sein kann, wenn wir ein Höchstmaß an Informationssicherheit und Datenschutz gewährleisten können. Deshalb muss ebenso dynamisch wie die Bedrohungslage durch Cyberangriffe auch unsere IT-Sicherheitsinfrastruktur kontinuierlich mitwachsen.

Hierzu braucht es gemeinsamer Strategien, es braucht die notwendigen technischen Voraussetzungen in jeder Kommune und es braucht vor allem auch die notwendigen fachlichen Kompetenzen durch qualifiziertes Fachpersonal.

Nach unserer Überzeugung bietet sich hierfür eine interkommunale Zusammenarbeit an, da sich zahlreiche Synergieeffekte nutzen lassen und da insbesondere kleine Kommunen – die kleinste Kommune im Landkreis Gießen hat rund 4000 Einwohner – nicht über die personellen und finanziellen Voraussetzungen verfügen, das Leistungspaket abzudecken, das wir den Kommunen im Rahmen der interkommunalen Zusammenarbeit auf dem Gebiet der Cybersicherheit anbieten.

Unsere interkommunale Zusammenarbeit ist zum 1. August 2022 gestartet und baut auf einem Vorgängerprojekt auf dem Gebiet der Cybersicherheit auf, das der Landkreis Gießen in den vergangenen fünf Jahren mit dem Landkreis Marburg-Biedenkopf gemeinsam erfolgreich durchgeführt hat.

Unser klares Ziel im Rahmen der interkommunalen Zusammenarbeit ist es, alle Kommunen im Landkreis Gießen auf ein hohes IT-Sicherheitslevel angelehnt an den BSI-IT-Grundschutz zu heben.

Das Projekt baut dabei im Wesentlichen auf drei Säulen auf:

1. Beratung, Warnung und Früherkennung in Bezug auf IT-Sicherheitsrisiken und Entwicklung von Handlungsempfehlungen: Die Beratung bezieht sich dabei sowohl auf organisatorische Maßnahmen, wie zum Beispiel die gemeinsame Erstellung und Implementierung eines IT-Notfallmanagements bzw. insgesamt eines Informationssicherheitsmanagements, als auch auf technische Aspekte, wie beispielsweise das Schließen von möglichen Schwachstellen in der IT-Infrastruktur der Kommunen nach eingehender Beratung. Einer unserer ersten Schritte im Rahmen des Projektes ist deshalb ein sog. „IT-Schwachstellen-Scan" in den Kommunalverwaltungen.

2. Sensibilisierungs- und Schulungsmaßnahmen für Mitarbeiterinnen und Mitarbeiter: Der Faktor Mensch ist zumeist leider der größte Risikofaktor in der IT-Sicherheitsinfrastruktur. Aus diesem Grund haben Schulungs- und Weiterbildungsangebote sowie Sensibilisierungskampagnen im Rahmen des Projektes einen hohen Stellenwert. Hierzu stellen wir eine Online-Lernplattform mit Fortbildungs- und Schulungsangeboten zur Verfügung und führen natürlich auch Präsenz-Schulungen und Fortbildungen durch. Auch der regelmäßige Austausch der IT-Beauftragten der Kommunen, die Zurverfügungstellung eines IT-Forums als Wissensdatenbank und die regelmäßige Durchführung von Anti-Pishing-Kampagnen sind Teil dieser zweiten Säule des Projektes.

3. Konkrete Unterstützung bei der technischen Absicherung der IT-Infrastruktur: Um das Ziel eines einheitlichen IT-Sicherheitsniveaus in allen Kommunen im Landkreis Gießen zu erreichen, werden im Rahmen des Projektes konkrete Hilfestellungen in Bezug auf technische Fragestellungen gegeben. In diesem Zusammenhang bieten wir eine enge Beratung und auch die Möglichkeit gemeinsamer Beschaffungen an.

Auch wenn es keine absolute Sicherheit gegen Cyberangriffe geben wird, so ist das Ziel unseres Cybersicherheitsprojektes, dass wir gemeinsam im interkommunalen Verbund eine robuste Antwort auf die immer weiter zunehmende Bedrohungslage durch Cyberangriffe geben können.

Zudem möchten wir neue und weitergehende Formen der Kooperation zwischen dem Landkreis und den Kommunen eröffnen, beispielsweise bei der gemeinsamen Nutzung von Fachanwendungen, was natürlich ein hohes Maß an IT-Sicherheit auf beiden Seiten voraussetzt.

Digitale Ausführungen zu unserem interkommunalen Projekt schließen sich auf den nachfolgenden Seiten an.

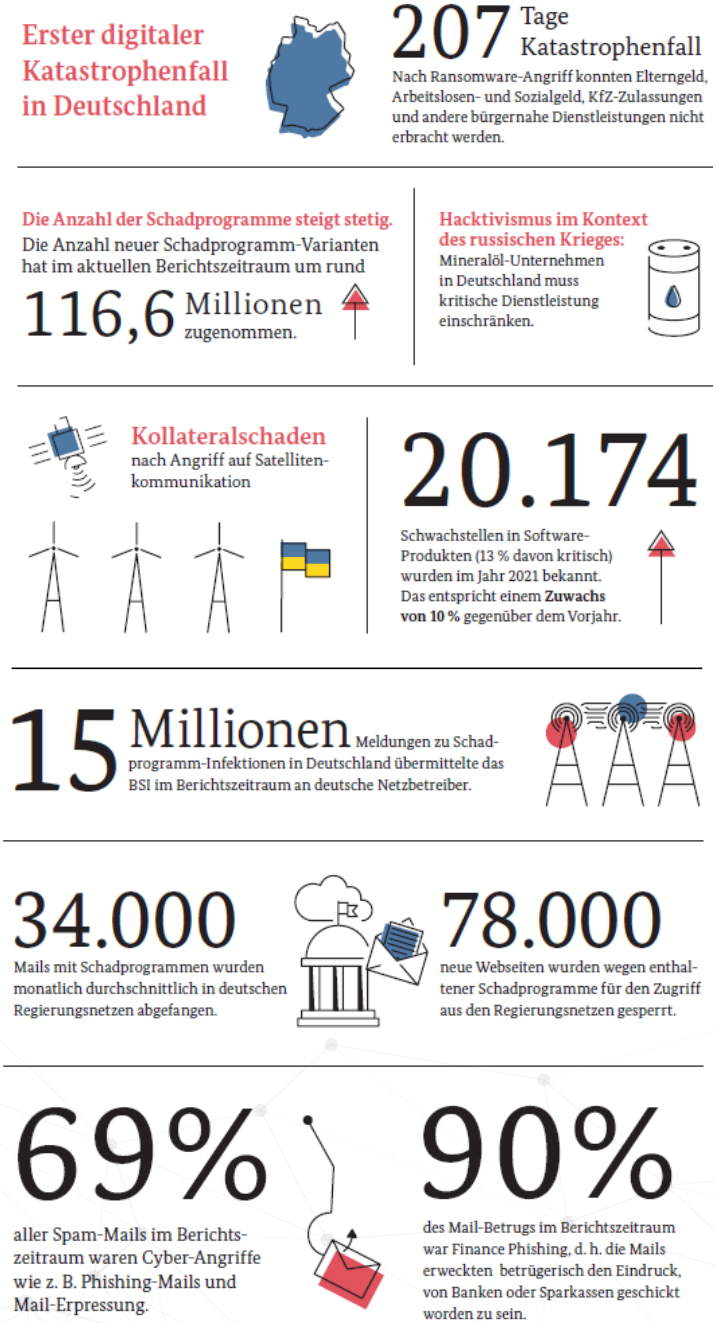
DIGITALISIERUNG DER VERWALTUNG SICHER GESTALTEN

CYBERSICHERHEIT ALS INTERKOMMULES PROJEKT IM LANDKREIS GIESSEN

David Pöhlmann,
Informationssicherheitsbeauftragter,
Landkreis Gießen

Landkreis Gießen
HESSENS MITTE • WISSEN WIRTSCHAFT & KULTUR

Die Lage der IT-Sicherheit in Deutschland 2022



BSI Bericht: Die Lage der IT-Sicherheit in Deutschland 2022

Ziele

Zielsetzung des interkommunalen Projektes

- Ausbau der Informationssicherheit in den Kommunen weiter verstärken, um eine robuste Antwort auf mögliche Cyberangriffe bieten zu können
- Informationssicherheit in allen teilnehmenden Kommunen auf ein Niveau heben, das an den BSI IT-Grundschutz angelehnt ist
- Zurverfügungstellung von qualifiziertem Fachpersonal, um auf die dynamische Bedrohungslage durch Cyberangriffe reagieren zu können
- Nutzung weiterer Synergien beim Ausbau der IT-Sicherheit und perspektivisch noch engere Zusammenarbeit zwischen Landkreis und Kommunen, z.B. bei Fachanwendungen

Leistungsumfang des interkommunalen Projektes

- Beratung der Behördenleitung
- Bereitstellung eines kompetenten Ansprechpartners (Cybersicherheitsbeauftragter)
- Gesamtkoordination des Informationssicherheitsprozesses
- Initiierung von Sensibilisierungs- und Schulungsmaßnahmen sowie eLearning-Angeboten
- Erstellung von Sicherheits- und Notfallkonzepten
- Warnung vor aktuellen Angriffsszenarien und Information zu möglichen Handlungsempfehlungen
- Untersuchung von Sicherheitsvorfällen
- Koordination von möglichen Synergieeffekten wie z. B. gemeinsame Projekte im Rahmen von Fortbildungen, Konfiguration von Sicherheitssystemen, Konzeptionieren von Schließ- und Zugangssystemen
- Betrieb eines gemeinsamen IT-Forums zum Austausch von Informationen (Wissensdatenbank, Konzepte, Vorlagen, Ausschreibungen etc.)
- Organisation und Durchführung von Arbeitskreisen und Informationsveranstaltungen
- Durchführung von Anti-Phishing-Kampagnen

Landkreis Gießen
HESSENS MITTE • WISSEN WIRTSCHAFT & KULTUR

Vorteile

Die Vorteile für die Beteiligten sind:

- Ein einheitlicher, qualitativ hoher Sicherheitsstandard
- Die Nutzung des bereits vorhandenen und Aufbau eines fachlichen „Know-Hows“ auf hohem Niveau zu wirtschaftlich günstigen Konditionen
- Einsparung von Kosten und Nutzung von Synergieeffekten durch die Zusammenarbeit
- Durch einen hohen Sicherheitsstandard auf beiden Seiten ist eine zukünftige, engere Zusammenarbeit möglich (Personalamt / Finanzabteilung / Revision).

