Hessisches Ministerium des
Innern und für Sport

HESSEN

Hessische Cybersicherheitsstrategie

2023

Impressum

Hessisches Ministerium des Innern und für Sport
Friedrich-Ebert-Allee 12
65185 Wiesbaden
Telefon: (0611) 353 – 0
E-Mail: poststelle@hmdis.hessen.de
Web: https://innen.hessen.de

HESSEN

Inhaltsverzeichnis

Grußwort

1. Grußwort Minister

In der heutigen Zeit ist die Welt stärker vernetzt als je zuvor. Dies eröffnet uns vielfältige Chancen in Wirtschaft, Gesellschaft und Politik und bietet Möglichkeiten für Wachstum und Innovation. Gleichzeitig bringt die Entwicklung neue Risiken und Herausforderungen mit sich. Mit der Digitalisierung hat Cybersicherheit eine zentrale Bedeutung für die Innere Sicherheit und unser Wohlergehen bekommen. Es liegt in unserer aller Verantwortung, geeignete Maßnahmen zu ergreifen, um die Informationssicherheit und die Widerstandsfähigkeit von IT-Systemen zu erhöhen.

Die Auswirkungen von Cyberangriffen sind enorm, sie können die Funktionsfähigkeit des Staates einschränken, existenzbedrohend für Unternehmen sein und die Versorgungssicherheit der Bevölkerung mit essenziellen Gütern und Dienstleistungen gefährden, insbesondere, wenn kritische Infrastrukturen betroffen sind. So waren auch hessische Kommunen und Unternehmen in den letzten Jahren zunehmend Cyberangriffen ausgesetzt. Prominente Beispiele sind die Angriffe mit der Ransomware „Emotet" auf Universitäten und Kommunalverwaltungen, bei denen das Ziel darin bestand, Daten zu verschlüsseln und Lösegeldzahlungen zu erpressen. Diese Vorfälle haben gezeigt, dass es dringend notwendig ist, unsere Schutzmechanismen zu verstärken.

Um einen gemeinsamen, übergeordneten Rahmen für die Anstrengungen der Hessischen Landesregierung zu schaffen, haben wir eine umfassende Cybersicherheitsstrategie für Hessen entwickelt, mit der wir Schwerpunkte setzen und Zielsetzungen definieren, um die Cybersicherheit künftig weiter zu erhöhen.

Dabei betrifft Cybersicherheit uns alle: Staat und Verwaltungen, Unternehmen, kritische Infrastrukturen, Bürgerinnen und Bürger, Wissenschaft und Forschung. Alle diese Bereiche und Akteure stehen auch aufgrund der Vernetzung miteinander in Wechselwirkung. Entsprechend gilt es, dass Staat, Wirtschaft und Gesellschaft noch enger zusammenwirken und entsprechende Vorkehrungen treffen.

Die hessische Cybersicherheitsstrategie ist ein zukunftsweisendes und ambitioniertes Projekt, das unsere Entschlossenheit widerspiegelt, die Digitalisierung in Hessen weiter sicher zu gestalten.

Peter Beuth

Hessischer Minister des Innern und für Sport

2. Vorwort des Chief Information Security Officer

In unserer heutigen digitalisierten Welt sind Cyberangriffe eine der größten Bedrohungen für staatliche Institutionen und ihre Bürgerinnen und Bürger. Es ist von größter Bedeutung, dass wir unsere Cybersicherheitsmaßnahmen ständig verbessern und anpassen, um uns gegen diese Bedrohung zu wappnen.

Die hessische Landesverwaltung ist sich der Gefahren von Cyberangriffen bewusst und hat in den letzten Jahren bedeutende Anstrengungen unternommen, um ihre IT-Systeme und Daten zu schützen. Unsere neue Cybersicherheitsstrategie basiert auf vier Säulen: Prävention, Erkennung, Reaktion und Kooperation. Wir haben uns zum Ziel gesetzt, unsere Präventionsmaßnahmen zu verstärken, um Cyberangriffe von vornherein zu verhindern. Gleichzeitig werden wir unsere Erkennungs- und Reaktionsfähigkeiten verbessern, um schnell auf Bedrohungen reagieren zu können. Wir werden auch weiterhin eng mit anderen Akteuren zusammenarbeiten, um unsere Cybersicherheitsmaßnahmen abzustimmen und Informationen auszutauschen.

Die Umsetzung unserer Cybersicherheitsstrategie erfordert eine umfassende Anstrengung aller Mitarbeiterinnen und Mitarbeiter der hessischen Landesverwaltung. Wir werden in Schulungen und Awareness-Programme investieren, um das Bewusstsein für die Bedrohungen zu erhöhen und die IT-Sicherheitskultur in der Verwaltung zu stärken.

Zeitgleich werden wir intensiv daran arbeiten, Schwachstellen abzustellen, Strukturen zu verbessern und Verfahren zu optimieren, um ein hohes Maß an Cybersicherheit für Hessen sicherzustellen. Zudem treffen wir umfangreiche Vorkehrungen zur Aufrechterhaltung der Arbeitsfähigkeit staatlicher Einrichtungen sowie zur Wiederherstellung im Falle von IT-Krisen. Mit all diesen Maßnahmen erhöhen wir die Resilienz der hessischen Landesverwaltung weiter.

Nur durch eine gemeinsame Anstrengung können wir unsere Cybersicherheit auf ein höheres Niveau heben und unsere Daten und Systeme effektiv schützen.

Ich möchte allen Mitarbeiterinnen und Mitarbeitern der hessischen Landesverwaltung für ihre Unterstützung danken und freue mich darauf, gemeinsam mit Ihnen unsere Cybersicherheitsmaßnahmen weiter zu verbessern.

Ralf Stettner

Chief Information Security Officer

Leitlinien der hessischen Cybersicherheits-strategie

Abbildung 1 Grafik zum Ökosystem und Gemeinschaften

3. Leitlinien der hessischen Cybersicherheitsstrategie

Cybersicherheit – wirkungsvoll und innovativ

Hessen nimmt mit seiner Cybersicherheitsstruktur bundesweit eine Vorreiterrolle ein. Als erstes Land hat Hessen 2019 eine Kompetenzstelle zur interdisziplinären Zusammenarbeit und institutionalisierten Kooperation staatlicher Behörden, das Hessen CyberCompetenceCenter (Hessen3C) im Hessischen Ministerium des Innern und für Sport, etabliert. Dieses bildet in Hessen die zentrale Anlaufstelle in Cybersicherheitsfragen und übernimmt die Schnittstellenfunktion zu anderen Landes- und Bundesbehörden. Als Kernorganisation ist sie ein wesentlicher Baustein der Cybersicherheitsarchitektur, die sich übergreifend aus dem zentralen IT-Dienstleister des Landes, der Hessischen Zentrale für Datenverarbeitung (HZD), Einrichtungen der Landesverwaltung, Kommunen sowie deren kommunalem IT-Dienstleister ekom21, kleinen und mittleren Unternehmen sowie Betreibern kritischer Infrastruktur (KRITIS) zusammensetzt.

Für Cybersicherheit zu sorgen, ist in Hessen eine Aufgabe höchster Priorität. Diese wurde durch Kabinettsbeschluss dem Leiter der Abteilung Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung in der Rolle des Zentralen Informationssicherheitsbeauftragten der Landesverwaltung (Chief Information Security Officer (CISO)) im Hessischen Ministerium des Innern und für Sport (HMdIS) übertragen. Er erstellt in Abstimmung mit den Ressorts die Informationssicherheitsleitlinie des Landes Hessen und wird durch das Hessen3C maßgeblich bei der Koordinierung und der Bearbeitung von landesweiten IT-Sicherheitsvorfällen unterstützt. Im Krisenfall leitet der CISO das IT-Krisenmanagement, welches sich aus Vertreterinnen und Vertretern aller Ressorts und dem zentralen IT-Dienstleister zusammensetzt.

Das Referat Zentrales Informationssicherheitsmanagement im Hessischen Ministerium des Innern und für Sport unterstützt den CISO in seiner Aufgabenwahrnehmung zur Erstellung der Informationssicherheitsleitlinie und der Beratung der Hessischen Staatskanzlei sowie der Ressorts der hessischen Landesverwaltung in Fragen der Informationssicherheit. In einem ressortübergreifenden Arbeitskreis werden die landesweite Umsetzung des Informationssicherheitsmanagementsystems (ISMS) koordiniert und landesweite Richtlinien zur Informationssicherheit zwischen den Ressorts abgestimmt.

Die „Förderrichtlinie Cybersicherheitsforschung in Hessen" und der 2020 durch das HMdIS ins Leben gerufene „Beirat Cybersicherheit" stellen die Vernetzung und enge Zusammenarbeit zwischen Verwaltung und Forschung sicher. Ziel ist es, das eigene Handeln fortwährend an innovativen Lösungen aus Forschung und Entwicklung auszurichten. Cybersicherheitsinnovationen werden so frühzeitig und konsequent bei der Entwicklung der Informationstechnik der hessischen Sicherheitsbehörden und Verwaltung berücksichtigt.

Digitale Souveränität – unabhängig und gestaltend

Die Hessische Landesregierung legt einen besonderen Schwerpunkt auf ein sicheres und faires Miteinander in der digitalen Welt und widmet den digitalen Spielregeln daher ein eigenes Handlungsfeld in ihrer Strategie „Digitales Hessen – Wo Zukunft zuhause ist". Souveränität im Cyberraum kommt dabei eine zentrale Rolle zu.

Darunter sind sichere und insbesondere resiliente IT-Infrastrukturen zum Schutz von Daten vor Diebstahl oder Manipulation sowie die Gewährleistung vertraulicher Kommunikation ebenso zu fassen wie die Hoheit über Schlüsseltechnologien.

Souveränität im Cyberraum funktioniert nicht ohne Investitionen in Forschung für moderne technologische Entwicklungen im Bereich der Informationssicherheit. Genauso sind Investitionen in eine breite digitale Aufklärung und Bildung essenziell, damit die Menschen in Hessen informiert und selbstbestimmt entscheiden können, wie und von wem Informationen über die eigene Person oder Institution erhoben, verarbeitet und weitergegeben werden.

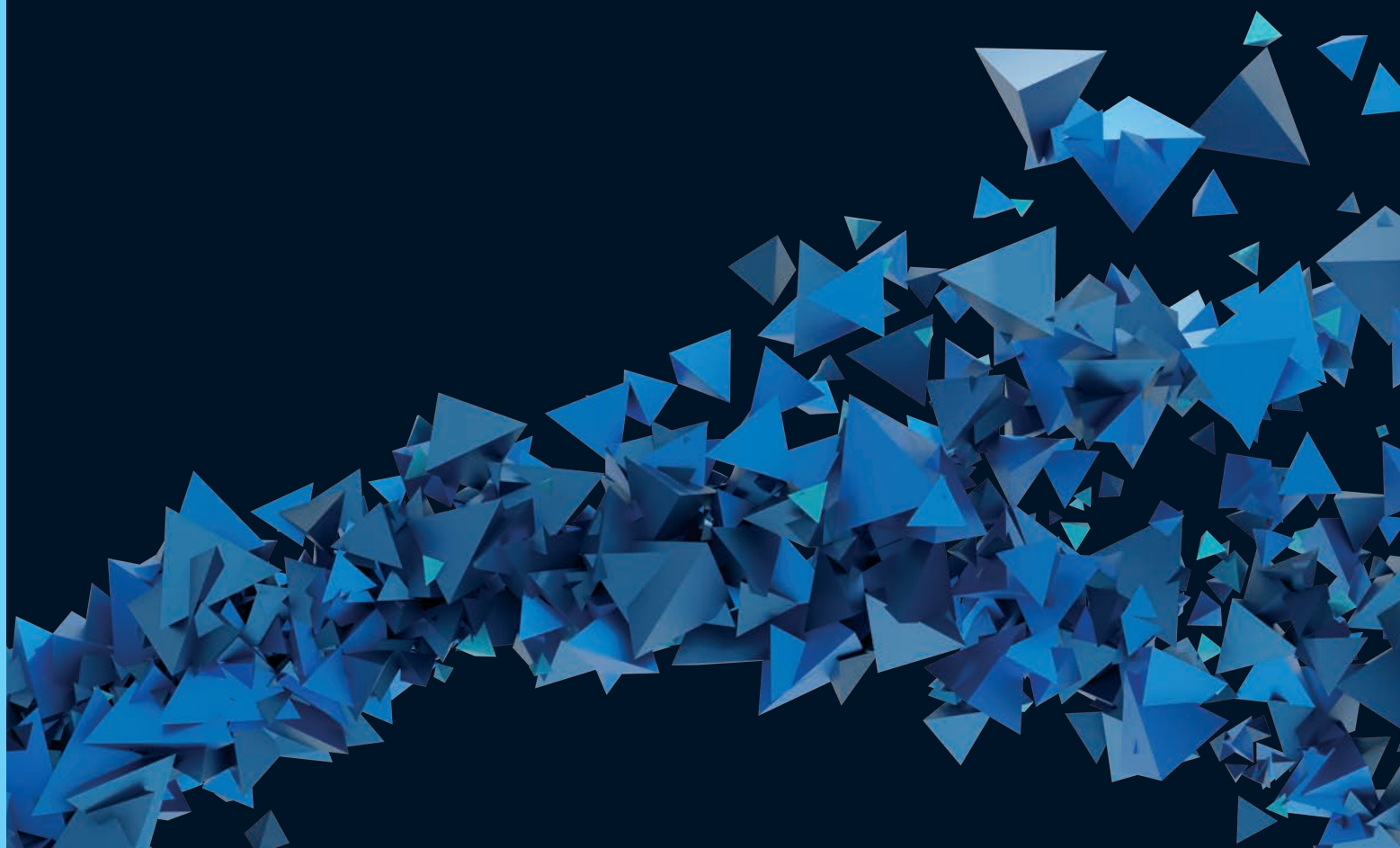
Hessen strebt an, die digitale Souveränität in Hessen zu steigern sowie jene der Bundesrepublik Deutschland und Europas mitzugestalten.