Vereinbarung und Finanzierung

Öffentlich-rechtliche Vereinbarung:

- Der Landkreis Gießen hat mit allen 18 kreisangehörigen Kommunen eine öffentlich-rechtliche Vereinbarung geschlossen.
- Die Vereinbarung regelt die Einstellung eines IT-Sicherheitsbeauftragten als Projektbeauftragten und einer Projektassistenz sowie die Dienstleistungen für alle teilnehmenden Kommunen.
- Projektlaufzeit 5 Jahre: 01.08.2022 – 31.07.2027.

Finanzielle Auswirkungen:

- Die Finanzierung des Projekts erfolgt sowohl aus Eigenmitteln des Landkreises Gießen (50 Prozent) und Kostenerstattungen der teilnehmenden kreisangehörigen Kommunen (50 Prozent).
- Die teilnehmenden Kommunen erstatten dem Landkreis Gießen ein jährliches Entgelt, welches sich an der Einwohnerzahl der jeweiligen Kommune orientiert.

Projektdurchführung

Erste Schritte:

- Ermittlung des IT IST-Standes bei den teilnehmenden Kommunen
- Besichtigung der technischen Gegebenheiten und „Schwachstellen-Scan“ bei den Kommunen
- Informieren und Beraten bei Bekanntwerden neuer Sicherheitslücken
- Auftaktveranstaltung „Arbeitskreis Cybersicherheit“
- Hessen3C/Ekom21 Schulung „Notfallmanagement“ (HECAAZ)
- Informationsveranstaltung Cyberversicherung
- Einrichten der ILIAS Lernplattform (Online-Schulungen) für Kommunen
- Bereitstellen von Infomaterial, Leitfäden und gemeinsam nutzbaren Dokumentenvorlagen (IT-Forum auf der ILIAS-Plattform)
- Initiales Erstellen und Pflegen benötigter Dokumentationen gemeinsam mit den Verantwortlichen vor Ort
- Planen und Terminieren von präzisen Maßnahmen zur Erhöhung der IT-Sicherheit an den einzelnen Standorten
- Beginn der Erstellung von individuellen Notfallplänen für Sicherheitsvorfälle

Landkreis Gießen
HESSENS MITTE • WISSEN WIRTSCHAFT & KULTUR

Ausblick

Ausblick I:

- Weiterer Ausbau des Projektes, um eine weitergehende interkommunale IT-Zusammenarbeit zwischen dem Landkreis und einzelnen Kommunen zu etablieren.
- Redundanzen schaffen, die sowohl Kosten sparen als auch die Kommunen in die Lage versetzen IT-grundschutzkonforme IT-Systeme zu betreiben, um ein einheitliches Datenschutz- und IT-Sicherheitsniveau zu erhalten.
- Voraussetzungen für eine tiefgreifendere interkommunale Zusammenarbeit (z. B. Finanzwesen, Personalwesen etc.).

Ausblick II:

- Netzwerkstrategie: Konzept zum Aufbau von Netzwerken zum Anbinden von Außenstellen und für Home-Office (VPN).
- Hilfe und Unterstützung bei der Einrichtung und Planung von Sicherheitseinrichtungen wie z.B. Firewalls, Virenscanner.
- Gemeinsame Beschaffungen/Ausschreibungen zum Erzielen von Synergien und Rabatten.
- Prozessbeobachtung bei der Umsetzung von Projekten wie z.B. E-Mail-Verschlüsselung und Einführung der E-Akte.
- Gemeinsame Sensibilisierungskampagne, z.B. regelmäßiger neuer „IT-Sicherheitstipp“ als Plakat, Flyer und digitalen Newsletter.

Ausblick III:

- Präsenzschulungen vor Ort mit Live-Hacking.
- Ausbau des Anti-Phishing-Angebotes zur permanenten Sensibilisierung der Mitarbeiterinnen und Mitarbeiter mit verschiedenen Kampagnen in den einzelnen Fachdiensten und dazu angepassten Online-Schulungen.
- Aufbau und Ausbau des Kursangebotes auf einer gemeinsamen E-Learning-Plattform mit Tests und Zertifikaten.
- Zertifikat bescheinigt ein erfolgreich geprüftes Grundwissen im geprüften Bereich und dient zwei Zwecken: Bescheinigung für Mitarbeiterinnen und Mitarbeiter sowie Nachweis der Behördenleitung über die Sensibilisierung.

KOMPETENZCENTER KOMMUNAL DIGITAL

DER LANDKREIS IN RICHTUNG DIGITAL-DIENSTLEISTER FÜR SEINE KOMMUNEN

WIE DER LANDKREIS MARBURG-BIEDENKOPF BESTEHENDE UND ERFOLGREICHE IKZ-PROJEKTE BÜNDELN UND ERWEITERN MÖCHTE.

Philipp Stöhr, Fachdienstleiter Digitale Dienste und Open Government, Chief Digital Officer, Landkreis Marburg-Biedenkopf

LANDKREIS MARBURG BIEDENKOPF

Mit dem neuen Kompetenzcenter Kommunal Digital will die Kreisverwaltung Marburg-Biedenkopf ihren kreisangehörigen Städten und Gemeinden eine noch bessere und zudem ganzheitliche Unterstützung im großen Bereich der Digitalisierung bieten. Der Landkreis agiert hier als zentraler Ansprechpartner für die Kommunen und unterstützt den Kompetenzaufbau im Bereich digitale kommunale Zusammenarbeit.

Dazu werden die bereits bestehenden Projekte interkommunaler Zusammenarbeit (IKZ) in das Kompetenzcenter integriert, dort fortgeführt und auch verstetigt. Die seit 2017 bestehende **IKZ Geodateninfrastruktur (GDI)** ist eines dieser Projekte. Ziel ist es, geodatenbasierte Themen des Landkreises in einem Kartensystem darzustellen und der Kreisgesellschaft, aber auch den Verwaltungsmitarbeitenden selbst, zur Verfügung zu stellen. So können beispielsweise, ähnlich wie bei Google Maps, Schulstandorte, Bauleitpläne, Baustellen oder E-Bike-Ladestationen eingesehen werden. Das Geoportal steht Bürgerinnen und Bürgern bereits zur Verfügung und kann jederzeit genutzt werden.

Weiterhin ist auch die **IKZ Cybersicherheit** Teil des Kompetenzcenters. Das Projekt dient der Schaffung und Erhöhung eines einheitlichen und anerkannten IT-Sicherheitsniveaus im Landkreis, was auch für den Datenschutz der Bürgerinnen und Bürger enorm wichtig ist. Eindrucksvoll zeigen schon die einfachsten Phishing-Kampagnen per E-Mail: Der Mensch ist unsere beste Firewall oder eben auch Einfallstor für potenzielle Gefahren. Maßnahmen wie eben genannte Phishing-Kampagnen sind ein fest integrierter Bestandteil der laufenden Zusammenarbeit – mit regelmäßigen Wiederholungen, viel Staunen und auch mit Überraschungen. Das Projekt verlief bisher sehr erfolgreich und soll auf Wunsch der Kommunen dauerhaft fortgeführt werden – nun unter dem Dach des Kompetenzcenters Kommunal Digital.

Auch die Koordination und Beratung im Bereich **Onlinezugangsgesetz (OZG)** wird im Zentrum abgebildet. Das Gesetz verpflichtet Bund, Länder und Kommunen dazu, sämtliche Verwaltungsleistungen auch digital anzubieten. Um die Kommunen in der Umsetzung weiterhin zu unterstützen, ist auch dieses Projekt Teil von Kommunal Digital.

Neben der Bündelung bereits bestehender Digitalisierungsprojekte im Kompetenzcenter, sollen auch neue Themenbereiche aufgenommen und bearbeitet werden. Der Bereich **Smart Region** beispielsweise bietet für unsere Städte und Gemeinden enorm viel Potenzial, um nutzenorientierte Digitalisierungsmöglichkeiten für die Bürger*innen anzubieten. So ist es in einer Smart Region z.B. möglich, die Pegel- und Wasserstände von Kanalisation oder Gewässern automatisiert zu überwachen und die Bevölkerung frühzeitig zu warnen oder mittels Sensorik einen Dienstleister zu beauftragen, bevor der Glascontainer hoffnungslos überläuft. Auch in weiteren Smart-Region-Bereichen, wie z. B. Gesundheit, Mobilität oder Umwelt, möchte die Kreisverwaltung den Kommunen als kompetente Ansprechpartnerin zur Seite stehen, sie beraten und in der Umsetzung unterstützen.