Sichere digitale Zukunft – kompetent und verlässlich

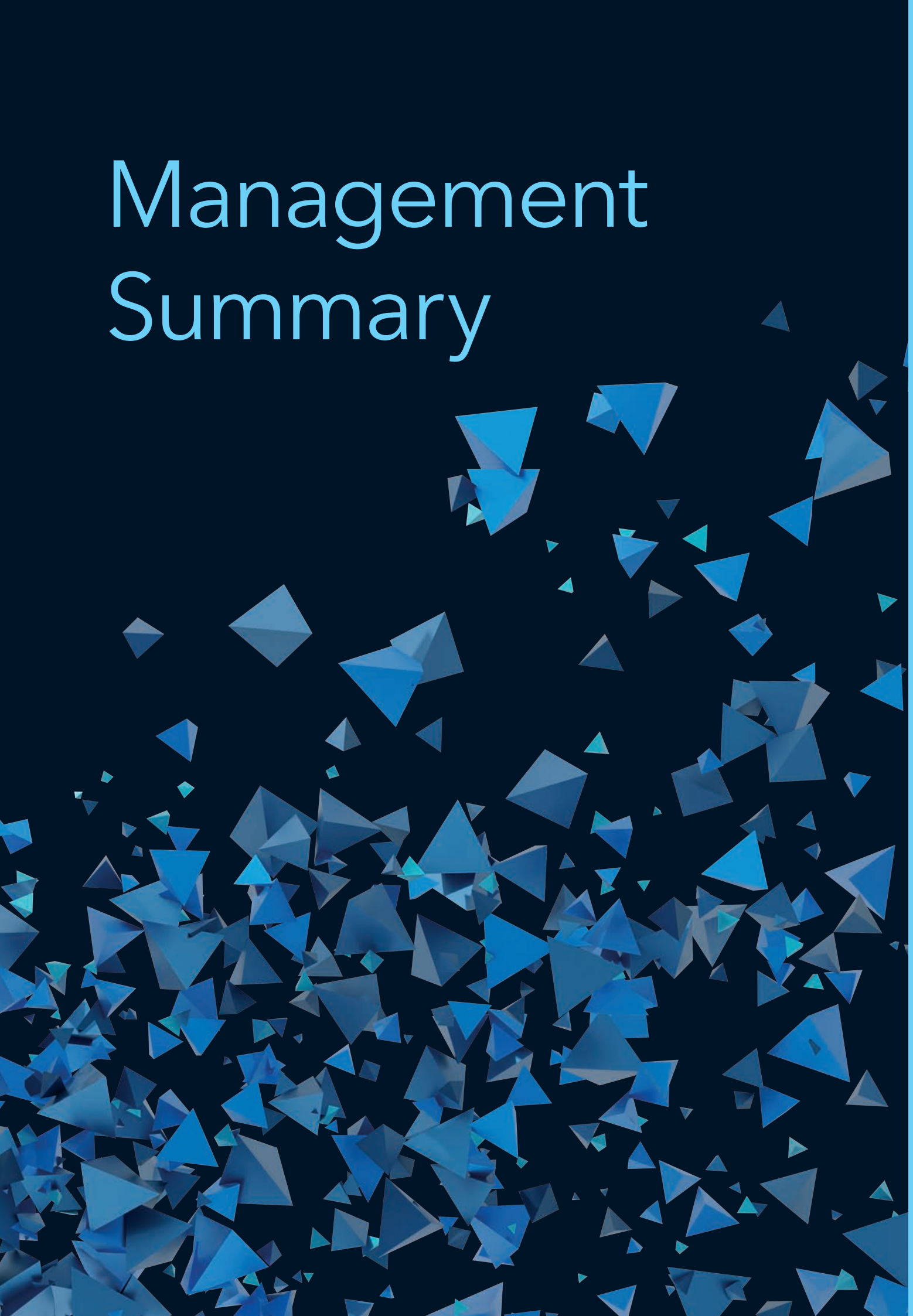
Sicherheit, ohne die Freiheit nicht denkbar wäre, zu gewährleisten, ist die Aufgabe des Staates. Dies gilt zunehmend auch für den Bereich der Cybersicherheit. Die rasanten technologischen Entwicklungen bedeuten eine besondere Herausforderung in der Abschätzung zukünftiger Sicherheitsbedrohungen im digitalen Raum.

Mit der Cybersicherheitsstrategie werden die konzeptionellen Überlegungen für den Weg Hessens in eine sichere digitale Zukunft ganzheitlich verankert. Die Handlungsfelder geben Orientierung für das Handeln der Gemeinschaften und deren Zusammenwirken. Im Fokus stehen insbesondere die Etablierung eines verantwortungsvollen Bewusstseins und eine ausgeprägte Sensibilität für Cybersicherheit in allen Bereichen.

Die bereits geschaffene und weiterzuentwickelnde Cybersicherheitsarchitektur zielt auf die zuverlässige Abwehrfähigkeit von Cyberangriffen ab. So trägt Hessen zur Sicherung der freiheitlich demokratischen Werte einer sich weiter modernisierenden Informationsgesellschaft in Deutschland bei.



Management Summary



4. Management Summary

Die Hessische Landesregierung bedient sich eines Ökosystemmodells, welches die Interaktionen der Akteure im Bereich Cybersicherheit darstellt.

Alle im Ökosystem (siehe Abbildung 1, Seite 13) aufgeführten Gemeinschaften sind in ihren unterschiedlichen Rollen gleichzeitig voneinander abhängig und beeinflussen sich gegenseitig. Neue technologische Entwicklungen und daraus resultierende Veränderungen im Cyberraum beeinflussen stetig die Interaktionen der Gemeinschaften und treiben deren Entwicklung voran. Die abgebildeten Akteure stellen in unterschiedlichen Rollen die Cybersicherheitsarchitektur in Hessen dar und tragen zur Gewährleistung des hohen Sicherheitsniveaus bei. Das Ökosystem basiert auf der grundlegenden Idee, durch eine ausgefeilte und gut vernetzte Cybersicherheitsarchitektur, die Sicherheit im Cyberraum auf einem hohen Niveau zu stabilisieren und eine höchstmögliche Resilienz gegen Angriffe zu schaffen.

Die im Ökosystem abgebildeten Akteure werden in der vorliegenden Strategie ihren unterschiedlichen Rollen entsprechend zu Gemeinschaften zusammengefasst. Die aus den Gemeinschaften abgeleiteten Handlungsfelder orientieren sich an den individuellen Aufgaben und Bedarfen der jeweiligen Akteure. Als wiederkehrende Struktur zur Ableitung messbarer Ziele werden die einzelnen Handlungsfelder anhand der drei Aspekte „Bedeutung", „Gegenwart" und „Zukunft" beleuchtet. Damit werden bestehende Zuständigkeiten und Initiativen sowie künftige Maßnahmen und Projekte strukturiert dargestellt.

Ziele und Leitlinie

Als Orientierung bei der Entwicklung von Zielen und Maßnahmen für die einzelnen Handlungsfelder dienen die drei zentralen Leitlinien zur Ausrichtung der hessischen Cybersicherheitsstrategie

- Cybersicherheit – wirkungsvoll und innovativ
- Digitale Souveränität – unabhängig und gestaltend
- Sichere digitale Zukunft – kompetent und verlässlich

Die Zuständigkeit der einzelnen Ministerinnen und Minister wird durch Beschluss der Landesregierung nach Art. 104 Abs. 2 der Verfassung des Landes Hessen festgelegt. Hierbei hat der Geschäftsbereich des Hessischen Ministers des Innern und für Sport die Zuständigkeit für Grundsatzfragen der IT- und Cybersicherheit inne. Die in dieser Strategie formulierten Ziele und Maßnahmen sind mit den Kernaufgaben der jeweiligen Ressorts verknüpft. Deren Umsetzung liegt in der Verantwortung des zuständigen Ministeriums.

Handlungsfelder

5. Handlungsfelder

Aufbau der Themen

Alle Themen der nachfolgenden Handlungsfelder der hessischen Cybersicherheitsstrategie werden in einem Dreiklang betrachtet.

Im ersten Teil der Betrachtung werden die **Bedeutung** des Themas sowie mögliche Schnittstellen zu anderen Gemeinschaften im Ökosystem und Bedarfe aus Sicht der Cyber- und IT-Sicherheit beleuchtet.

Bereits laufende und zukünftige Maßnahmen der hessischen Landesverwaltung und deren Partnern in der Cyber- und IT-Sicherheit werden unter **Gegenwart** und **Schwerpunkte / Ziele** erläutert.

Daran anknüpfend werden abschließend die Akteure, die aktuell und zukünftig, thematisch und in ihren unterschiedlichen Rollen des Ökosystems für die inhaltliche Ausgestaltung und Umsetzung verantwortlich sind, dargestellt.

Staatliche Verwaltung, Kommunen und Gefahrenabwehr- und Sicherheitsbehörden

5.1 Staatliche Verwaltung, Kommunen und Gefahrenabwehr- und Sicherheitsbehörden

In Hessen ist es gelungen, eine stabile und zukunftsfähige Cybersicherheitsarchitektur zu errichten. Die Landesverwaltung, die Kommunen sowie die Gefahrenabwehr- und Sicherheitsbehörden sind in der Pflicht, die Funktionsfähigkeit des Staates durch robuste und krisensichere IT-Systeme sowie stabile Abwehrmechanismen zu gewährleisten. Dies schafft Vertrauen der Bürgerinnen und Bürger in ihr digitales Lebensumfeld und ermöglicht eine zukunftsorientierte (digitale) Interaktion mit den staatlichen Verwaltungen. Die Vorteile der Digitalisierung können so in all ihren Facetten genutzt werden. Die Hessische Landesregierung steht zu ihrer Verantwortung, über Schwerpunktsetzungen den Steuerungsrahmen für eine sichere „Cyberlandschaft Hessen" zu gestalten und nimmt ihre Rolle als Unterstützer und Förderer anderer Gemeinschaften innerhalb des Ökosystems wahr.

5.1.1 Chief Information Security Officer (CISO)

Bedeutung

Mit dem Ziel der Bündelung von Zuständigkeiten und Aufgaben im Bereich Cyber- und IT-Sicherheit hat die Hessische Landesregierung die Funktion eines zentralen Informationssicherheitsbeauftragten (CISO) geschaffen. Der CISO hat den übergeordneten Auftrag, die Informationssicherheit in der Landesverwaltung kontinuierlich zu verbessern, die Staatskanzlei und die Ressorts zu beraten und Empfehlungen zu geben. Er agiert dabei koordinierend, als Impulsgeber und Unterstützer. Zudem ist der CISO die Eskalationsinstanz für ressortübergreifende Informationssicherheitsthemen und vertritt die hessische Landesverwaltung in Belangen der Informationssicherheit nach außen.

Gegenwart

Der zentrale Informationssicherheitsbeauftragte der hessischen Landesverwaltung (CISO) wurde im August 2016 erstmals per Kabinettsbeschluss ernannt. Aktuell hat diese Funktion der Leiter der Abteilung VII „Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung" des HMdIS inne. Dessen Ernennung erfolgte durch Kabinettsbeschluss vom 10. September 2019.

Dem CISO kommt in der Informationssicherheitsleitlinie für die hessische Landesverwaltung (ILL) eine herausgehobene Stellung bei Informationssicherheitsthemen zu. In Wahrnehmung seiner Aufgaben setzt sich der CISO fortwährend für eine ganzheitliche Stärkung der Informationssicherheit in der Landesverwaltung ein. Unter anderem werden durch den CISO landesweite Maßnahmen zur Erhöhung der Informationssicherheit koordiniert.

Vor dem Hintergrund einer allgemein erhöhten Bedrohungslage bedarf es der umfassenden präventiven Vorbereitung auf IT-Krisensituationen, um diese strukturiert bewältigen und schnellstmöglich in den Regelbetrieb zurückkehren zu können. In diesem Zusammenhang kommt dem CISO die Leitung des im HMdIS konzipierten IT-Krisenmanagements sowie eine Rolle im Landeskrisenstab zu.