Zudem ist es weiterhin geplant, auch eine technische Beratung und Unterstützung bei weiteren Digitalisierungsthemen wie Chatbot, Behördennummer 115 oder auch der technischen OZG-Umsetzung aus dem Zentrum heraus anzubieten.

Damit die Umsetzung des Gesamtvorhabens gelingt, soll der Fachdienst Digitale Dienste und Open Government, in dem das Kompetenzcenter bei der Kreisverwaltung Marburg-Biedenkopf beheimatet ist, u. a. weitere personelle Unterstützung erhalten. Die Kosten für die Projekte im Zentrum sollen über Fördermittel und finanzielle Beiträge der Kommunen gedeckt werden, Grundlage wird dazu eine öffentlich-rechtliche Vereinbarung zwischen Kommunen und Landkreis bilden. Bisher haben sich im Rahmen eines Interessensbekundungsverfahrens 19 Kommunen für die Zusammenarbeit ausgesprochen (Stand Dezember 2022).

Für die Kreisverwaltung und die Kommunen des Landkreises bildet das Kompetenzcenter zukünftig die Basis für die Zusammenarbeit im Themenfeld Digitalisierung. Grundlagen wie Cybersicherheit können dabei direkt mitbedacht werden. Dadurch lassen sich nicht nur Synergien effizienter nutzen, sondern auch der Zugang zu Digitalisierungsangeboten und deren Struktur wird durch eine effiziente und effektive Arbeit im Zentrum vereinfacht. Vor allem aber stärkt das Kompetenzcenter die Arbeitsgemeinschaft im gesamten Landkreis sowie die Kooperationen unter- und miteinander – ein Gewinn für alle.

Kreisausschuss Marburg-Biedenkopf

Kompetenzcenter Kommunal Digital

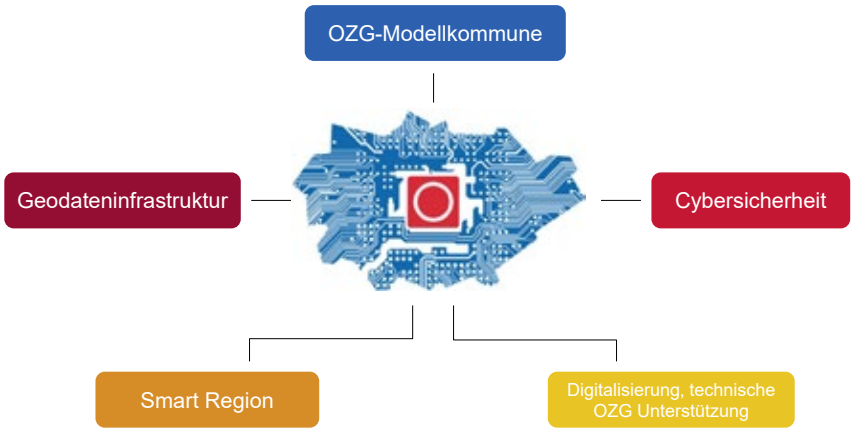
Der Landkreis in Richtung Digitaldienstleister für seine Kommunen

Fachtagung Interkommunale Zusammenarbeit
im Bereich der Cybersicherheit | 13. Dezember 2022 | Wiesbaden

Phishing Kampagne 2022

LANDKREIS MARBURG BIEDENKOPF

Übersicht



Cybersicherheit

Laufzeit	Teilnehmende Kommunen	Ziele	Fazit
01.08.2017 - 31.07.2022	26 Kommunen + 2 Landkreise	• Erhöhung und Schaffung eines einheitlichen anerkannten IT-Sicherheitsniveaus welches an den IT-Grundschutz des BSI anlehnt	• Erfolgreicher Abschluss dieses Jahr und Auslaufen zum 31.07. • Sehr positives Feedback & Verstetigung durch Kommunen gewünscht

Geodateninfrastruktur

Laufzeit	Teilnehmende Kommunen	Ziele	Fazit
01.01.2017 – 5 Jahre – automatische Verlängerung	21 Kommunen + 1 Landkreis	• Gemeinsamer Geodatenserver betreiben (Bauleitplanung) • GIS-Themen gemeinsam darstellen (Baustellen, Hochwasser, Sirenen)	• Einstimmige Entscheidung bereits gezahlte Gelder beim LK für die Umsetzung weiterer Projekte zu belassen • Erfolgreicher Wissenstransfer auf Nachfolger und aktuelle Planung weitere Projekte

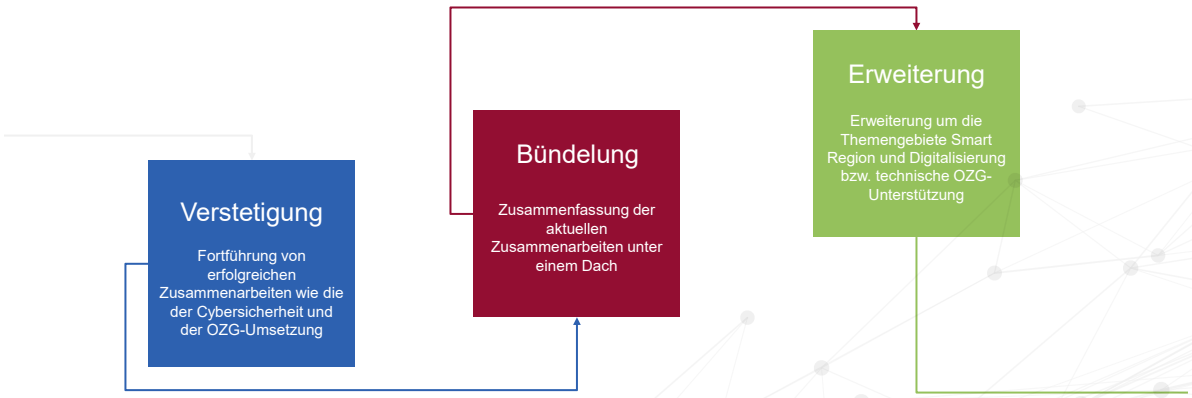
OZG-Modellkommune

Laufzeit	Teilnehmende Kommunen	Ziele	Fazit
01.08.2021 - 31.07.2023	16 Kommunen + 1 Landkreis	• Koordinierende und beratende Unterstützung bei der Umsetzung des Onlinezugangs-gesetzes (OZG)	• Positiver Anlauf und bereits erste Fortschritte • Mehrheitlicher Wunsch d. Kommunen neben Koordinierung auch technische Unterstützung anzubieten und diese mit zu finanzieren

Smart Region / Digitalisierung und OZG-Technik

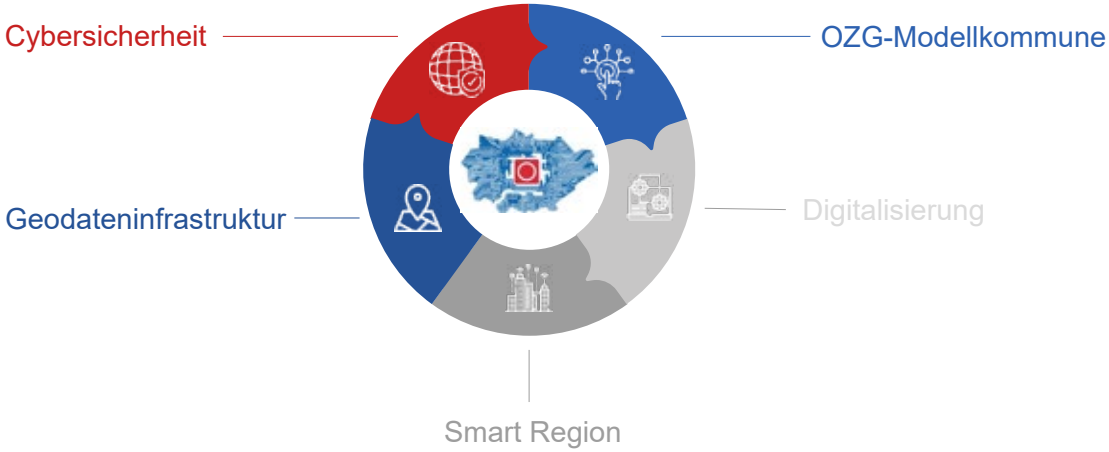
	Laufzeit	Ziele
Smart Region	so lange wie notwendig	• Förderung der **digitalen Daseinsvorsorge** im **ländlichen Raum** • Nutzenbasierte Implementierung von **digitalen Lösungen zur Erhöhung der Lebensqualität** • **Koordinierung, Beratung und Unterstützung** in der Umsetzung von **smarten Digitalisierungsprojekten** • Integration einer vorhandenen Personalressourcen
Digitalisierung OZG Technik	so lange wie notwendig	• **Technische Unterstützung** bei der OZG-Umsetzung (gemeinsamer Civento Prozess Designer) • **Unterstützung und Beratung** bei weiteren Digitalisierungsprojekten z.B. Chatbot oder Behördennummer 115 • Schaffung weiterer Personalressourcen

Prozess



LANDKREIS MARBURG BIEDENKOPF

Bündelung



Ziele der Zusammenarbeit

Ganzheitlichere Unterstützung
Noch bessere und ganzheitlichere Unterstützung der Städte und Gemeinden

Landkreis als Digital-Dienstleister
Ein Ansprechpartner für Kommunen

Zusammenführung und Bündelung
Zusammenführung und Bündelung der verschiedenen Projekte/Ressourcen

Erweiterung der Themen
Smart Region, Digitalisierung und technische Unterstützung

Weiterer Kompetenzaufbau
Zentraler Kompetenzaufbau im Bereich digitale kommunale Zusammenarbeit

Verstetigung erfolgreicher Projekte
Wie am Beispiel Cybersicherheit

Vorteile der Zusammenarbeit

Nutzung von Synergien
Durch die Kombination aus dem Know-how und die Zusammenführung ergeben sich neue Impulse

Zeitersparnis und Effiezienz
Gleiche Ansprechpersonen der Kommunen, Arbeitskreise, Themen

Vereinfachung durch Strukturierung
Strukturierung der vorhandenen Angebote sowie der Organisation (bspw. einheitliche Vereinbarung)

Kontinuierliche Zusammenarbeit
Aufbau einer kontinuierlichen Zusammenarbeit/Unterstützung

Leistungen

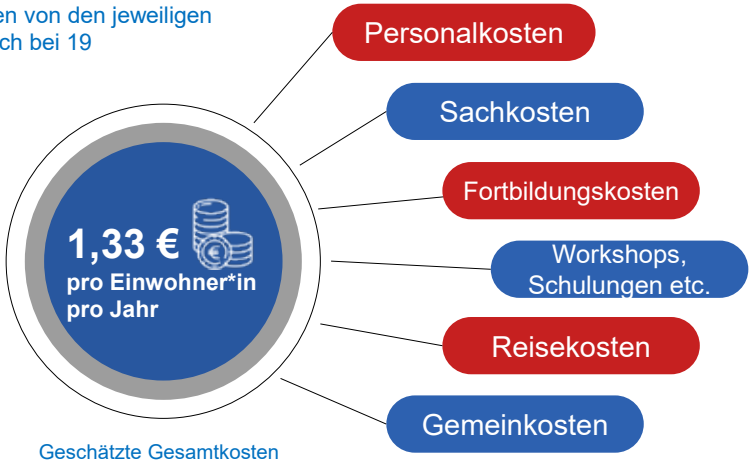
- **Beratung** auf strategischer sowie operativer Ebene
- **Informationsaufbereitung** und Weitergabe von Informationen (z.B. Neuigkeiten, Sicherheitswarnungen, …)
- **Koordination / Durchführung von Maßnahmen** mit **Synergieeffekten**
- **Dokumentation** und **Begleitung** von Maßnahmen
- **Vertretung** in verschiedenen **Gremien**, bspw. auf Landesebene
- Vorbereitungen von zentralen Empfehlungen
- **Organisation** von Arbeitskreisen, Workshops, Produktpräsentationen, etc.
- **Erstellen und Durchführen** von **Schulungen** und **E-Learnings**
- **Vernetzung** und Fördern des **Austauschs untereinander**
- **Zentraler Betrieb** von Softwarelösungen wie **Projektplattform**, **ViKo-Systeme, Phishing-Backend,…**
- **Unterstützung** bei **Erstellung Leitlinien**, Einführung von ISMS, usw.
- **Berichte** und **Überzeugungsarbeit in politischen Gremien**
- **Alles was Sinn macht und möglich ist…**

Angebot nach Baukastenprinzip:
Kommunen können passgenau die Bausteine (= Leistungen) auswählen, die sie benötigen

Kostenplanung

Die Kosten für die Kommunen hängen von den jeweiligen Einwohnerzahlen an und belaufen sich bei 19 teilnehmenden Kommunen auf:

- Zu Beginn werden die Kosten geringer ausfallen, da noch nicht alle IKZ Projekte inkludiert sind
- Eine etwaige Förderung konnte noch nicht berücksichtigt werden, ein Förderantrag ist in Vorbereitung



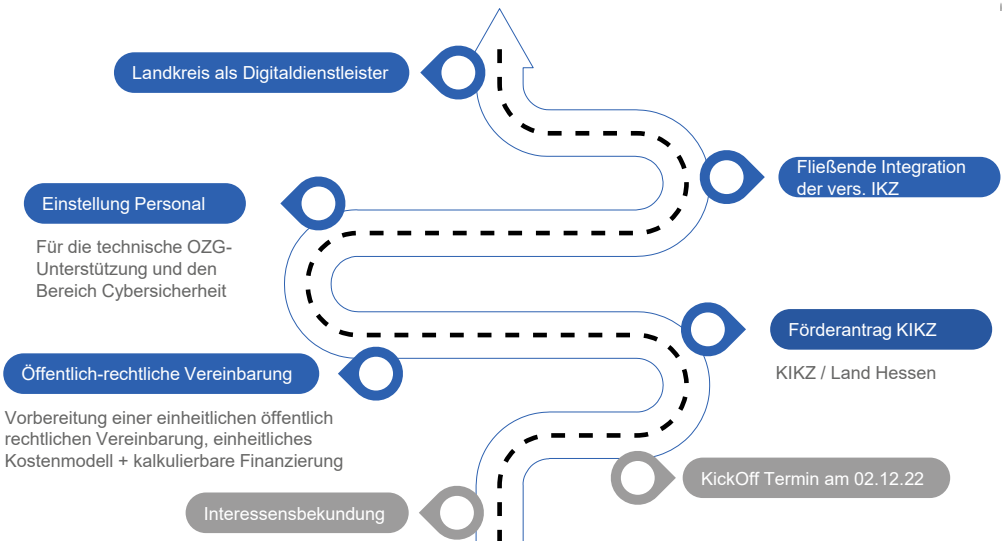
Geschätzte Gesamtkosten von 193.056,15 € pro Jahr

Teilnehmende Kommunen

- Amöneburg
- Angelburg
- Biedenkopf
- Cölbe
- Ebsdorfergrund
- Fronhausen
- Kirchhain
- Neustadt (Hessen)
- Steffenberg
- Weimar (Lahn)
- Wohratal
- Gladenbach
- Dautphetal
- Breidenbach
- Lohra
- Bad Endbach
- Wetter (Hessen)
- Lahntal
- Münchhausen

LANDKREIS MARBURG BIEDENKOPF

Roadmap



Kickoff Termin am 02.12.2022

- Organisatorisches, Kommunikation, Ansprechpersonen aus den Kommunen
- Vorstellung der verschiedenen Themenbereiche und Ansprechpersonen
- Inhaltlicher Schwerpunkt OZG-Umsetzung mit Best-Practises aus anderen Kommunen
- Austausch und Vernetzung
- …

Vielen Dank für Ihre Aufmerksamkeit !

Wenden Sie sich bei Fragen gerne an

Philipp Stöhr
Fachdienstleiter, Chief Digital Officer (CDO)
StoehrP@marburg-biedenkopf.de

Stabsstelle Dezernatsbüro des Landrats
FD 13.5 - Digitale Dienste und Open Government
Im Lichtenholz 60 • 35043 Marburg

FÖRDERUNG DER INTERKOMMUNALEN ZUSAMMENARBEIT VON KOMMUNEN

VORAUSSETZUNG EINES VOLLSTÄNDIGEN UND ERFOLGREICHEN IKZ-ANTRAGS

Andrea Reusch-Demel, Referatsleiterin Kommunale Strukturen und Interkommunale Zusammenarbeit, Hessisches Ministerium des Innern und für Sport

HESSEN

Meine sehr geehrten Damen und Herren,

ich darf die heutige sehr informative Veranstaltung abschließen und möchte einen Bogen über die Vorträge schlagen. Wir haben am Vormittag schon gehört, welche Herausforderungen durch die Thematik „Cybersicherheit" an Sie als Kommunen gestellt werden. Insbesondere die „Best Practice"-Beispiele haben aber auch eindrucksvoll unterstrichen, welche Chancen in einer Zusammenarbeit von Kommunen liegen können.

Das Projekt des Landkreises Gießen ist nach der Rahmenvereinbarung zur Förderung der Interkommunalen Zusammenarbeit (IKZ-Rahmenvereinbarung) gefördert worden und hat heute im Rahmen der Veranstaltung von Herrn Staatssekretär Sauer einen Förderbescheid übergeben bekommen.

Ich möchte Sie mit meinem Vortrag bei der Stellung eines erfolgreichen IKZ-Antrags unterstützen und Ihnen daher erläutern: Wie wird ein Antrag gestellt, welche Voraussetzungen sind für einen erfolgreichen Antrag erforderlich, was ist bei der Antragstellung zu beachten?

Ich bedanke mich an dieser Stelle herzlich bei den Kollegen des Landkreises Gießen, die mir freundlicherweise einzelne Dokumente Ihres Antrags zur Verfügung gestellt haben, damit ich Ihnen anhand des konkreten Beispiels hilfreiche Tipps und Vorlagen geben kann, die Ihnen sicher weiterhelfen werden.

Einleitend habe ich Ihnen die erste Seite der IKZ-Rahmenvereinbarung eingeblendet, sie dürfte den meisten von Ihnen bekannt sein. Sie finden die IKZ-Rahmenvereinbarung auf der Homepage der Stabstelle „Kommunales Beratungszentrum Hessen" bzw. auf der Internetseite des Hessischen Innen-ministeriums.

In der IKZ-Rahmenvereinbarung sind die konkreten Voraussetzungen für die Antragstellung und das Antrags- und Bewilligungsverfahren festgehalten, aber dazu werde ich im Laufe meines Vortrages noch näher eingehen.

Bestandteile des IKZ-Antrags sind nach der IKZ-Rahmenvereinbarung ein Anschreiben, eine schriftliche Vereinbarung, die jeweiligen Gremienbeschlüsse und die Effizienzberechnung.