Schwerpunkt / Zielsetzung

Die Resilienzfähigkeit bei Cyberangriffen ist eine wichtige Säule der Handlungsfähigkeit der Landesverwaltung. Mit dem Ziel der raschen Bewältigung möglicher landesweiter IT-Krisen setzt sich der CISO für den Ausbau und die Weiterentwicklung entsprechender Organisationsstrukturen sowie die Einrichtung von Prozessen in der Landesverwaltung ein.

Zur weiteren Stärkung der Informationssicherheit hat die Abteilung VII, HMdIS, gestützt auf den Beschluss über die Zuständigkeit der einzelnen Ministerinnen und Minister nach Art. 104 Abs. 2 der Verfassung des Landes Hessen vom 26.03.2019, die Initiative zur Wahrnehmung der speziellen Fachaufsicht der HZD als Betreiber des hessischen Landesnetzes übernommen.

Ferner soll der Austausch zwischen dem CISO und Unternehmen sowie staatlichen Akteuren innerhalb der nationalen Cybersicherheitsarchitektur weiter intensiviert werden.

Verantwortlichkeit

HMdIS – Abteilung VII, Referat 13
CISO

5.1.2 Business Continuity Management

Bedeutung

Die steigende Anzahl der Cyberangriffe belastet zunehmend den Geschäftsbetrieb sowie die Aufgabenerfüllung der Institutionen. Ein absoluter Schutz hiervor existiert nicht. Mithilfe eines angemessenen Business-Continuity-Managements (BCM) können sich Institutionen jedoch auf Schadensereignisse vorbereiten, die sich kritisch auf den Geschäftsbetrieb auswirkten. Ziel des BCM ist es, den Geschäftsbetrieb im Falle eines Cyberangriffs auf einem Notbetriebsniveau aufrechtzuerhalten oder zumindest nach einem Ausfall in kürzester Zeit fortführen zu können. Das BCM umfasst daher neben organisatorischen und technischen Aspekten auch bauliche, vertragliche und personelle Maßnahmen, um in einer Institution die notwendige Resilienz bei Informationssicherheitsvorfällen zu gewährleisten.

Das BCM ist ein Prozess, der einer kontinuierlichen Verbesserung und Anpassung an die internen und externen Rahmenbedingungen bedarf. Daneben trägt auch eine frühzeitige und regelmäßige Risikoanalyse indirekt dazu bei, die Resilienz der Institutionen zu stärken. Einem vorbereiteten IT-Krisenmanagement kommt darüber hinaus eine besondere Rolle zu, um die Reaktionsfähigkeit der handelnden Akteure zu verbessern. Ein Überblick der wesentlichen Geschäftsprozesse der Landesverwaltung und der zugehörigen Business Impact Analyse in Verbindung mit Risikobewertungen sind notwendige Voraussetzungen zur Einschätzung der Bedrohungslage und Vorbereitung entsprechender BCM-Maßnahmen.

Gegenwart

Der aktualisierte Entwurf des BSI-Standards 200-4 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beschreibt die Methodik des ganzheitlichen Business Continuity Management Systems (BCMS). Dieser über das bisherige Notfallmanagement hinausgehende neue Aspekt soll auch in der hessischen Landesverwaltung umgesetzt werden. In Ergänzung und Orientierung an die Vorgaben der ILL wurde, unter Berücksichtigung aller Zielgruppen und Akteure, ein aufwachsender Prozess der Vorfallbearbeitung, beginnend im CERT bis zur Einberufung des ressortübergreifenden IT-Krisenmanagements (IT-KM) unter Leitung des CISO sowie in letzter Instanz der Erklärung einer Landeskrise entwickelt. Darin werden auch prozessbegleitende Maßnahmen hinsichtlich der Prävention und Reaktion betrachtet und anlassbezogen evaluiert. Darüber hinaus wurden in der ganzheitlichen Betrachtung die Schnittstellen zu den IT-Dienstleistern der Landes- und Kommunalverwaltung definiert.

Zur Stärkung der Kommunen in der Cyber- und IT-Sicherheit hat das Hessen3C gemeinsam mit der ekom21 und dem Kommunalen Dienstleistungszentrum Cybersicherheit (KDLZ-CS) zur Förderung und Verbesserung der Cyber- und IT-Sicherheit in den Kommunen das Hessische Cyberabwehrausbildungszentrum Land/Kommunen (HECAAZ L/K) initiiert. Das Schulungsangebot wird in enger Abstimmung und mit starker Unterstützung durch den Hessischen Landkreistag für die kreisangehörigen Kommunen ortsnah angeboten. Thematisch werden Cybersicherheit und BCM damit direkt bei den Verantwortlichen vor Ort eingebracht.

Schwerpunkt / Zielsetzung

Die Weiterentwicklung des bestehenden Notfallmanagements zu einem übergreifenden, auch IT-Systeme umfassenden BCM, sowie die Etablierung des BCM in allen Ressorts werden von der Hessischen Landesregierung als Schwerpunkt der kommenden Jahre gesehen. Dieses Ziel wird auf Landes- und kommunaler Ebene maßgeblich durch das Programm HECAAZ L/K unterstützt, welches zukünftig als fester Fortbildungsbestandteil in der Hochschule für öffentliches Management und Sicherheit (HöMS) integriert werden soll.

Um die Krisenfestigkeit des Landes und die Handlungssicherheit der Beschäftigten zu erhöhen, wird die bisherige aktive Teilnahme an Übungen zum Krisenmanagement, wie beispielsweise der LÜKEX, intensiviert und um eigene hessische Übungen erweitert. Damit strebt die Landesregierung eine verstärkte Harmonisierung und Standardisierung behördenübergreifender Prozesse und länderübergreifender Zusammenarbeit in Krisenstabsorganisationen an.

Verantwortlichkeit

Alle Ressorts

5.1.3 Kommunen

Bedeutung

Für Kommunen sind Cyber- und IT-Sicherheit besondere Herausforderungen. Diese können nur gemeinsam durch das Land Hessen und dessen Kommunen in enger Zusammenarbeit gewährleistet werden.

Das Land Hessen hat den Handlungsbedarf im kommunalen Umfeld erkannt und bindet die Kommunen als auch die kommunalen Spitzenverbände (KSpV) bei Maßnahmen zur Erhöhung der Cyber- und IT-Sicherheit eng ein.

Hinsichtlich der Cyber- und IT-Sicherheit bestehen wechselseitige Bezüge und Verpflichtungen zwischen Landes- und Kommunalverwaltung. Bei einzelnen bundesweiten Ereignissen und Vorgängen, wie etwa der Bundestagswahl oder der OZG-Umsetzung, sind auch Vorgaben des Bundes zu beachten.

Gegenwart

Das Land Hessen schafft bereits heute durch Förderrichtlinien, wie beispielsweise der „Rahmenvereinbarung zur Förderung der interkommunalen Zusammenarbeit", Anreize und finanzielle Möglichkeiten zur Unterstützung der Kommunen auch bei Maßnahmen zur Erhöhung des Cybersicherheitsniveaus.

Das HMdIS hat gemeinsam mit dem kommunalen IT-Dienstleister in Hessen, der ekom21, das Kommunale Dienstleistungszentrum Cybersicherheit (KDLZ-CS) zur Förderung und Verbesserung der Cyber- und IT-Sicherheit in den Kommunen gegründet und weiterentwickelt. Das Angebot des KDLZ-CS kann von allen 443 hessischen Kommunen in Anspruch genommen werden. In Erweiterung der Unterstützungsleistung des Landes zur Stärkung der Kommunen in der Cyber- und IT-Sicherheit wurde von den vorgenannten Einrichtungen gemeinsam das Hessische Cyberabwehrausbildungszentrum Land/Kommunen (HECAAZ L/K) initiiert. Das Schulungsangebot wurde in enger Abstimmung mit den KSpV und mit starker Unterstützung durch den Hessischen Landkreistag erstellt.

Aspekten der Daten- und IT-Sicherheit wird auch in der Richtlinie zur Förderung smarter Kommunen und Regionen im Programm „Starke Heimat Hessen" Rechnung getragen.

Schwerpunkt / Zielsetzung

Die Landesregierung wird bei der zukünftigen Fortentwicklung der Förderrichtlinien für Kommunen einen Schwerpunkt auf Cyber- und IT-Sicherheitsthemen legen und stellt somit sicher, dass das Sicherheitsniveau in den hessischen Kommunen erhöht wird.

Zur Stärkung des Austauschs und der Vernetzung wird das Land Hessen geeignete Formate zu Fragen der Cyber- und IT-Sicherheit zwischen Land, Kommunen, kommunalen Spitzenverbänden und dem kommunalen IT-Dienstleister etablieren.

Das Programm HECAAZ L/K zukünftig als festen Fortbildungsbestandteil an der HöMS zu etablieren, ist erklärtes Ziel der Hessischen Landesregierung.

Verantwortlichkeit

HMdIS – Abteilung VII, Referat 12 (Hessen3C)
HMinD

5.1.4 Gefahrenabwehr- und Sicherheitsbehörden

Bedeutung

Die zunehmende Digitalisierung und Vernetzung aller Lebensbereiche erhöht die Angriffsfläche und stellt verschärfte Anforderungen an die Sicherheitsarchitektur. Der Umgang mit dieser veränderten Landschaft und den vielfältigen Cybersicherheitsbedrohungen erfordert einen ganzheitlichen Ansatz.

Die Polizei Hessen steht mit einem ihrer Kernaufträge, der Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung, als Ansprechpartner für Bürgerinnen und Bürger, Landesverwaltung, Kommunen und Unternehmen in Hessen zur Verfügung. Die Fallzahlen im Bereich Cybercrime im engeren Sinne sind seit Jahren ansteigend und die Angriffsformen der Täter vielfältig sowie komplex. Diese Straftaten, die sich unmittelbar gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten, sind Delikte, zu deren Begehung sich die Täter moderner Methoden bedienen müssen oder das erforderliche Know-how im Darknet erwerben können. Dies erfordert eine ebenso technisch versierte Ermittlungsarbeit seitens der Strafverfolgungsbehörden. Mit dem Vertrauen der Bürgerinnen und Bürger sowie hessischer Unternehmen in die Strafverfolgungsbehörden kann auch das Dunkelfeld der Cyberkriminalität weiter reduziert werden. In der digitalen Gesellschaft führen die Spuren nahezu aller Deliktsbereiche ins Internet. Hier wird der herkömmliche analoge Ermittlungsansatz um die technische Ermittlungsunterstützung ergänzt, damit digitale Aktivitäten und die dahinterstehenden realen Personen für eine beweissichere Strafverfolgung zusammengeführt werden.

Aufgrund weitgehender Anonymität etablieren sich Kryptowährungen zunehmend und umfangreich als Bestandteil des digitalen Zahlungsverkehrs und werden auch für kriminelle Zwecke in allen Deliktsbereichen verwendet. Zahlungsmittel im Rahmen von Erpressungen nach Cyberangriffen und erfolgreichen Systemverschlüsselungen sind ausschließlich Kryptowährungen. Für Ermittlungsbehörden ist die Nachverfolgung von Geldflüssen sowohl bei der Identifizierung der Täter als auch für die Erbringung von Tatnachweisen eine Grundvoraussetzung.

Der stark zunehmende Einsatz von mit dem Internet verbundenen Geräten (Internet of Things - IoT), wie beispielsweise Smartphones, Smart-Home-Geräte, Kfz-IT und sogenannte Wearables (beispielsweise Smart-Watches und Fitnesstracker) erhöhen mögliche Angriffsflächen und Einfallstore für Cyberkriminelle.

Der Verfassungsschutz dient dem Schutz der freiheitlich demokratischen Grundordnung und ist somit ein wichtiges Instrument der wehrhaften Demokratie. Das Landesamt für Verfassungsschutz Hessen (LfV Hessen) schützt die Demokratie und hält insbesondere die analytischen Kompetenzen zur Beurteilung jener Gefahren vor, die Demokratie und Menschenrechten durch extremistische Bestrebungen drohen. Dem LfV Hessen kommt insbesondere im digitalen Wirtschaftsschutz und bei der Abwehr von Cyberspionage eine besondere Bedeutung zu.

Der Brand- und Katastrophenschutz hat die Aufgabe, alle notwendigen Maßnahmen zu treffen, um Mensch, Umwelt und bedeutende Sachwerte in und vor der Entstehung einer Katastrophe zu schützen sowie unmittelbare Gefahren von Bürgerinnen und Bürgern abzuwehren. Eine hochverfügbare IT ist dabei elementares Arbeitsmedium einer zukunftsorientierten Gefahrenabwehr. Die Verflechtung von physischer Sicherheit und Cybersicherheit ist auch hier von entscheidender Bedeutung. Dies zeigt sich ebenfalls beim Blick auf die Versorgungsleistung der Betreiber Kritischer Infrastrukturen (KRITIS), deren Aktivitäten zur Vermeidung von und der Vorbereitung auf (unvermeidbare) Störungen / Ausfälle dem ursachenübergreifenden All-Gefahren-Ansatz folgen.

Die zielgerichtete Zusammenarbeit der bestehenden Sicherheitsbehörden mit Akteuren aus Verwaltung, Wirtschaft und Wissenschaft kann nur auf Grundlage eines interdisziplinären Informationsaustausches erfolgreich sein.