Das **Anschreiben** ist ein formloses Schreiben, d. h., es gibt keine zwingenden Vorgaben für den Inhalt und die Form. Im Gegensatz zu anderen Förderverfahren wird kein Formular bzw. keine Maske vorgeben, welche dann auszufüllen sind. Vielmehr bleibt Ihnen der Umfang und die Tiefe der Schilderung überlassen. Vorteilhaft ist es, wenn anhand der Schilderung für einen Außenstehenden erkennbar ist, wie die Kooperation ausgestaltet sein soll. Aus dem Inhalt sollte sich daher herauslesen lassen, in welchem Aufgabenbereich eine künftige Zusammenarbeit beabsichtigt ist, welche Kommunen beteiligt sind und wie die Zusammenarbeit konkret aussehen soll (z. B. gibt es eine Kommune, die die Aufgaben für die anderen erledigt oder wer ist für welche Teilbereiche zuständig). Zudem sollte noch kurz erläutert werden, auf welcher rechtlichen Grundlage Sie zusammenarbeiten wollen. Optional ist ein kurzer Ausblick, wie die künftige Zusammenarbeit ausgestaltet sein soll, z. B. ob eine spätere Erweiterung der Kooperation möglich ist bzw. sogar angestrebt wird.

Das „Kernstück" des Antrags ist die **schriftliche Vereinbarung,** denn diese ist die rechtliche Grundlage für die Kooperation. Wie Sie der IKZ-Rahmenvereinbarung entnehmen können, gibt es für Sie vielfältigste Möglichkeiten. Zum einen stehen Ihnen die Kooperationsformen nach dem Gesetz über Kommunale Gemeinschaftsarbeit (KGG) zur Verfügung (Zusammenarbeit in Form einer Arbeitsgemeinschaft, als Zweckverband, über eine öffentlich-rechtliche Verein-barung oder gemeinsame kommunale Anstalt). Möglich ist darüber hinaus, dass die Beteiligten einen öffentlich-recht-lichen Vertrag nach § 54 Hessisches Verwaltungsverfahrensgesetz abschließen oder sich für eine Kooperationsform nach Privatrecht (z. B. GmbH) entscheiden.

Nach den bisherigen IKZ-Anträgen, die meinem Referat zur Prüfung vorgelegt wurden, ist festzustellen, dass am häufigsten eine öffentlich-rechtliche Vereinbarung als rechtliche Grundlage genommen wird. Die öffentlich-rechtliche Vereinbarung bietet den Vorteil, dass sie auf die Kooperation sehr flexibel angepasst werden kann und nicht wie eine Satzung beim Zweckverband eine starre Regelung mit hohen Formerfordernissen ist.

Anhand der öffentlich-rechtlichen Vereinbarung des Landkreises Gießen für das Projekt „Cybersicherheit" können Sie gut nachvollziehen, welche Regelungen enthalten sein sollten, wobei eine Anpassung auf den jeweiligen Einzelfall zu erfolgen hat.

Aus der öffentlich-rechtlichen Vereinbarung müssen alle Vertragsparteien zu erkennen sein, auch sollte die jeweilige Rechtsgrundlage zu Beginn zitiert werden. Zudem sollten Regelungen bezüglich des Aufgabenbereichs enthalten sein und ggfs. aus welchem Grund zukünftig zusammengearbeitet werden soll. Empfehlenswert sind Festlegungen hinsichtlich der konkreten Aufgaben der Vertragsparteien und einer Kostenregelung im Innenverhältnis. Zwingender Bestandteil der öffentlich-rechtlichen Vereinbarung ist eine Regelung zur Laufzeit der Kooperation, die mindestens auf 5 Jahre angelegt sein muss.

Zur Klärung von Fragen und um zu vermeiden, dass die jeweilige schriftliche Vereinbarung im Laufe des weiteren Verfahrens nachgebessert werden muss, wird empfohlen im Vorfeld eine Abstimmung mit der jeweiligen Aufsichtsbehörde durchzuführen.

Dem Antrag sind zudem die **Beschlüsse der obersten kommunalen Organe** der beteiligten Kommunen, d. h. der Gemeindevertretung, der Stadtverordnetenversammlung bzw. Kreistages beizufügen.

Eine Beschlussfassung „nur" der Verwaltungsbehörden (Gemeindevorstand, Magistrat bzw. Kreisausschuss) ist nicht ausreichend, denn die von Ihnen angestrebte IKZ fußt auf der gemeinsamen Erledigung von Aufgaben innerhalb einer Kooperation, d. h. es sind konkrete Zuständigkeiten der beteiligten Kommune betroffen. Damit handelt es sich um eine wesentliche Angelegenheit der Kommune.

Grundlage für die Beschlussfassung in den Gremien ist eine Vorlage. Damit eine einheitliche zweifelsfreie Beschlussfassung in allen beteiligten Kommunen gegeben ist, wird eine einheitliche Vorlage empfohlen, so dass kein Raum für spätere Interpretationen bzw. auch Missverständnisse bleibt.

So hat es auch der Landkreis Gießen gehandhabt. Der Vorlage ist eine Beschreibung der Zusammenarbeit nebst der finanziellen Auswirkung zu entnehmen, um den Gremienmitgliedern eine fundierte Grundlage für diese Entscheidung zu geben. Zudem ist ein Beschlussvorschlag enthalten, so dass in allen Kommunen einheitliche Gremienbeschlüsse gefasst werden können.

An dieser Stelle möchte ich den Hinweis geben, dass für die Antragsunterlagen ein „einfacher" Protokollauszug ausreichend ist, er muss nicht beglaubigt sein.

Als letzter Bestandteil des IKZ-Antrags ist eine **Effizienzberechnung** mit vorzulegen. Die IKZ-Rahmenvereinbarung definiert hierzu, „durch die Zusammenarbeit soll eine Einsparung der personellen und sächlichen Ausgaben in den kooperierenden Aufgabenbereichen von mindestens 15 v. H. pro Jahr erzielt werden (Effizienzgewinn)."

Die Darstellung der Effizienzberechnung erfolgt durch eine Gegenüberstellung der Kosten, die für die gemeinsame Aufgabenerledigung innerhalb der Kooperation entstehen mit den Kosten, die entstehen, wenn jede Kommune die Aufgaben selbstständig erledigt. Da es sich um eine zukünftige teilw. auch neue Aufgabenerledigung handelt, handelt es sich zum Zeitpunkt der Antragstellung um eine Prognose. Empfohlen wird aus Gründen der Übersichtlichkeit und einfacheren Nachvollziehbarkeit eine tabellarische Darstellung!

Zum besseren Verständnis möchte ich auf die sehr übersichtliche Darstellung des Landkreises Gießen (auf den nachfolgenden Seiten) verweisen. In der oberen Tabelle werden die künftigen zu erwartenden jährlichen Personal- und Sachkosten für die Kooperation dargestellt, die untere Tabelle umfasst die Kostenkalkulation, d. h. die Personal- und Sachkosten, die jeder der beteiligten Kommunen entstehen würden, wenn sie die Aufgaben separat erledigen würde. Aus der Differenz der beiden Summen ergibt sich der prognostizierte Effizienzgewinn. Die Berechnungsgrundlage bzw. den Berechnungsschlüssel für die Kostenkalkulation ohne Kooperation ist zur besseren Verständlichkeit gesondert abgebildet. Im vorliegenden Projekt hat man als Bedarfsschlüssel die Einwohnerzahlen der beteiligten Kommunen zu Grunde gelegt.

Abschließend möchte ich noch darauf hinweisen, dass diese Darstellung als Basis für den Sachbericht herangezogen werden kann, der im fünften Jahr des Bestehens der Kooperation vorzulegen ist.

Der Vollständigkeitshalber möchte ich Ihnen zum Abschluss noch den **Ablauf des Förderverfahrens** kurz schildern.

Eine der beteiligten Kommune hat die Federführung, d. h. sie stellt den Förderantrag und ist auch Adressat des Förderbescheides. An diese Kommune wird die bewilligte Fördersumme komplett ausgezahlt. Eine Verwendung bzw. Aufteilung innerhalb der Kooperation wird im Innenverhältnis geregelt.

Die Antragstellung erfolgt seit der neuen Rahmenvereinbarung 2021 auf elektronischem Wege. Der Dienstweg ist weiterhin einzuhalten, d. h. der Antrag wird über die zuständigen Aufsichtsbehörden dem Hessischen Innenministerium vorgelegt. Die Aufsichtsbehörden achten auf die Vollständigkeit des Antrages und geben eine eigene Bewertung ab.

Sodann erfolgt die Prüfung durch mein Referat, im Anschluss werden die Kommunalen Spitzenverbände eingebunden und danach die Zustimmung des Hessischen Finanzministeriums eingeholt. Nach der Unterzeichnung durch den Innenminister, erhält die antragstellende Kommune den Förderbescheid. Als Zeitrahmen können für das Prüfungsverfahren insgesamt zwei Monate veranschlagt werden.