Gegenwart

Hessen3C

Im April 2019 gründete der Hessische Minister des Innern und für Sport in Wiesbaden das zentrale Element der hessischen Cybersicherheitsarchitektur: das Hessen CyberCompetenceCenter (Hessen3C). Dieses ist ein Referat der Abteilung „Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung" und unterstützt den Chief Information Security Officer (CISO). Das Hessen3C bietet eine bundesweit in dieser Form erstmals realisierte Plattform und einen Rahmen für eine strukturierte und behördenübergreifende Zusammenarbeit.

Hessen3C ist ein wesentlicher Bestandteil der hessischen und nationalen Cybersicherheitsarchitektur. Das Hessen3C ist zentraler Ansprechpartner bei Cybersicherheitsvorfällen in Hessen.

Der durch das Hessen3C neu geschaffene regelmäßige Lageaustausch zwischen den Bereichen Cybersecurity, Cybercrime und Cyberintelligence, dem Hessischen Landeskriminalamt und dem Landesamt für Verfassungsschutz Hessen ermöglicht es, Schwachstellen, Angriffe und aktuelle Kriminalitätsphänomene im Cyberraum effizient und umfassend zu bewerten sowie zielgerichtete und abgestimmte Maßnahmen einzuleiten.

Das Aufgabenspektrum des Hessen3C erstreckt sich vom Schutz der Landesverwaltung vor Cybersicherheitsbedrohungen über die Unterstützung der Sicherheitsbehörden bei der Bekämpfung von Cybercrime und Cyberspionage bis hin zur Beratung von Kommunen, Unternehmen, KRITIS-Betreibern sowie von Bürgerinnen und Bürgern.

Im Hessen3C werden von der strategischen Planung ausgehend bis hin zur operativen Umsetzung ganzheitliche Lösungen zu Fragen der Cybersicherheit erarbeitet, die auf die jeweiligen Zielgruppen abgestimmt sind.

Operative Elemente des Hessen3C

- Das Computer Emergency Response Team (CERT) Hessen des Hessen3C erstellt werktäglich einen Schwachstellenbericht im Rahmen eines Warn- und Informationsdienstes für die Landesverwaltung und die Kommunen.
- Mit der Einrichtung eines Mobile Incident Response Teams (MIRT) unterhält das Hessen3C eine mobile Einheit, die im Falle von schweren Informationssicherheitsvorfällen bei Bedarf vor Ort unterstützt.
- Vorgangsbearbeitung bei Meldungen, akuten Vorfällen sowie forensischen Analysen durch das CERT und Beratungen zum Krisenmanagement.
- Das Hessen3C unterstützt zur Evaluierung und Weiterentwicklung bestehender Prozesse regelmäßig Krisen- und Alarmierungsübungen im Rahmen des IT-Krisenmanagements (IT-KM) innerhalb der Landesverwaltung.
- Gemäß BSI-Gesetz ist das Hessen3C die zentrale Kontaktstelle für das BSI in Angelegenheiten der Sicherheit in der Informationstechnik bei Betreibern Kritischer Infrastrukturen in Hessen.

Polizei Hessen

In Fragen der Prävention stehen den Bürgerinnen und Bürgern Fachberatungsstellen der Prävention-Cybercrime unter Koordination des Hessischen Landeskriminalamts (HLKA) als versierte Anlaufstellen in allen Polizeipräsidien bereit. Die Landeskoordination im Hessischen Landeskriminalamt nimmt neben der Koordinierungsfunktion die Aufgaben der Fachberatungen mit hessenweitem Charakter wahr. Darüber hinaus bildet die Zentrale Ansprechstelle Cybercrime (ZAC) des Hessischen Landeskriminalamtes für die Wirtschaft eine Brücke zwischen Gefahrenabwehr und Strafverfolgung, indem sie hessische Unternehmen im Vorgriff auf und während Cybervorfällen zu sämtlichen Leistungen der hessischen Polizei berät.

Zur Bekämpfung von Straftaten stehen im HLKA die Spezialisten der Zentralen Ansprechstelle Cybercrime für die Wirtschaft (ZAC) mit einer telefonischen Hotline den Wirtschafts- und KRITIS-Unternehmen zur qualitativ hochwertigen Anzeigenaufnahme zur Verfügung und gewährleisten bei Cyberangriffen die schnelle Einleitung von Erstmaßnahmen zur Sicherung häufig flüchtiger Spuren. Die ZAC leistet die Koordination von Ermittlungen innerhalb der Polizei und in der Zusammenarbeit mit der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) bei der Generalstaatsanwaltschaft Frankfurt am Main. Gleichfalls übernehmen besonders ausgebildete Polizeivollzugsbeamte der Cybercrime-Ermittlungen des HLKA herausragende Ermittlungsverfahren. Spezialisierte Zentralkommissariate in den Polizeipräsidien bearbeiten grundsätzlich die Delikte in örtlicher Zuständigkeit. Die Ermittlungsdienststellen zum Phänomen „Cybercrime im engeren Sinne" (§§ 202a ff., 263a, 269 f., 303a f. StGB) haben das einzigartige Mittel der bundesweit abgestimmten „Zentralen Ermittlungen" geprägt. Hierbei führt eine Ermittlungsdienststelle für eine definierte Straftatenwelle die Spuren zusammen und ermittelt diese aus. Ermittlungsberichte werden in der Folge den aktenführenden Dienststellen bundesweit zur Verfügung gestellt und in die dortigen Verfahren integriert. Mit diesem modernen Mittel der Ermittlungsführung werden Vielfach-Befassungen minimiert und die fortwährende Strafverfolgung der Vielzahl von Angriffen im Cyberraum ressourcenschonend gewährleistet. Hierzu leistet auch die Polizei Hessen ihren Beitrag.

Die Technische Ermittlungsunterstützung (TEU) des HLKA erbringt zusammen mit den Fachkommissariaten der Polizeipräsidien den essenziellen Service der digitalen Identifizierung von Personen / Tätern sowie Spurensuche und -interpretation für die Phänomenbereiche abseits der Cybercrime im engeren Sinne. Zur Anwendung kommen regelmäßig die Informationsgewinnung aus frei verfügbaren Internetquellen (OSINT) sowie das Sammeln, Auswer-

ten und Darstellen von Benutzerinhalten auf Social-Media-Plattformen (SOCMINT). Die TEU des HLKA als Fachstelle der Polizei Hessen koordiniert und etabliert Verfahrensweisen sowie Standards und führt darüber hinaus technisch komplexe Maßnahmen durch. In ihrer Zentralstellenfunktion bildet die TEU die Schnittstelle zu den Dienstanbietern für Soziale Netzwerke (SPOC-Funktion) ab und beteiligt sich an verschiedenen Forschungsprojekten.

Als Zentralstelle stellt das HLKA das Bindeglied zu den Services des BKA dar. Die Entwicklung des BKA als zentraler Dienstleister für die Länderpolizeien in einem globalen Kriminalitätsphänomen wird mit den verfügbaren Mitteln unterstützt, sodass hessische Strafverfolgungsbehörden maximal von den Angeboten des Bundes profitieren können.

Besondere Deliktsphänomene im Zusammenhang mit Kryptowährungen und Smart Contracts sowie Ermittlungsverfahren im Bereich des Darknets werden aufgrund ihrer Komplexität und des erforderlichen Fachwissens derzeit vorrangig im HLKA geführt. Die Polizei Hessen hat als eine der ersten Polizeibehörden in Deutschland neben dem klassischen Erkennungsdienst auch einen Digitalen Erkennungsdienst (DED) etabliert, wodurch gezielt digitale Spuren als Beweismittel in Strafverfahren sichergestellt werden.

Landesamt für Verfassungsschutz

Das Landesamt für Verfassungsschutz (LfV) dient dem Schutz der Inneren Sicherheit und informiert die Landesregierung und die Öffentlichkeit über die Sicherheitslage. Es ist zuständig für die Sammlung und Auswertung von Informationen über nachrichtendienstlich gesteuerte sowie extremistisch oder terroristisch motivierte Cyberangriffe.

Insbesondere auf dem Feld der hybriden Bedrohung wird derzeit eine Zunahme der Aktivitäten fremder Mächte festgestellt. Ziel der Angriffe ist es, die öffentliche Meinung zu beeinflussen, die Gesellschaft zu spalten und insgesamt die Demokratie zu destabilisieren. Offene, pluralistische und demokratische Gesellschaften bieten hierfür große Angriffsflächen. Der Cyberraum ist dabei für Spionage und Sabotage sowie für Desinformation und Propaganda ein bevorzugter Operationsraum hybrider Akteure. Hybride Kampagnen sind ein neuer Standard geopolitischer Konflikte in den weltweiten Auseinandersetzungen zwischen einzelnen Staaten.

Brand- und Katastrophenschutz

Der hessische Katastrophenschutz deckt ein breites Aufgabenspektrum ab. Dabei durchdringt die IT mittlerweile sämtliche Aufgabenbereiche, insbesondere die Bereiche „Führung" sowie „Information und Kommunikation" (IuK) – zum Beispiel in Form von smarten Führungsmitteln, zur Darstellung und zum Austausch von Lageinformationen oder für das Einsatzkräfte- und Helfermanagement. Cybersicherheit spielt dabei nicht nur im Sinne der Hochverfügbarkeit dieser Mittel (auch in Krisensituationen) eine zentrale Rolle, sondern auch hinsichtlich des Schutzes der verarbeiteten meist sensiblen Daten vor illegitimem Abgriff und hinsichtlich ihrer Authentizität.

Flankierend zu den Maßnahmen der originär zuständigen Fachbehörden ist der Schutz Kritischer Infrastrukturen (KRITIS) eine Querschnittstätigkeit über alle Aufgabenbereiche des Katastrophenschutzes hinweg. In Zusammenarbeit mit den KRITIS-Betreibern werden – parallel zu den Vorkehrungen, um Ausfälle zu vermeiden – insbesondere Maßnahmen ergriffen, um sich bestmöglich auf (unvermeidbare) Ausfälle vorzubereiten. Der Katastrophenschutz unterstützt im Falle eines Falles die Krisenmanagementmaßnahmen der Betreiber und Fachbehörden zur (Not-)Versorgung der Bevölkerung und anderer KRITIS im Sinne der Abwehr von unmittelbaren Gefahren für Leib und Leben und der Linderung der schlimmsten Folgen für die Bevölkerung. Für einen großflächigen, langandauernden Stromausfall bspw. hat das Land den hessischen Katastrophenschutzorganisationen entsprechende Stromerzeuger zur Verfügung gestellt – auch um wichtige IT-Infrastruktur weiter betreiben zu können.

Im Hessischen Ministerium des Innern und für Sport – als oberste Katastrophenschutzbehörde – ist zudem die sogenannte Ressort-Koordinierungsstelle „Kritische Infrastrukturen" (KoSt KRITIS) eingerichtet, die Belange des KRITIS-Schutzes zwischen den Ressorts der Landesregierung unter Wahrung der fachlichen Ressortzuständigkeiten koordiniert und als Ansprechpartner für die Koordinierungsstellen der Länder sowie die Koordinierungsstelle des Bundes fungiert. Im Sinne der Netzwerkarbeit wird hierüber ebenfalls der Schulterschluss mit KRITIS-Betreibern sowie die Verzahnung mit Hessen3C und weiteren Akteuren in strategischen wie operativen Fragen der Cybersicherheit ermöglicht – von präventiven Konzepten über prophylaktische Vorbereitungen für Störungssituationen und trainierenden Übungen bis hin zur reaktiven Vorfallsbewältigung.

Schwerpunkt / Zielsetzung

Die Stärkung und konsequente Fortentwicklung des Hessen3C zu dem behördenübergreifenden Cyber- und IT-Sicherheitskompetenzzentrum des Landes Hessen sowie der Ausbau der hiervon ausgehenden Unterstützungs- und Beratungsleistung werden in den kommenden Jahren mit Nachdruck vorangetrieben. Die Kommunen gilt es bei der Erhöhung ihres Cyber- und IT-Sicherheitsniveaus zukünftig noch stärker zu unterstützen.

Der rasanten technologischen Entwicklung und den geopolitischen Ereignissen ist zukünftig schnell und hochflexibel mit kontinuierlicher Anpassung technischer, personeller und organisatorischer Rahmenbedingungen zu begegnen. Um dies zu erreichen, wird eine Verstärkung der bestehenden MIRT sowie der personelle und technische Ausbau der ZAC sowie der zuständigen Fachdienststellen der Polizei angestrebt. Fachkräfte der Sicherheitsbehörden werden verstärkt, orientiert an den aktuellen technologischen Entwicklungen, sowie in Zusammenarbeit mit den Forschungseinrichtungen in Hessen aus- und fortgebildet.

Die Schnittstellen zu den weltgrößten Dienstanbietern für Soziale Netzwerke werden für die Polizei aber auch im Kampf gegen Hass und Hetze im Netz weiter ausgebaut.

Verantwortlichkeit

HMdIS – Landespolizeipräsidium
HMdIS – Abteilung V
HMdIS – Abteilung II
HMdIS – Abteilung VII – Referat 12 (Hessen3C)
HMdIS – Abteilung VII – Referat 13
CISO
Landesamt für Verfassungsschutz Hessen

5.1.5 Informationssicherheit

5.1.5.1 Informationssicherheitsleitlinie

Bedeutung

Die Leitlinie für Informationssicherheit der öffentlichen Verwaltung des IT-Planungsrats (Stand 2018) gilt für alle Behörden und Einrichtungen der Bundes- und Landesverwaltung. Sie beinhaltet Mindestsicherheitsstandards und übergreifende Regelungen zu den folgenden Handlungsfeldern:

1. Informationssicherheitsmanagement
2. Absicherung der IT-Netzinfrastrukturen der öffentlichen Verwaltung
3. Einheitliche Sicherheitsstandards für ebenen-übergreifende IT-Verfahren
4. Gemeinsame Abwehr von IT-Angriffen
5. IT-Notfallmanagement

Die Informationssicherheitsleitlinie der hessischen Landesverwaltung (ILL) legt unter Berücksichtigung der Regelungen aus der Leitlinie des IT-Planungsrats unter anderem die strukturellen Vorgaben für das Informationssicherheitsmanagement (ISM) der hessischen Landesverwaltung fest. Die hierin enthaltenen Regelungen und Empfehlungen sind zu berücksichtigen. Sie bildet damit auch die Basis für die Informationssicherheitsmanagementprozesse des Landes und kann als Beratungsgrundlage für die Kommunen in eigener Zuständigkeit herangezogen werden.

Gegenwart

Mit der aktuellen Version der ILL der hessischen Landesverwaltung, welche am 22. November 2021 durch das HMdIS in Kraft gesetzt wurde, wurde die Leitlinie aus 2016 fortgeschrieben.

Die Etablierung des CISO Hessen sowie die Ernennung von Informationssicherheitsbeauftragten für jede Dienststelle sind als zentrale Elemente der ILL Hessen umgesetzt.

Schwerpunkt / Zielsetzung

Die hessische Landesverwaltung wird die flächendeckende Erstellung von Informationssicherheitskonzepten nach BSI-Standard 200-2 bei übergreifenden Fachverfahren und vor der Inbetriebnahme von IT-Systemen und Infrastrukturen in den kommenden Jahren vehement

vorantreiben, da diese die wesentliche Grundlage zur Absicherung von Sicherheitsvorfällen sind.

Um Trends im Bereich von Cyberbedrohungen frühzeitig zu erkennen und die Koordination von Cybersicherheitsvorfällen zu erleichtern, wird die zentrale Erfassung und Auswertung von Sicherheitsvorfällen in IT-Anwendungen / Systemen und Infrastrukturen weiter ausgebaut. Hieraus gewonnene Erkenntnisse fließen unmittelbar in die Risikobeurteilung, Absicherung und Verbesserung der vorhandenen IT-Landschaft ein.

Die Landesregierung verfolgt hierbei insbesondere den Ausbau des Risikomanagements für sensible Bereiche, welche einen sehr hohen Schutzbedarf aufweisen.

Verantwortlichkeiten

HMdIS – Abteilung VII – Referat VII 3
HMdIS – Abteilung VII – Referat VII 12 (Hessen3C)
HMdIS – Abteilung VII – Referat 13
CISO

5.1.5.2 Informationssicherheitsmanagement

Bedeutung

Ein Informationssicherheitsmanagementsystem ist ein Rahmenwerk zur Etablierung und Fortführung eines kontinuierlichen Prozesses zur Planung, Durchführung, Kontrolle und Verbesserung jener Konzepte und Aufgaben, die der Wahrung der Informationssicherheitsziele in einer Institution dienen. Zur Wahrung dieser Ziele ist es notwendig, ein angemessenes und ausreichendes Sicherheitsniveau umzusetzen, zu erhalten und fortzuentwickeln.

Gegenwart

Für jede Dienststelle ist ein Informationssicherheitsbeauftragter (ISB) bestellt. Dieser betreibt das jeweilige ISMS und entwickelt es nach den Grundsätzen security by design bzw. security by default sowie im Sinne eines ständigen Verbesserungsprozesses weiter.

Schwerpunkt / Zielsetzung

Zur Stärkung des landesweiten Cyber- und IT-Sicherheitsniveaus sieht die Landesregierung in ihrer Cybersicherheitsstrategie für jede Dienststelle die Entwicklung und den Betrieb eines Informationssicherheitsmanagementsystems (ISMS) vor.

Verantwortlichkeit

Alle Ressorts

5.1.5.3 Standardisierung der Prozesse und Produkte

Bedeutung

Standardisierte Prozesse und Produkte sind als wesentliches Element der Informationssicherheit bereits durch die ILL identifiziert. Diese Standardisierung und Synergieeffekte gilt es, in allen Prozessen und Produkten anzustreben.

Gegenwart

Das Land Hessen hat mit dem HessenPC einen standardisierten Client zur Nutzung in der Landesverwaltung eingeführt. Dieser wird kontinuierlich an den Bedarfen der Dienststellen orientiert angepasst und in der jeweiligen Konfigurierungs- und Planungsphase weiterentwickelt.

Die Standards werden in spezifischen ressortübergreifenden Gremien und Arbeitskreisen erarbeitet.

Die Hessische Zentrale für Datenverarbeitung (HZD) arbeitet an der Umsetzung eines auf die Bedürfnisse der Landesverwaltung zugeschnittenen und mit dem Hessischen Ministerium der Finanzen sowie der Hessischen Ministerin für Digitale Strategie und Entwicklung abgestimmten Programms zur Cloud-Transformation, mit höchsten Sicherheitsstandards und kompetenter Cloud-Beratung.

Schwerpunkt / Zielsetzung

Mit der geplanten Einführung einer Cybersicherheitsquote für Projekte in Höhe von 15 % des Gesamtbudgets will die Landesregierung einen wichtigen Impuls zur Verankerung von Cybersicherheit in Landesvorhaben setzen.

Die verpflichtende Betrachtung der Informationssicherheit über alle Projektphasen hinweg und insbesondere bei der Ausschreibung wird somit sichergestellt. Zur stärkeren Standardisierung von IT-Projekten wird das „Projektmanagementhandbuch für IT-Projekte des Landes Hessen“ um die Aspekte der Informationssicherheit angepasst und zukunftsfähig weiterentwickelt.

Um ein größtmögliches Sicherheitsniveau des in der Landesverwaltung verwendeten HessenPC zu gewährleisten, werden bei der Fortentwicklung des HessenPC aktuelle hard- und softwarebasierte Sicherheitstools erprobt und integriert.

Verantwortlichkeit

HMinD - in Abstimmung mit den Ressorts
HZD
HMdIS – Abteilung VII – Referat VII 3
HMdIS – Abteilung VII – Referat VII 13
CISO

5.1.6 Analyse und Reaktionsfähigkeit

Bedeutung

Um der gestiegenen Bedrohungslage für informationstechnische Systeme angemessen begegnen zu können, sind festgelegte, kooperative und standardisierte Vorgehensweisen notwendig. Diese müssen stetig an aktuelle Entwicklungen angepasst werden. Nur durch aufeinander abgestimmte und gleichlaufende Prozesse sowie definierte Schnittstellen ist das Zusammenwirken länder- und behördenübergreifender Einheiten möglich.

Hierzu müssen bei Beginn eines Angriffs auch die Analysemethode und notwendige Reaktionen harmonisiert werden, sodass unterschiedliche Akteure zeitnah und effektiv zusammenarbeiten können.

Gegenwart

Mit dem CERT Hessen als integralem Bestandteil des Hessen3C steht den hessischen Landesbehörden, Kommunen sowie KMU eine Anlaufstelle zu Cybersicherheitsfragen mit einer 24/7-Erreichbarkeit zur Verfügung.

- Werktäglicher Schwachstellenbericht zur IT-Sicherheit
- Anlassbezogene Beratungsleistung
- Unterstützung bei IT-Sicherheitsvorfällen
- Beratung zum IT-Krisenmanagement
- Analyse der Angriffswege auf die IT-Infrastruktur
- Beratung zu gesetzlichen Meldepflichten und Erstattung von Strafanzeigen
- Unterstützung mit Sicherheitsprodukten, wie
    - Hessen Leak Checker: Prüfung und Warnung vor durch Diebstahl oder Datenlecks kompromittierten dienstlichen E-Mail-Adressen
    - Malware Information Sharing Plattform (MISP) für Kommunen

Mit dem Mobile Incident Response Team (MIRT) verfügt das CERT Hessen über eine Notfalleinheit, die Betroffene im Bedarfsfall vor Ort unterstützt.

Das Hessen3C übernimmt hierbei die Funktion eines Bindeglieds zu den jeweiligen zuständigen hessischen Sicherheitsbehörden.

Das Computer Security Incident Response Team (CSIRT-HZD) der HZD ist die zentrale Managementinstanz und Anlaufstelle für sicherheitsrelevante Ereignisse und Beobachtungen in der IT-Infrastruktur der Landesverwaltung. Es hat die technischen und organisatorischen Ressourcen für die proaktive und reaktive Bekämpfung von Risiken für die Informationssicherheit im IT-Betrieb der HZD. Um diese zu gewährleisten, werden reaktive Maßnahmen zum schnellen Schließen von Sicherheitslücken mit präventiven Aktivitäten zum Umgang mit Schwachstellen kombiniert. Das CSIRT-HZD berät die Dienststellen hierzu bei Bedarf.

Weitere operativ und analytisch tätige Einheiten befinden sich im Bereich der hessischen Sicherheitsbehörden (Zentrale Ansprechstelle Cybercrime (ZAC) des Hessischen Landeskriminalamtes) und in weiteren Ressorts der Landesverwaltung, wie beispielsweise das CERT-Justiz sowie das Kommunale Dienstleistungszentrum Cybersicherheit (KDLZ-CS) der ekom21.

Schwerpunkt / Zielsetzung

Zur Stärkung der Analysekompetenz der Fachdienststellen in Hessen wird zukünftig mehr in gezielte Fortbildungsmaßnahmen investiert.

Mit der Schaffung von gesetzlichen Rahmenbedingungen und dem Ausbau eingesetzter Hard- und Software plant die Landesregierung eine effizientere und effektivere Verarbeitung von Informationen und Steigerung der Analyse- und Reaktionsfähigkeit zum Schutz der hessischen Landesverwaltung, der Kommunalverwaltung und der Wirtschaftsunternehmen in Hessen.

Verantwortlichkeit

HZD
HMdJ
HMdIS – Abteilung VII – Referat VII 12 (Hessen3C)
CISO
HMdIS – Landespolizeipräsidium

5.1.7 Gemeinsame Abwehr von Cyberangriffen

Bedeutung

Aufgrund der Zunahme fortgeschrittener und gezielter Cyberangriffe ist die Früherkennung von Sicherheitslücken von besonderer Bedeutung. Die gemeinsame Abwehr von Angriffen auf Anwendungen und IT-Systeme bedarf sowohl einer präventiven als auch einer reaktiven Betrachtung. Der Austausch und die Zusammenarbeit mit Partnern im Bereich der Cybersicherheit ist aufgrund der Komplexität und Vielfalt der Themen essenziell. Für Hessen nimmt Prävention deshalb in der erfolgreichen Abwehr von Cyberangriffen eine zentrale Rolle ein. In reaktiver Hinsicht stellen vorbereitete, eingeübte und professionalisierte Verfahrensabläufe zur schnellstmöglichen Wiederaufnahme des Normalbetriebs in Folge eines Cyberangriffs ein wesentliches Erfolgskriterium dar.

Gegenwart

Das Hessen3C ist sowohl auf Landesebene als auch länderübergreifend und auf Bundesebene mit zahlreichen Akteuren vernetzt. Seitens des Hessen3C werden anlassbezogene und regelmäßige Lageberichte mit Einrichtungen der Landesverwaltung, Kommunen sowie hessischen Unternehmen ausgetauscht. Darüber hinaus finden wöchentliche Lagebesprechungen mit den hessischen Sicherheitsbehörden statt. Alle gewonnenen Erkenntnisse und Lageentwicklungen fließen in die Beratungs- und Awareness-Veranstaltungen des Hessen3C ein.

Über den VerwaltungsCERT-Verbund besteht im länderübergreifenden Kontext eine kooperative Zusammenarbeit mit den CERTs der Länder und des Bundes (VCV). Die Verbindung zur Bundesebene stellt ein ständiger Vertreter Hessens über die Teilnahme im Nationalen Cyber-Abwehrzentrum sicher, welcher an den täglichen Lagebesprechungen und anlassbezogenen Zusammenarbeitsformaten teilnimmt.

Mit der aktuellen ILL wurden notwendige Voraussetzungen zur koordinierten Vorfallsbearbeitung und Meldewege für die Ressorts definiert. So wurde ein weiterer Schritt für die Erstellung eines ressortübergreifenden Lagebildes umgesetzt.

Schwerpunkt / Zielsetzung

Die Abwehr von Cyberangriffen steht für die Landesregierung an erster Stelle, diese soll mit der Weiterentwicklung der landeseigenen IT-Infrastruktur gewährleistet werden. Bei erfolg-

ten Angriffen stehen die Fachdienststellen den Betroffenen zur Unterstützung und Hilfeleistung zur Verfügung.