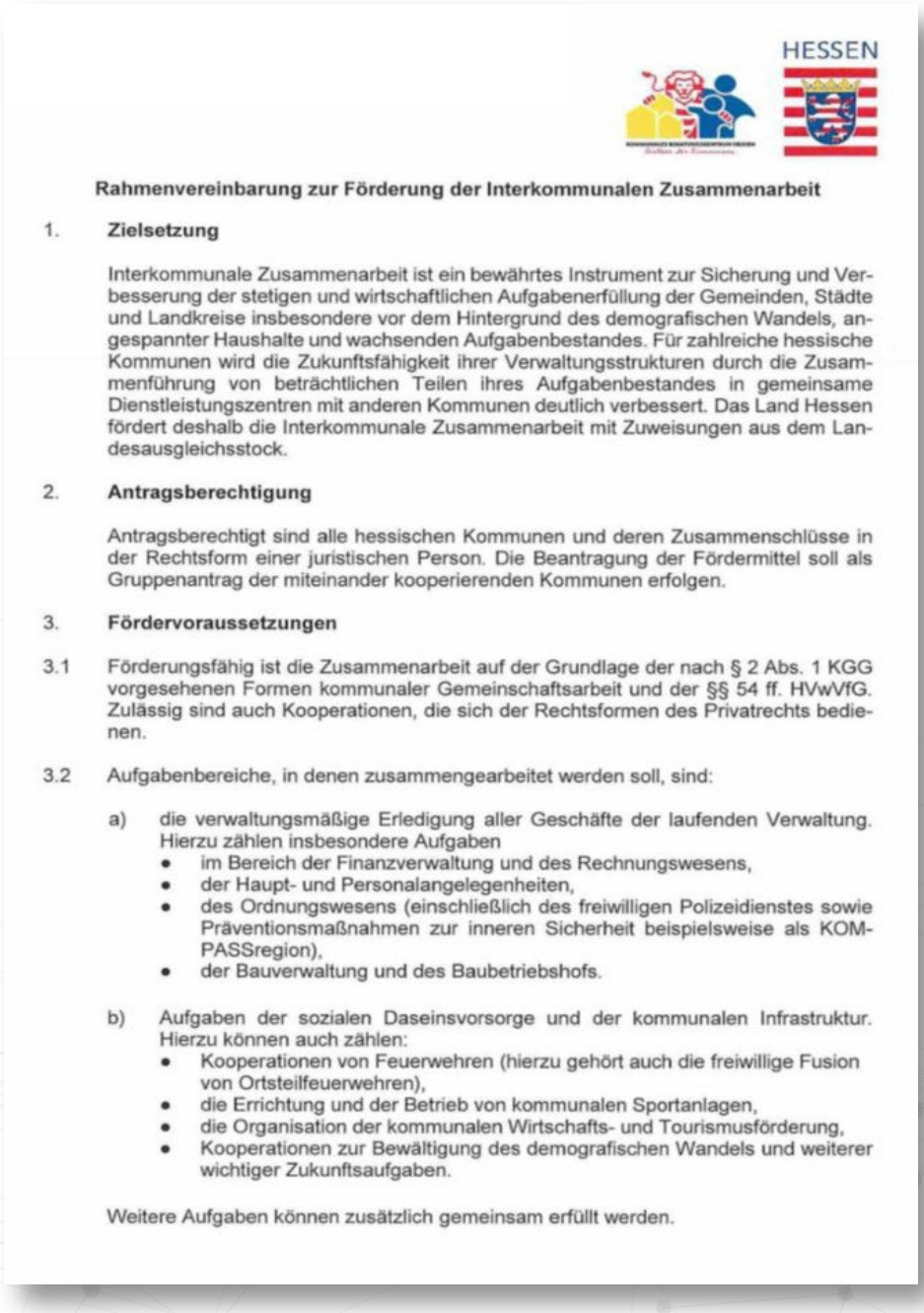
Ich bedanke mich für die Aufmerksamkeit.

HESSEN

Interkommunale Zusammenarbeit im Bereich der Digitalisierung

Förderung der interkommunalen Zusammenarbeit von Kommunen

Voraussetzungen eines vollständigen und erfolgreichen IKZ-Antrags



HESSEN

Rahmenvereinbarung zur Förderung der Interkommunalen Zusammenarbeit

1. **Zielsetzung**

Interkommunale Zusammenarbeit ist ein bewährtes Instrument zur Sicherung und Verbesserung der stetigen und wirtschaftlichen Aufgabenerfüllung der Gemeinden, Städte und Landkreise insbesondere vor dem Hintergrund des demografischen Wandels, angespannter Haushalte und wachsenden Aufgabenbestandes. Für zahlreiche hessische Kommunen wird die Zukunftsfähigkeit ihrer Verwaltungsstrukturen durch die Zusammenführung von beträchtlichen Teilen ihres Aufgabenbestandes in gemeinsame Dienstleistungszentren mit anderen Kommunen deutlich verbessert. Das Land Hessen fördert deshalb die Interkommunale Zusammenarbeit mit Zuweisungen aus dem Landesausgleichsstock.

2. **Antragsberechtigung**

Antragsberechtigt sind alle hessischen Kommunen und deren Zusammenschlüsse in der Rechtsform einer juristischen Person. Die Beantragung der Fördermittel soll als Gruppenantrag der miteinander kooperierenden Kommunen erfolgen.

3. **Fördervoraussetzungen**

3.1 Förderungsfähig ist die Zusammenarbeit auf der Grundlage der nach § 2 Abs. 1 KGG vorgesehenen Formen kommunaler Gemeinschaftsarbeit und der §§ 54 ff. HVwVfG. Zulässig sind auch Kooperationen, die sich der Rechtsformen des Privatrechts bedienen.

3.2 Aufgabenbereiche, in denen zusammengearbeitet werden soll, sind:

a) die verwaltungsmäßige Erledigung aller Geschäfte der laufenden Verwaltung. Hierzu zählen insbesondere Aufgaben
- im Bereich der Finanzverwaltung und des Rechnungswesens,
- der Haupt- und Personalangelegenheiten,
- des Ordnungswesens (einschließlich des freiwilligen Polizeidienstes sowie Präventionsmaßnahmen zur inneren Sicherheit beispielsweise als KOMPASSregion),
- der Bauverwaltung und des Baubetriebshofs.

b) Aufgaben der sozialen Daseinsvorsorge und der kommunalen Infrastruktur. Hierzu können auch zählen:
- Kooperationen von Feuerwehren (hierzu gehört auch die freiwillige Fusion von Ortsteilfeuerwehren),
- die Errichtung und der Betrieb von kommunalen Sportanlagen,
- die Organisation der kommunalen Wirtschafts- und Tourismusförderung,
- Kooperationen zur Bewältigung des demografischen Wandels und weiterer wichtiger Zukunftsaufgaben.

Weitere Aufgaben können zusätzlich gemeinsam erfüllt werden.

IKZ-Antrag

- Anschreiben (Ziffer 5 Abs. 3 und Ziffer 3 RV)
- Schriftliche Vereinbarung (Ziffer 3 Abs. 1 RV)
- Gremienbeschlüsse (Ziffer 5 Abs. 1 RV)
- Effizienzberechnung (Ziffer 3 Abs. 6)

IKZ-Antrag – **Anschreiben**

- **Darstellung/Umfang**
  - keine zwingenden Vorgaben
  - formloses Schreiben, keine Formalien wie in anderen Förderverfahren
  - Darstellung im Fließtext
- **Inhalt**
  - Beschreibung, Skizzierung der Kooperation:
    - Aufgabenbereich – wesentlicher Bereich (keine Investitionen)
    - beteiligte Kommunen
    - Rechtsform der Kooperation
    - Historie
  - Ausblick/Planung der künftigen Zusammenarbeit

IKZ-Antrag – **Schriftliche Vereinbarung**

- **Kernstück**

  (Kommunen in Gestaltung frei)
  - Kooperationsformen nach dem KGG - Gesetz über kommunale Gemeinschaftsarbeit - (Arbeitsgemeinschaft, öffentlich-rechtliche Vereinbarung, Zweckverband, gemeinsame kommunale Anstalt)
  - öffentlich-rechtlicher Vertrag nach § 54 HVwVfG - Hessisches Verwaltungsverfahrensgesetz -
  - Kooperationsformen nach Privatrecht (z.B. GmbH)
  - Regelung zur Laufzeit der Kooperation (mindestens 5 Jahre)

- ***Hinweis***: Abstimmung mit der zuständigen Aufsichtsbehörde im Vorfeld

HESSEN

Öffentlich-rechtliche Vereinbarung

über das Projekt

„Cybersicherheit in öffentlichen Verwaltungen im Landkreis Gießen“

zwischen dem

Landkreis Gießen,
vertreten durch den Kreisausschuss,
Riversplatz 1-9, 35394 Gießen,
dieser vertreten durch Frau Landrätin Anita Schneider und
Herrn Ersten Kreisbeigeordneten Christopher Lipp

– im Folgenden „**Landkreis Gießen**“ genannt –

und

der Stadt Allendorf (Lumda),
vertreten durch den Magistrat,
Bahnhofstraße 14, 35469 Allendorf,
vertreten durch
den Bürgermeister Thomas Benz und
die Erste Stadträtin Petra Sommerlad

und
…

– im Folgenden „**Vereinbarungspartner**“ genannt –

wird gemäß der §§ 24 Abs. 1 und 25 Abs. 1 und Abs. 2 des Hessischen Gesetzes über Kommunale Gemeinschaftsarbeit (KGG) vom 16.12.1969 (GVBl. I. S. 307), zuletzt geändert durch Artikel 1 des Gesetzes vom 11. Dezember 2019 (GVBl. I S. 416) die nachfolgende **öffentlich-rechtliche Vereinbarung** geschlossen:

Präambel

Im Rahmen des Pilotprojektes Cybersicherheit haben die Landkreise Marburg-Biedenkopf und Gießen bislang gemeinsam mit kreisangehörigen Städten und Gemeinden im Aufgabenfeld „Cybersicherheit in öffentlichen Verwaltungen“ über einen Zeitraum von fünf Jahren interkommunal zusammengearbeitet.