Die Landesregierung hat Cybersicherheit als wichtiges Thema erkannt. Unter Koordinierung des HMdIS übernehmen die Ressorts gemeinsam Verantwortung zur Sicherstellung von Cybersicherheit. Zur Gewährleistung eines Normalbetriebs in Folge eines Cybersicherheitsvorfalls gibt die Landesregierung den Fachdienststellen vor, durch regelmäßige Übungen sowie die Fortentwicklung des IT-KM in Zusammenarbeit mit den relevanten Akteuren aus Bund, Ländern, Kommunen und KRITIS mögliche Szenarien zu üben und vorzubereiten.

Verantwortlichkeit

Alle Ressorts
HMdIS – Abteilung VII
HMdIS – Abteilung VII – Referat VII 12 (Hessen3C)
HMdIS – Abteilung VII – Referat VII 13
CISO
HZD

5.1.8 Rechtliche Rahmenbedingungen

Bedeutung

Ein normativer Rahmen ist zentrale Voraussetzung zur Schaffung notwendiger Befugnisse, um zu einer Erhöhung der Cybersicherheit auf Landesebene beitragen zu können.

Ferner sind darüber hinaus in Teilbereichen der rechtlichen Normierung, wie beispielsweise dem Internet der Dinge (IoT), EU-weite gesetzliche Anforderungen inklusive Marktzugangsregelungen sowie Normen und Standards für Unternehmen im Bereich der Cybersicherheit notwendig.

Ein gesetzlicher Rahmen schafft Handlungssicherheit für alle Akteure der Cybersicherheit. Im Bereich der IT- und Informationssicherheit gibt es zahlreiche Gesetze und Verordnungen, die diesen Handlungsrahmen definieren, z. B. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0), Telekommunikationsgesetz (TKG), Telemediengesetz (TMG), Datenschutzgrundverordnung (DSGVO), Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) sowie die Richtlinien des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS 1 und NIS 2 - Richtlinie). Somit wird deutlich, dass Cybersicherheit in einer Vielzahl unterschiedlicher Rechtsvorschriften sowohl auf nationaler als auch europäischer Ebene aufgegriffen wird, aber nicht innerhalb eines einheitlichen Gesetzeswerkes kodifiziert ist.

Adressaten dieser IT-sicherheitsrechtlichen Regelungen sind Systeme, Hersteller, Anbieter, Betreiber und Nutzer von IT-Systemen und Produkten sowie diejenigen, die an der Einhaltung von Verpflichtungen mitwirken oder sie durchsetzen, etwa Prüfunternehmen, IT-Sicherheits- oder Strafverfolgungsbehörden.

Das derzeitige rechtliche Instrumentarium bildet den digitalen Raum jedoch nicht ausreichend ab, da aufgrund der Gesetzgebungsverfahren der rechtliche Rahmen mit der rasanten technischen Entwicklung häufig nicht Schritt halten kann.

Gegenwart

Mit dem Hessischen IT-Sicherheitsgesetz (HITSiG) schafft Hessen die landesgesetzlichen Rahmenbedingungen zur Stärkung der Analyse- und Reaktionsfähigkeit in der IT-Sicherheit sowie den Ausbau der hessischen Cybersicherheitsarchitektur. Mit den in der Informations-

sicherheitsleitlinie für die hessische Landesverwaltung (2021) definierten Rollen, Zuständigkeiten und Meldewegen wurde insbesondere für die Reaktion auf Cybersicherheitsvorfälle eine Basis gelegt. Damit hat Hessen frühzeitig die gemeinsam zwischen Bund und Ländern festgelegten Anforderungen des IT-Planungsrats umgesetzt.

Zudem sind auch in Hessen IT-Sicherheit und Datenschutz untrennbar miteinander verbunden. Dies spiegelt sich insbesondere in der engen Zusammenarbeit der für Cybersicherheit zuständigen Behörden mit dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit wider.

Schwerpunkt / Zielsetzung

Das hessische Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG) ist als Handlungsrahmen für die Landesverwaltung zur Erhöhung der Cyber- und IT-Sicherheit von wesentlicher Bedeutung. Der Landtag hat das Hessische Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG) beschlossen. Dieses Gesetz wurde am 10. Juli 2023 verkündet und trat am Tag nach der Verkündung in Kraft (Nr. 21 – Gesetz- und Verordnungsblatt für das Land Hessen – 10. Juli 2023).

Darüber hinaus wird die hessische Landesregierung sicherstellen, dass notwendige (landes-) gesetzliche Anpassungen im Rahmen ihrer Zuständigkeit sowie mittels entsprechender Eingaben für nationale und europäische Gesetzgebungsverfahren eingebracht werden.

Verantwortlichkeit

HMdIS – Abteilung VII - Abteilungsstab
HMdIS – Abteilung II
HMdIS – Landespolizeipräsidium

5.1.9 Cybersicherheitszertifizierungen

Bedeutung

Die Zertifizierung von Produkten, Dienstleistungen und Prozessen schafft Vertrauen sowie Vergleichbarkeit und spielt bei der Erhöhung des Cybersicherheitsniveaus eine bedeutende Rolle.

Der Stellenwert von Informationssicherheit ist in den letzten Jahren deutlich gestiegen. Damit sind auch die Anforderungen an das Informationssicherheitsmanagementsystem (ISMS) gewachsen. Dies kommt durch die zunehmende Forderung nach Zertifizierung zum Ausdruck. Durch die Prozessausrichtung sind davon praktisch alle Bereiche einer Organisation betroffen und können nicht losgelöst voneinander betrachtet werden. Mit der Berücksichtigung von Datenschutz und Nachhaltigkeit gewinnen zudem auch Compliance-Themen an Bedeutung.

Gegenwart

In Bündelung einer gesamtheitlichen Zertifizierungsstrategie hat die HZD eine Compliance-Strategie integriert. Ausgangspunkt der auf mehrere Jahre ausgelegten Aktivitäten ist die Zertifizierung des hessischen Anschlusses an das Verbindungsnetz des Bundes. Dieses ist eine Kerninfrastruktur in Deutschland, über die Einrichtungen der Bundes- und Landesverwaltung sowie Kommunen miteinander kommunizieren. Um die Sicherheitsstandards für dieses Verbindungsnetz verbindlich zu machen, hat der IT-Planungsrat die neuen Anschlussbedingungen beschlossen. Dieses Projekt erfüllt eine Vorbildfunktion, da die Erfahrungen und Vorgehensweisen auch für noch folgende Zertifizierungsvorhaben herangezogen werden sollen. Die Zertifizierung ist somit nicht nur der erste Schritt der HZD-Zertifizierungsstrategie, sondern auch Wegbereiter zukünftiger Maßnahmen.

Im BSI ist die nationale Behörde für Cybersicherheitszertifizierung (NCCA) verortet, welche für die Überwachung und Durchsetzung der Vorschriften im Rahmen der europäischen Schemata gemäß der Verordnung (EU) 881/2019 (Cybersecurity Act) zuständig ist.

Die durch das HMdIS sichergestellte Koordinierung und Überwachung der Einführung von flächendeckenden Informationssicherheitskonzepten sowie von Informationssicherheitsmanagementsystemen gemäß der Vorgabe des BSI unter anderem zum IT-Grundschutz stellt die Grundlage für weitere Zertifizierungen im IT-Sicherheitsbereich in Hessen dar. Der

Betrieb eines ISMS ist die Basis für eine erfolgreiche Zertifizierung. Das HMdIS hat in Zusammenarbeit mit der ekom21 das kommunale Dienstleistungszentrum Cybersicherheit (KDLZ-CS) ins Leben gerufen. Dieses hat die Erhöhung des Cybersicherheitsniveaus bei Kommunen zum Ziel und orientiert sich in der aktuellen Ausbaustufe ebenfalls am BSI-Grundschutz.

Schwerpunkt / Zielsetzung

Die Landesregierung unterstützt die Umsetzung von übergreifenden und harmonisierten Standards im Cyber- und IT-Sicherheitsbereich und verfolgt die Umsetzung und Erfüllung des BSI-Grundschutzes für alle relevanten Organisationseinheiten. Für den kommunalen Bereich ist mit Blick auf ein hohes einheitliches Cybersicherheitsniveau eine Erweiterung der etablierten Förderung des KDLZ-CS vorgesehen.

Verantwortlichkeit

HMdIS

HZD

5.1.10 Cybersicherheit in Schulen

Bedeutung

Den Schulen in Hessen kommt bei der Vermittlung praxisrelevanter Cybersicherheitskompetenzen eine besondere Rolle und Verantwortung zu. Mit einer Integration von Fragen der Cybersicherheit im Rahmen der digitalen Bildung in den Schulen kann bereits frühzeitig ein Bewusstsein geschaffen werden, um Cyberangriffen vorbeugen zu können.

Die Kultusministerkonferenz hat die Bedeutung von digitaler Bildung erkannt und mit der Strategie „Bildung in der digitalen Welt" und dem Ergänzungspapier „Lehren und Lernen in der digitalen Welt" beschlossen, dass Schülerinnen und Schüler während ihrer Pflichtschulzeit digitale Kompetenzen erwerben sollen.

Auch im Zuge des zunehmend digital gestützten Unterrichts, etwa über den zunehmenden Einsatz von Videoplattformen während der Covid-19-Pandemie hat das Thema und die Notwendigkeit von Cybersicherheit in ein neues Licht gerückt, um etwa Unbefugten keinen Zutritt zu den Konferenzen zu verschaffen. Schülerinnen und Schülern einen sicheren digitalen Raum zum Lernen zu gewährleisten, muss prioritäre Aufgabe der Verantwortlichen sein.

Gegenwart

Im Bildungsbereich investiert Hessen umfassend im Rahmen des Landesprogramms „Digitale Schule Hessen" in die Verbesserung der digitalen Ausstattung von Schulen mit zeitgemäßer Technik. Das Land stellt den Schulen darüber hinaus mit dem Schulportal Hessen eine sichere Lern- und Arbeitsplattform bereit. Diese wurde um ein sicheres und einheitliches Videokonferenzsystem ergänzt, um hessische Schülerinnen und Schüler sowie deren Daten vor Cyberangriffen zu schützen.

Das Thema Cybersicherheit findet auch im stetig wachsenden Fortbildungsangebot für Lehrkräfte zur Förderung ihrer digitalen Kompetenzen Berücksichtigung. Mit der Einrichtung der Beratungsstelle Jugend und Medien Hessen durch das Hessische Kultusministerium (HKM) und die Hessische Ministerin für Digitale Strategie und Entwicklung (HMinD) werden neben den Lehrkräften, Schülerinnen und Schüler auch die Eltern in Fragen des sicheren und verantwortungsvollen Umgangs mit digitalen Medien unterstützt.

Ab dem Schuljahr 2022/2023 startete Hessen mit dem Pilotprojekt „Digitale Welt" die Einführung eines neuen Unterrichtsfachs an zwölf Pilotschulen in Hessen. Dieses Fach verbin-

det grundlegende Kompetenzen der Informatik mit der ökonomischen und ökologischen Bildung. Die Schülerinnen und Schüler lernen im Unterricht, wie digitale Technologien zur Lösung sozialer, ökonomischer und ökologischer Problemstellungen beitragen können. Das Pilotprojekt wird in Kooperation mit dem Hasso-Plattner-Institut (HPI) in Potsdam durchgeführt und von der Goethe-Universität in Frankfurt am Main wissenschaftlich begleitet und nach einem Jahr evaluiert.

Schwerpunkt / Zielsetzung

Sich im digitalen Raum zu bewegen, ist für Kinder und Jugendliche heute selbstverständlich. Die Hessische Landesregierung stellt daher sicher, dass Cybersicherheitsthemen im Unterricht fest verankert werden. Durch die regelmäßige Fortschreibung der Lehrinhalte an Trends und Entwicklungen im Bereich der Cybersicherheit soll die Aktualität sichergestellt werden.

Gleichermaßen gilt dies für aktuelle und zukünftige Lehrkräfte an den hessischen Schulen, die in allen Ausbildungsphasen die notwendigen Kompetenzen erlangen sollen.

Nach Prüfung der Ergebnisse der Evaluation des neu eingeführten Schulfachs „Digitale Welt“ an den Pilotschulen unterstützt die Landesregierung seine flächendeckende Einführung. Mit der regelmäßigen Weiterentwicklung des „Schulportal Hessen“ soll eine dauerhafte, zuverlässige und sichere Lern- und Arbeitsumgebung gewährleistet werden.

Verantwortlichkeiten

HKM

5.1.11 Cybersicherheit Dokumentenmanagementsystem (DMS)

Bedeutung

Informationssicherheit ist eine Grundvoraussetzung für die Modernisierung interner Verwaltungsprozesse, deren zentrales Element die digitale Realisierung übergreifender E-Government-Dienste ist. Lücken in der Sicherheitsarchitektur von Digitalisierungsprojekten und daraus resultierende erfolgreiche cyberkriminelle Attacken können neben erheblichen rechtlichen Konsequenzen einen massiven Vertrauensverlust in die Digitalisierung der hessischen Verwaltung sowohl bei den Anwendenden wie auch bei den Bürgerinnen und Bürgern bewirken. Für das Projekt „DMS-Modernisierung", das die Einführung eines neuen Dokumentenmanagementsystems (DMS) in der hessischen Landesverwaltung für die elektronische Bearbeitung von Akten, Vorgängen und Dokumenten zum Ziel hat, sind deshalb Präventionsmaßnahmen zur Abwehr von Cyberkriminalität von großer Bedeutung. Das neue DMS 4.0 wird das im Jahr 2004 eingeführte Dokumentenmanagementsystem Hessische eDokumentenverwaltung (HeDok) ablösen und den Anwenderinnen und Anwendern ein performanteres, zukunftsfähiges Arbeitsumfeld bieten mit komfortableren intuitiven Prozessen, modernen integrierten Anwendungen und einem höheren Digitalisierungsgrad mit entsprechenden Sicherheitsstandards.

Gegenwart

Die Festlegung und Erfüllung von Sicherheitsanforderungen im Bereich elektronische Aktenführung und Vorgangsbearbeitung sind als strategische Projektziele definiert, insbesondere zur Gewährleistung von Informationssicherheit, Datenschutz und Geheimschutz. Es wird der Nachweis geführt, dass die Regelungen der Datenschutz-Grundverordnung (DS-GVO), des Bundesdatenschutzgesetzes (BDSG) und für Hessen des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG) Anwendung finden.

Die gemeinsame Infrastruktur des Landes Hessen, die die Hessische Zentrale für Datenverarbeitung (HZD) für alle Dienststellen des Landes bereitstellt, gewährleistet ein hohes Niveau an Cybersicherheit. Als standardisierte Landeslösung wird das DMS 4.0 auf dieser sicheren Infrastruktur allen Verwaltungsmitarbeiterinnen und -mitarbeitern zur Verfügung stehen. Durch die Integration in die gemeinsame Infrastruktur findet auch der Einsatz weiterer Anwendungen wie Office-Produkte etc. in einem geschützten Umfeld statt. Potentielle Risiken durch Medienbrüche werden mittels größtmöglicher Standardisierung und durchgängiger elektronischer Prozesse vermieden. Für das DMS 4.0 werden ein IT-Sicherheitskonzept in enger

Abstimmung mit der HZD und ein Datenschutzkonzept inkl. Datenschutzfolgenabschätzung, Verzeichnis der Verarbeitungstätigkeiten und Berechtigungskonzept unter Beteiligung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) erstellt. Letzteres entspricht – im Rahmen des Verantwortungsbereichs des Handelnden – den Anforderungen der DS-GVO, dort insbesondere den Art. 5, 25 und 32 DS-GVO, bzw. gibt Aufschluss darüber, wie die dort niedergelegten Grundsätze eingehalten werden. Die Vorlage der Konzepte ist Voraussetzung für die Produktivsetzung des neuen DMS.

Schwerpunkt / Zielsetzung

Ziel ist, mit dem neuen DMS 4.0 ein hochperformantes, zukunftsfähiges Arbeitsumfeld zu schaffen, das den Anwenderinnen und Anwendern unter Beachtung aller relevanten Sicherheitsaspekte mehr Komfort und Flexibilität bietet. Die Pilotierung im Projekt DMS-Modernisierung ist in der ersten Jahreshälfte erfolgt (19. Juni 2023). Die vorbereitenden organisatorischen Maßnahmen im Rahmen der Rolloutplanung erfolgen seit Anfang des Jahres 2023 in den ersten Behörden. Der erste Go-live im Rahmen des flächendeckenden Rollouts ist für Ende Oktober 2023 avisiert. Bis zum Jahr 2026 sollen rund 25.000 potenzielle Büroarbeitsplätze sowie weitere 15.000 Arbeitsplätze, für die eine E-Akte-Nutzung im Rahmen von Fachanwendungen in Betracht kommt, mit dem neuen DMS ausgestattet werden.

Verantwortlichkeit

HMdIS

HMdIS – Abteilung VII – Referat VII 10

5.1.12 Cybersicherheit Elektronische Personalakte (ePA)

Hauptnutzen der ePA für die Landesverwaltung besteht in der Standardisierung digitaler personalverwaltender Prozesse, Vermeidung von Medienbrüchen sowie einer modernen Archivierung mit einhergehender Auflösung bestehender Papieraktenarchive.

Ziel des Projekts ist die Pilotierung und Einführung der elektronischen Personalakte im HMdIS auf der Basis des Landesreferenzmodells Personalwesen (SAP-Lösung) unter Einbeziehung der Versorgungsakten sowie der Bezügeakten im Regierungspräsidium Kassel. In einem ersten Schritt werden drei Piloten im Innenressort ausgestattet, im Anschluss ist die landesweite Einführung geplant.

Bedeutung

Die Digitalisierung der Personaladministration setzt die Verarbeitung der Personalaktendaten, also sensibler Daten der Beschäftigten in der Landesverwaltung, voraus. Eine profunde Betrachtung und Umsetzung der Anforderungen im Bereich Cyber- und IT-Sicherheit sind auch in Ansehung des Schutzbedarfs der Personalaktendaten unerlässlich.

Gegenwart

Das Projekt räumt den Interessen und Anforderungen der Cyber- und IT-Sicherheit über alle Projektphasen hinweg hohe Bedeutung ein. In der aktuellen Teststellungsphase wurde ein Schwerpunkt im Bereich Datenschutz und IT-Sicherheit gesetzt. Grundlegende Datenschutz- sowie IT-Sicherheitskonzepte werden in die Bearbeitung aufgenommen. Die Gesamtprojektleitung (GPL) stellt sicher, dass diese bis zu einem Produktionsübergang (Pilotphase) vorliegen.

Schwerpunkt / Zielsetzung

Die IT-Sicherheit wird durch die GPL in enger Zusammenarbeit mit dem zentralen Landesdienstleister (HZD) berücksichtigt und umgesetzt. Ein weiterer Schutz wird durch ein zentrales Berechtigungsrahmenkonzept abgebildet. Zudem ist die Einbindung ressorteigener Kompetenzen zum zentralen Informationssicherheitsmanagement geplant.

Die Durchführung eines PEN-Tests wird vor einer Inbetriebnahme in den Pilotdienststellen erfolgen. Das IT-Architekturkonzept wird die Grundsätze security by design bzw. security by default berücksichtigen.

Verantwortlichkeit

HMdIS

HMdIS – Abteilung VII – Referat VII 11

HZD

5.1.13 Ganzheitliche Lagebilderstellung

Bedeutung

Lagebilder ermöglichen es, Entscheidungsträgerinnen und Entscheidungsträgern aktuelle Phänomene zu erfassen, Entwicklungen zu verfolgen und mögliche zukünftige Entwicklungen daraus abzuleiten. Ein Lagebild, welches Informationen unterschiedlicher Quellen bündelt, ermöglicht ein besonders umfassendes Gesamtbild. Damit können Gefahrenabwehrbehörden Bedrohungen für die Cybersicherheit frühzeitig identifizieren, bewerten und mit entsprechenden Maßnahmen reagieren. Neben der operativen Befassung dienen ganzheitliche Lagebilder als Grundlage für strategische Entscheidungen.

Die Cybersicherheitslage auf Landesebene ist mit der weltweiten Entwicklung zu vergleichen, um aussagekräftige operative Informationen zu gewinnen und so mögliche Angriffsvektoren, Zielgruppen und Eintrittswahrscheinlichkeiten sowie Auswirkungen identifizieren zu können.

Gegenwart

Das Hessen3C stellt anlassbezogen operative Lageberichte für unterschiedliche Zielgruppen in Hessen zur Verfügung. Diese umfassen neben selbst gewonnenen Erkenntnissen Informationen aus der Zusammenarbeit mit den Behörden und Einrichtungen anderer Länder. Zudem werden auf technischer Ebene Informationen gesammelt, Indikatoren aktueller Bedrohungen aufbereitet und zusammen mit Empfehlungen für präventive Maßnahmen bereitgestellt.

Hessen3C beteiligt sich zudem an dem Forschungsprojekt CYWARN der Technischen Universität Darmstadt, der Universität Duisburg und des IT-Beratungsunternehmens Virtimo AG zur Entwicklung von Strategien und Technologien zur Analyse und Kommunikation der Sicherheitslage im Cyberraum. Das Projekt verfolgt das Ziel, CERTs bei der Erfassung, Analyse und Kommunikation des Cyberlagebilds zu unterstützen. Dabei entsteht ein Demonstrator, der die automatisierte Sammlung öffentlicher und geschlossener Datenquellen sowie eine Datenauswertung mit Glaubwürdigkeitsanalyse und Informationspriorisierung ermöglicht. Durch den hohen Grad an Automatisierung werden die Teams dazu befähigt, Cyberbedrohungen effizienter zu erkennen, zu analysieren und zu kommunizieren. Die Ergebnisse fließen in Handlungsempfehlungen, Sensibilisierungsmaßnahmen, Lageberichte und Warnmeldungen ein, die für die zielgruppengerechte Kommunikation mit der Bevölkerung,

Behörden oder KRITIS-Betreibern verwendet werden. Akzeptanz und Anwenderfreundlichkeit werden bei der Entwicklung ebenso berücksichtigt wie ethische, rechtliche und soziale Rahmenbedingungen.

Schwerpunkt / Zielsetzung

Informationen sind die Grundlage von Entscheidungen zur Erhöhung des Cybersicherheitsniveaus. Hessen strebt die automatisierte Erfassung sowie Bündelung aller Informationen zur Cybersicherheit, unter Einbindung relevanter Partner aus dem Cybersicherheitsnetzwerk, in einem behördenübergreifenden hessischen Cyber- und IT-Sicherheitslagebild an.

Für die verbesserte Informationsgewinnung, den erforderlichen Austausch zwischen Bund und Ländern und dessen Verstetigung, werden, wo notwendig, weitere Anpassungen der rechtlichen Rahmenbedingungen vorgenommen.

Verantwortlichkeit

HMdIS – Abteilung VII – Referat VII 12 (Hessen3C)
Landesamt für Verfassungsschutz Hessen
HMdIS – Landespolizeipräsidium

5.1.14 Sicherheit durch Verschlüsselung

Bedeutung

Verschlüsselungstechnologien sind ein wesentlicher Eckpfeiler der Informationssicherheit, der in dem Moment seine Wirkung entfaltet, in dem alle anderen Sicherungsmaßnahmen scheitern. E-Mails, Dateien und Netzwerkkommunikation sind für Personen, die unbefugt auf diese zugreifen, wertlos, wenn eine Entschlüsselung der Daten nicht möglich ist.

Gegenwart

In der hessischen Verwaltung ist der HessenPC das Hauptarbeitsmittel. Aus Sicherheitsgründen ist die Festplatte des HessenPCs verschlüsselt. So kann bei einem Diebstahl zwar die Hardware entwendet werden, die Sicherheit der Daten bleibt jedoch gewahrt, da diese im Regelfall nicht entschlüsselt werden können.

Darüber hinaus bietet das Land Hessen Nutzerinnen und Nutzern die Möglichkeit, E-Mails per Public-Key-Infrastructure (PKI) zu verschlüsseln.

In Reaktion auf die Covid-19-Pandemie und dem damit einhergehenden gesteigerten Bedarf an mobilen Arbeitsplätzen kommen VPN-Zugänge mit sicherer TLS-Verschlüsselung zum Einsatz. Auch bei mobilen Endgeräten werden in Hessen aktuelle Verschlüsselungsmethoden eingesetzt.

Schwerpunkt / Zielsetzung

Der Schutz der in der Landesverwaltung verarbeiteten Daten und Informationen von Bürgerinnen und Bürgern ist für die Landesregierung von höchster Bedeutung. Mit der flächendeckenden Erweiterung von PKI-Verschlüsselung wird dieser Schutz weiter intensiviert und auch zukünftig werden die eingesetzten Verschlüsselungstechnologien und -standards an aktuelle technologische Entwicklungen angepasst.

Verantwortlichkeit

HZD

Wirtschaft und KRITIS

5.2 Wirtschaft und KRITIS

Cyberkriminelle greifen nicht nur die Verwaltung an, sondern ebenso hessische Wirtschaftsunternehmen und die für das Gemeinwesen besonders bedeutsamen Betreiber kritischer Infrastrukturen. Die Cyber- und IT-Sicherheit und der Schutz von Einrichtungen zur Versorgung richtet sich nach den Kriterien aus der Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz. Neben der Etablierung von Sicherheitsstandards durch die Unternehmen selbst, unterstützt das Land Hessen die hiesigen KRITIS-Betreiber durch die Zusammenarbeit mit verantwortlichen Bundeseinrichtungen. Der Blick der Hessischen Landesregierung richtet sich insbesondere auch auf die kleinen und mittleren Unternehmen (KMU). Mit ihrer Wirtschaftsleistung schultern sie die für das Gemeinwohl in Hessen elementaren Wertschöpfungsketten. Alle KMU sind daher wesentliche Akteure in der Gemeinschaft der Wirtschaftsunternehmen und KRITIS-Betreiber, deren Resilienz gegen Cyberangriffe in der strategischen Ausrichtung der hessischen Cybersicherheit besonders bedeutsam ist.