Das beschriebene Projekt hat sich in der Praxis gut bewährt und wird nun – nach dem Auslaufen des bisherigen übergreifenden Projektes zum 31. Juli 2022 – in überarbeiteter Form vom Landkreis Gießen mit den teilnehmenden kreisangehörigen Kommunen fortgeführt. Die nachfolgende öffentlich-rechtliche Vereinbarung bildet die Grundlage der Zusammenarbeit.

§ 1 Vertragsgegenstand

Modernes Verwaltungshandeln ist heute ohne elektronische Kommunikationsmedien und IT-Verfahren undenkbar. Mit der zunehmenden Digitalisierung der Verwaltungen nimmt auch der Schutzbedarf der IT-Systeme und der Daten zu. Um das Verwaltungshandeln zu gewährleisten, ist die Sicherheit und Verfügbarkeit der IT-Systeme und Daten sicherzustellen.

Zunehmende und immer zielgerichtetere Angriffsszenarien erfordern einen hohen Sicherheitsstandard. Das Erreichen dieses Sicherheitsstandards stellt für Städte und Gemeinden, die häufig nur über geringe personelle Ressourcen verfügen, eine kaum bewältigbare Aufgabe dar. Der Landkreis Gießen möchte mit seinen Ressourcen und Fachwissen die am Projekt teilnehmenden Kommunen unterstützen und beraten. Durch die Zusammenarbeit soll ein einheitlicher Standard an Informations- und Datensicherheit erreicht werden.

§ 2 Aufgaben der Vertragsparteien

(1) Zur Umsetzung der in § 1 genannten Ziele stellt der Landkreis Gießen für das Projekt einen Projektbeauftragten und eine Projektassistenz im Umfang von insgesamt 2,0 Vollzeitäquivalenten ein. Die Stelleninhaber arbeiten mit den themenbezogenen Organisationseinheiten der Kreisverwaltung Gießen zusammen und verfolgen die Zielsetzung einer umfassenden Unterstützung sämtlicher Vereinbarungspartner.

…

§ 3 Leistungsumfang

…

§ 4 Optionale Aufgaben

…

§ 5 Kosten

(1) Die Vereinbarungspartner erstatten dem Landkreis Gießen für die Erbringung der in § 3 und § 4 dieser Vereinbarung beschriebenen Aufgaben ein jährliches Entgelt, welches sich nach der am 30. Juni 2022 durch das Statistische Landesamt ermittelten Einwohnerzahl der jeweiligen Kommune zwischen den Vereinbarungspartnern aufteilt. Eine Übersicht der zu erwartenden Beträge der einzelnen Vereinbarungspartner auf der Grundlage der in § 5 Absatz 3 dargestellten jährlichen Projektkosten ist dieser Vereinbarung als Anlage beigefügt. Etwaige Fördermittelzuschüsse nach § 5 Absatz 6 oder Reduzierungen nach § 5 Absatz 4 dieser Vereinbarung bleiben bei dieser Übersicht zunächst unberücksichtigt.

…

§ 6 Personal

…

§ 7 Inkrafttreten/Geltungsdauer/Kündigung/Vertragsanpassung

(1) Diese Verwaltungsvereinbarung tritt am 01. August 2022 in Kraft, sofern mindestens die Hälfte der kreisangehörigen Kommunen als Vereinbarungspartner an dem Projekt teilnehmen. Diese Vereinbarung hat eine Laufzeit von fünf Jahren bis zum 31. Juli 2027 und verlängert sich jeweils um ein Jahr, sofern sie nicht spätestens sechs Monate vor ihrem Auslaufen von einer der Vertragsparteien aus wichtigem Grund gekündigt wird.

…

§ 8 Datenschutz

…

§ 9 Salvatorische Klausel

…

§ 10 Beitritt weiterer Vereinbarungspartner

…

§ 11 Schlussbestimmungen

…

Gießen, den . Juli 2022

Für den **Landkreis Gießen**

Anita Schneider
Landrätin

Christopher Lipp
Erster Kreisbeigeordneter

Für die **Stadt Allendorf (Lumda)**

IKZ-Antrag – **Gremien-Beschlüsse**

- **Gremien-Beschlüsse** = Gemeindevertretungen, Stadtverordnetenversammlung, Kreistag
- Nicht ausreichend sind Beschlüsse der Verwaltungsbehörden (Gemeindevorstand, Magistrat, Kreisausschuss)

- empfohlen wird eine **einheitliche** Vorlage
- Protokollauszug – muss nicht beglaubigt sein

HESSEN

Muster-Beschlussvorlage
Stadtverordnetenversammlung / Gemeindevertretung

Interkommunale Zusammenarbeit: Projekt „Cybersicherheit in öffentlichen Verwaltungen im Landkreis Gießen“

Beschluss-Antrag:

1 **Die Stadtverordnetenversammlung/Gemeindevertretung beschließt die Teilnahme am IKZ-Projekt „Cybersicherheit in öffentlichen Verwaltungen im Landkreis Gießen“.**

2 **Zur Umsetzung des Projektes wird der Magistrat/Gemeindevorstand beauftragt, mit dem Landkreis Gießen sowie den sonstigen teilnehmenden Kommunen eine entsprechende öffentlich-rechtliche Vereinbarung auf der Grundlage des als Anlage beigefügten Entwurfes abzuschließen.**

Begründung:

Im Rahmen des interkommunalen Projektes Cybersicherheit haben die Landkreise Marburg-Biedenkopf und Gießen bislang gemeinsam mit kreisangehörigen Städten und Gemeinden im Aufgabenfeld „Cybersicherheit in öffentlichen Verwaltungen“ über einen Zeitraum von 5 Jahren zusammengearbeitet. Das beschriebene Projekt hat sich in der Praxis gut bewährt und soll nun – nach dem Auslaufen des bisherigen übergreifenden Projektes zum 31. Juli 2022 – in überarbeiteter Form vom Landkreis Gießen mit seinen kreisangehörigen Kommunen fortgeführt werden.

Ziel des Projektes ist es, Maßnahmen auf dem Gebiet der Cybersicherheit für die Projektpartner anzubieten, welche einem anerkannten Standard entsprechen und an den BSI-Grundschutz angelehnt sind. Beabsichtigt ist es, den Städten und Gemeinden des Landkreises Gießen in diesem Bereich ein Angebot zu machen, das den Ausbau der Informationssicherheit in den Kommunen weiter verstärken soll und eine robuste Antwort auf mögliche Cyber-Angriffe bietet.

Modernes Verwaltungshandeln ist heute ohne elektronische Kommunikationsmedien und IT-Verfahren undenkbar. Mit der zunehmenden Digitalisierung der Verwaltungen nimmt auch der Schutzbedarf der IT-Systeme und der Daten zu. Um das Verwaltungshandeln zu gewährleisten ist die Sicherheit und Verfügbarkeit der IT-Systeme und Daten sicherzustellen.

Zunehmende und immer zielgerichtetere Angriffsszenarien erfordern einen hohen Sicherheitsstandard. Das Erreichen dieses Sicherheitsstandards stellt für Städte und Gemeinden, die häufig nur über geringe personelle Ressourcen verfügen, eine kaum bewältigbare Aufgabe dar.

Der Landkreis Gießen möchte mit seinen Ressourcen und dem vorhandenen Fachwissen die am Projekt teilnehmenden Kommunen unterstützen und beraten. Durch die Zusammenarbeit soll ein einheitlicher Standard an Informations- und Datensicherheit erreicht werden.

Zielsetzung ist es, die Informationssicherheit (in allen teilnehmenden Kommunen) auf ein Niveau zu bringen, welches an den BSI IT-Grundschutz anlehnt ist. In diesem Zusammenhang sollen die Kommunen bei der Erstellung und Fortschreibung von Sicherheits- und Notfallkonzepten sowie entsprechenden Umsetzungsstrategien unterstützt werden. Weiterhin ist unter anderem eine Unterstützung bei der Einführung eines Informationssicherheits-Management-Systems vorgesehen.

Zur Vernetzung unter den IT-Administratoren/innen wird eine gemeinsame Projektplattform angeboten. Mehrmals jährlich findet ein IT-Forum statt. Zudem sind Sensibilisierungs- und Schulungsmaßnahmen für die Mitarbeiterinnen und Mitarbeiter der teilnehmenden Kommunen vorgesehen. Die Unterstützung und Begleitung nach einem Cyber-Angriff ist ebenfalls Bestandteil des Projektes.

Nähere Details zu den Aufgabenstellungen und den Beziehungen zwischen den teilnehmenden Kommunen sind der im Entwurf beigefügten öffentlich-rechtlichen Vereinbarung (Anlage) zu entnehmen.

Finanzielle Auswirkungen:

Die Finanzierung des Projekts erfolgt aus Eigenmitteln des Landkreises Gießen und den Kostenerstattungen der teilnehmenden kreisangehörigen Kommunen. Die teilnehmenden Kommunen erstatten dem Landkreis Gießen für die Erbringung der in § 3 und § 4 der öffentlich-rechtlichen Vereinbarung beschriebenen Aufgaben ein jährliches Entgelt, welches sich an der Einwohnerzahl der jeweiligen Kommune orientiert.

Grundlagen für die Ermittlung der Kosten sind die Mitarbeiterkosten und die Arbeitsplatz- und Gemeinkosten. Die Projektkosten orientieren sich an der Arbeitgeberbelastung für eine Stelle der jeweils gültigen Entgeltgruppe EG 11 TVöD für den Projektbeauftragten und EG 8 TVöD für die Projektassistenz. Dies sind derzeit insgesamt 172.400,00 Euro pro Jahr. Die Projektkosten für die gesamte Projektdauer von fünf Jahren betragen damit rund 862.000,00 Euro. Für den Landkreis Gießen betragen damit (gerechnet ohne möglichen Fördermittelzuschuss nach § 5 Absatz 5 der öffentlich-rechtlichen Vereinbarung) die jährlichen Kosten 86.200,00 Euro; derselbe Betrag wird jährlich von den Vereinbarungspartnern entsprechend des auf Grundlage der Einwohnerzahl der jeweiligen Kommune berechneten Anteils getragen.

IKZ-Antrag – **Effizienzberechnung**

- Reduzierung von Aufwendungen von mindestens 15% in jedem Jahr
- Kalkulation der Kosten (Personal und Sachkosten) = Prognose
- Gegenüberstellung Kosten bei gemeinsamer Aufgabenwahrnehmung mit Kosten bei eigenständiger Aufgabenwahrnehmung als **tabellarische Darstellung**
- Basis für den Sachbericht im 5. Jahr der Kooperation

Kostenkalkulation mit Kooperation:	**1x**	**1x**	
	EG 11 TVÖD, St. 3	**EG 8 TVÖD, St. 3**	**Gesamt**
	in €	**in €**	**in €**
Personalkosten EG 11 TVöD, St. 3	70.218,50	52.690,32	
Sachkosten n. KGSt	9.700,00	9.700,00	
Fortbildungskosten/Reisekosten	5.000,00	2.000,00	
Gemeinkosten 20 %	14.043,70	10.538,06	
Jahressumme gesamt:	**98.962,20**	**74.928,38**	**173.890,58**

Kostenkalkulation ohne Kooperation:	**3,875x**	**1x**	
	EG 11 TVÖD, St. 3	**EG 8 TVÖD, St. 3**	**Gesamt**
	in €	**in €**	**in €**
Personalkosten	272.096,69	52.690,32	
Sachkosten n. KGSt	37.587,50	9.700,00	
Fortbildungskosten/Reisekosten	19.375,00	2.000,00	
Gemeinkosten 20 %	54.419,34	10.538,06	
Jahressumme gesamt:	**383.478,53**	**74.928,38**	**458.406,91**

prognostizierte Einsparung 62% pro Jahr

HESSEN

Kostenkalkulation ohne Kooperation:

Die Aufgabenwahrnehmung durch jeden einzelnen Kooperationspartner würde zu nachfolgendem Stellenbedarf führen, der Anhand eines Bedarfsschlüssels angenommen wurde. Der Bedarfsschlüssel orientiert sich an der Einwohnerzahl der Kooperationspartner:

	Einwohner		
Kommunen	**0 bis 10.000**	**10.001 bis 50.000**	**über 50.000**
Allendorf (Lumda)	x		
Biebertal	x		
Buseck		x	
Fernwald	x		
Gießen			x
Grünberg		x	
Heuchelheim	x		
Hungen		x	
Langgöns		x	
Laubach	x		
Lich		x	
Linden		x	
Lollar		x	
Pohlheim		x	
Rabenau	x		
Reiskirchen		x	
Staufenberg	x		
Wettenberg		x	
SUMME	**7**	**10**	**1**

Berechnung der Stellen Cybersicherheitsbeauftragter:			
	Kommunen	Schlüssel	Stellen
Kommunen bis 10.000 Einwohner	7	0,125	0,875
Kommunen von 10.001 - 50.000 Einwohner	10	0,25	2,5
Kommunen über 50.000 Einwohner	1	0,5	0,5
Anzahl Stellen			**3,875**

IKZ-Antrag – **Ablauf des Förderverfahrens**

- **Antragstellung**
  - IKZ-Antrag wird von **einer** der beteiligten Kommunen gestellt
    → diese ist Adressat des Förderbescheids
    → bewilligte Fördersumme wird an diese ausgezahlt
    (*Verwendung/Aufteilung ist im Innenverhältnis zu klären*)
  - Antrag ist **elektronisch** auf dem Dienstweg an HMdIS zu richten (Ziffer 5 Abs. 4 RV)
  - Aufsichtsbehörden (Landrat und Regierungspräsidium) nehmen Stellung
- **Prüfung (im HMdIS)**
  - Prüfung der Antragsvoraussetzungen im HMdIS Referat IV 3
  - Beteiligung der Kommunalen Spitzenverbände mit einer Frist von 2 Wochen
  - Einholung Zustimmung HMdF – Hessisches Finanzministerium
  - Vorlage Hausspitze
  - Zeitdauer für das Bewilligungsverfahren ca. 2 Monate

IMPRESSIONEN

VON DER TAGUNG IN WIESBADEN
AM 13. DEZEMBER 2022

1 Kirstin Scheel – Wissenschaftliche Mitarbeiterin, ATHENE Fraunhofer SIT; Claus Spandau, Kommunales Beratungszentrum Hessen – Partner der Kommunen

2 Stefan Sauer – Staatssekretär, Hessisches Ministerium des Innern und für Sport

3 Kirstin Scheel – Wissenschaftliche Mitarbeiterin, ATHENE Fraunhofer SIT

4 Philipp Stöhr – Fachdienstleiter Digitale Dienste und Open Government, Chief Digital Officer, Landkreis Marburg-Biedenkopf

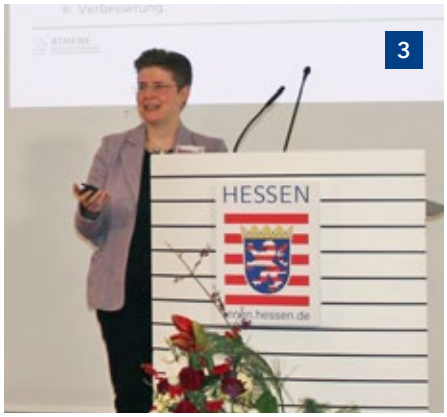
5 David Pöhlmann – Informationssicherheitsbeauftragter, Landkreis Gießen

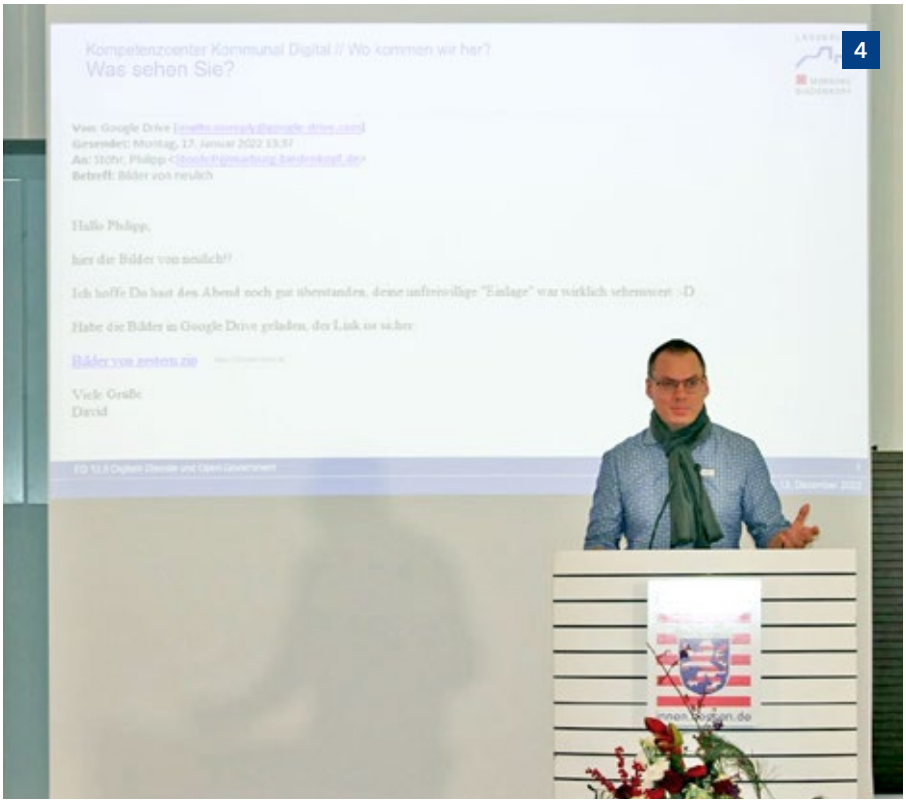
6 Andrea Reusch-Demel – Referatsleiterin Kommunale Strukturen und Interkommunale Zusammenarbeit, Hessisches Ministerium des Innern und für Sport

7 Dirk Dohn, Leiter Referat Innovationsmanagement Cybersicherheit Abteilung Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung vom HMdIS

8 Christopher Lipp – Erster Kreisbeigeordneter, Landkreis Gießen

9 Referent*innen und Teilnehmer*innen vor Ort


3
HESSEN


4
Kompetenzcenter Kommunal Digital // Wo kommen wir her?
Was sehen Sie?
Hallo Philipp,
Ich hoffe Du hast den Abend noch gut überstanden, deine unfreiwillige "Einlage" war wirklich sehenswert :-D
Viele Grüße
David


5
HESSEN


6
HESSEN


7
HESSEN


8
HESSEN


9

HESSEN

Hessisches Ministerium des Innern und für Sport

Friedrich-Ebert-Allee 12
65185 Wiesbaden

www.innen.hessen.de