5.2.1 Schutz der Wirtschaft vor Spionage und Sabotage

Bedeutung

Wirtschaftsunternehmen entwickeln Ideen, innovative Techniken, Produkte und Problemlösungen, an denen ausländische Nachrichtendienste oder konkurrierende Unternehmen interessiert sind. Deshalb dient der Wirtschaftsschutz dazu, für entsprechende Gefahren zu sensibilisieren und diese abzuwehren.

Ziel des Wirtschaftsschutzes ist es, durch Aufklärung von u. a. Unternehmen, Forschungseinrichtungen und Verbänden zu einer nachhaltigen Festigung eines angemessenen Sicherheitsbewusstseins beizutragen sowie mit KMU und KRITIS-Betreibern in Hessen eine vertrauensvolle Zusammenarbeit zu pflegen.

Gegenwart

Das Landesamt für Verfassungsschutz Hessen (LfV Hessen) erstellt in den Bereichen Wirtschaftsschutz, Spionageabwehr und Cyberspionage zahlreiche Informationen und Handlungsempfehlungen, um gefährdete Unternehmen für entsprechende Gefahren zu sen-

sibilisieren und bei der Abwehr zu unterstützen. Das LfV Hessen steht bei der Einführung von individuellen Sicherheitskonzepten beratend zur Seite. Es informiert vertraulich sowie praxisgerecht und hilft bei der Klärung von Spionageverdachtsfällen.

Vorträge und Präventionsveranstaltungen zu ausgewählten Themen des Wirtschaftsschutzes sowie die Aufklärung über bestehende Risiken und Gefahren sind die wichtigsten Maßnahmen gegen Wirtschaftsspionage. Sie tragen wesentlich zur Risikominimierung bei der Ausspähung sensibler Informationen bei.

Perspektiven aus der Zusammenarbeit mit Verbänden, Kammern, Arbeitskreisen und Institutionen sowie Sicherheitspartnerschaften fließen in die Unterstützungs- und Beratungsangebote des LfV Hessen ein. Das LfV Hessen nimmt zusammen mit Vertreterinnen und Vertretern der hessischen Polizei an wöchentlichen Lagebesprechungen des Hessen3C teil, um aktuelle Erkenntnisse und Entwicklungen auszutauschen und präventive Maßnahmen im Zuge des Wirtschaftsschutzes abzustimmen. Das Hessen3C liefert wöchentlich neue Erkenntnisse und technische Indikatoren zu relevanten Akteuren und Bedrohungen an das LfV Hessen. Diese werden entweder selbst oder aus dem Kooperationsnetzwerk des Hessen3C und der Teilnahme am Nationalen Cyber-Abwehrzentrum in Bonn (Cyber-AZ) gewonnen.

Schwerpunkt / Zielsetzung

Die Wirtschaft ist eine der tragenden Säulen in Hessen. Um diese auch weiterhin vor der Ausspähung von Daten zu schützen, verfolgt die Landesregierung das Ziel, den Austausch der handelnden Akteure zu intensivieren und entsprechende Präventionsangebote durch die Fachdienststellen auszubauen.

Aufgrund der steigenden Bedrohungslage sieht die Landesregierung insbesondere im Bereich von Schlüsseltechnologien und besonders gefährdeten Branchen einen Schwerpunkt neu aufzusetzender Präventionsmaßnahmen und Beratungsangebote.

Verantwortlichkeit

Landesamt für Verfassungsschutz Hessen
HMdIS – Abteilung VII – Referat VII 12 (Hessen3C)

5.2.2 Erhöhung der Resilienz gegen Cyberangriffe

Bedeutung

Kleine und mittlere Unternehmen (KMU) stellen zahlenmäßig die größte Angriffsfläche im Bereich der Wirtschaft dar. Angesichts immer komplexer werdender IT-Infrastrukturen stehen KMU vor der Herausforderung, sich wirksam gegen Cyberangriffe zu schützen. Die Erhöhung digitaler Resilienz ist ein Kernanliegen der Landesregierung – je mehr digitale Infrastrukturen das Rückgrat von Wirtschaft und Gesellschaft bilden, umso mehr muss ihre Widerstandsfähigkeit gestärkt werden.

Informations- und Kommunikationstechnologien (IKT) tragen zunehmend zur Wertschöpfung von Unternehmen bei, woraus sich eine enorme Abhängigkeit von funktionierenden und zuverlässigen Systemen ergibt. Daher sollten präventiv die notwendige IKT-Infrastruktur, erforderliche Rahmenbedingungen sowie personelle Ressourcen geschaffen werden, die es Unternehmen ermöglichen, Betriebsstörungen jeglichen Ausmaßes bis hin zu Krisen- und Katastrophenfällen schnellstmöglich zu bewältigen und zum Regelbetrieb zurückzukehren. Resilienz ist somit eine Fähigkeit, die in der Risikobewertung Wettbewerbsvorteile sichern kann.

Gegenwart

Hessen3C unterstützt KMU durch kostenlose Präventions- und Awareness-Veranstaltungen sowie durch konkrete Beratung zum Thema Cybersicherheit. Hierzu werden reichweitenstarke Netzwerkpartner und Multiplikatoren wie z. B. Industrie- und Handelskammern oder der TÜV Hessen einbezogen.

Eine besondere Bedeutung nehmen Veranstaltungsreihen mit branchenspezifischer Ausrichtung ein. Inhaltlich an aktuellen Kriminalitätsphänomenen orientiert, werden thematische Schwerpunkte zur Sensibilisierung und Erhöhung der allgemeinen Resilienz gesetzt. So wurden im Rahmen der Covid-19-Pandemie insbesondere in essenziellen Bereichen des Gesundheitswesens Veranstaltungen durchgeführt.

Das LOEWE-Zentrum (Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz, eine Förderrichtlinie des HMWK) erarbeitet im Rahmen des Forschungsprojekts „emergenCITY“ („Resiliente Digitale Stadt“) Lösungen, die in Krisenfällen den Notbetrieb für und mit Informations- und Kommunikationstechnologien sicherstellen. Durch schnelle Hilfe soll eine effiziente Rückkehr zur Normalität unterstützen werden.

Darüber hinaus beinhaltet auch das ATHENE Forschungszentrum einen Forschungsbereich Secure Urban Infrastructures (SecUrban), dessen Hauptziel ist, sichere und zuverlässige Informations- und Kommunikationsinfrastrukturen für kritische Infrastrukturen bereitzustellen. Hierbei dient die Digitalstadt Darmstadt als empirisches Beispiel. KMU erhalten im Rahmen einer geförderten Digitalisierungsberatung der RKW Hessen GmbH Unterstützung bei der Digitalisierung ihrer Unternehmen. Schwerpunkte der Beratung können dabei neben Themen wie der Digitalisierung von Geschäftsprozessen, Dienstleistungen und Produkten auch die Datensicherheit sein. Die Beratungsinhalte werden dabei immer ganz individuell auf das jeweilige Unternehmen abgestimmt.

Speziell abgestimmt auf das Handwerk bieten die hessischen Handwerkskammern den Handwerksbetrieben kostenfreie Digitalisierungsberatungen an.

Bei der Umsetzung von Digitalisierungsvorhaben unterstützt das Förderprogramm DIGI-Zuschuss hessische KMU bei der Einführung neuer digitaler Systeme der Informations- und Kommunikationstechnik (IKT) und der Verbesserung der IKT-Sicherheit mit einem Zuschuss von bis zu 10.000 Euro. Mehr als ein Drittel der geförderten Unternehmen nutzt den DIGI-Zuschuss gezielt für Investitionen in ihre IT-Sicherheit.

Schwerpunkt / Zielsetzung

Über 99 Prozent der hessischen Unternehmen gehören dem Mittelstand an und sind das Rückgrat der hessischen Wirtschaft. Die Landesregierung weiß um die wichtige Rolle der KMU im Wirtschaftskreislauf und verfolgt das Ziel, mit dem Ausbau der Beratungsleistung sowie der Kooperations- und Multiplikatorennetzwerke die Resilienz der Unternehmen zu stärken.

Verantwortlichkeit

HMWEVW
HMinD
HMdIS – Abteilung VII – Referat VII 12 (Hessen3C)

5.2.3 Schutz kritischer Infrastrukturen

Bedeutung

Kritische Infrastrukturen wie beispielsweise Strom- und Telekommunikationsnetze, Klinikverbünde oder Finanzsysteme sind für das Funktionieren des privaten, wirtschaftlichen und öffentlichen Lebens unerlässlich. Sie sind zunehmend von einer störungsfreien und verlässlichen IT-Infrastruktur abhängig. Eine Störung oder ein Ausfall durch einen IT-Sicherheitsvorfall kann zu erheblichen Versorgungsengpässen oder existenziellen Beeinträchtigungen der öffentlichen Sicherheit und Ordnung führen. Auch hier gilt es, die digitale Resilienz zu erhöhen.

Gegenwart

Derzeit existieren Festlegungen für KRITIS-Betreiber nur seitens des Bundes durch das IT-SiG 2.0 sowie weitere Fachgesetze wie z. B. dem EnWG. Darin sind sowohl Verpflichtungen als auch Handlungsempfehlungen für die Betreiber enthalten, welche durch Bundesgesetzgebung definiert ist.

Hessen übernimmt die Verantwortung für die Koordination und Weitergabe von Informationen für regional ansässige Unternehmen, die von der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz nicht abgedeckt sind, aber dennoch für das Land und eine Region kritische Versorgungsleistungen erbringen.

Das Hessen3C führt in enger Zusammenarbeit mit der Koordinierungsstelle KRITIS in Hessen Sensibilisierungs- und Awarenessveranstaltungen durch. So ist die Umsetzung von IT-Sicherheit als ein elementarer Baustein zum physischen Schutz versorgungskritischer Einrichtungen zu verstehen. Die Koordinierungsstelle KRITIS (KoSt KRITIS) koordiniert unter Wahrung der fachlichen Zuständigkeiten die ressortübergreifende Zusammenarbeit, leitet eingehende Informationen weiter, vermittelt Kontakte und vernetzt Aktivitäten auf Landesebene.

Darüber hinaus ist Hessen mit zwei Vertreterinnen und Vertretern aus den Bereichen KRITIS und Cybersicherheit im Umsetzungsplan-KRITIS (UP-KRITIS), eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen, vertreten. Hessen bringt somit wertvolle Einblicke und Impulse aus den Bereichen des physischen Schutzes und der Cybersicherheit ein. Dies ermöglicht eine holistische Herangehensweise im Sinne des All-Gefahren-Ansatzes.

Schwerpunkt / Zielsetzung

Unternehmen der kritischen Infrastrukturen sind zentrale Elemente des privaten, wirtschaftlichen und öffentlichen Lebens, die es in besonderer Weise zu schützen gilt. Die Hessische Landesregierung macht es sich zur Aufgabe, für Unternehmen, die aus Landessicht kritische Versorgungsleistung erbringen, eigene Richtwerte zu formulieren.

Als Mitglied im UP-KRITIS wird sich Hessen dafür einsetzen, dass die Interessen der hessischen Unternehmen dort vertreten werden. Die Hessische Landesregierung setzt sich weiter dafür ein, dass hessische Unternehmen an diesem Gremium in ausreichender Anzahl teilnehmen können.

Bestehende zielgruppenspezifische Veranstaltungen zur Steigerung der Cyber- und IT-Sicherheit für KRITIS Unternehmen sollen zukünftig weiter ausgebaut und vermehrt in Präsenz- und Onlineformaten angeboten werden.

Die Landesregierung ist bestrebt, die physische Sicherheit mit Cyber- und IT-Sicherheit stärker zu vernetzen. Die besonderen Risiken und Bedarfe von KRITIS Unternehmen sollen den Beschäftigten der jeweiligen Fachaufsichten in der öffentlichen Verwaltung im Rahmen von verpflichtenden Fortbildungsmaßnahmen zu den Abhängigkeiten zwischen physischer und Cyber- und IT-Sicherheit vermittelt werden.

Verantwortlichkeit

HMdIS – Abteilung VII – Referat VII 12 (Hessen3C)
HMdIS – Abteilung V - Koordinierungsstelle KRITIS

5.2.4 Cybersicherheit im Gesundheitswesen

Bedeutung

Der Wohlstand einer Gesellschaft bemisst sich unter anderem an der Funktionsfähigkeit des Gesundheitswesens und an der Sicherstellung einer flächendeckenden und zuverlässigen medizinisch und pflegerischen Versorgung. Auch hier schreitet die Digitalisierung immer weiter voran und eröffnet die Möglichkeit, die Gesundheitsversorgung noch wirksamer und effizienter zu gestalten. Die Erfahrung der Vergangenheit zeigt, dass aber auch Risiken damit einhergehen. Cyberangriffe auf Einrichtungen des Gesundheitswesens können verheerende Folgen haben: Vom Ausfall der Homepage bis hin zur vollständigen Lahmlegung der Gesundheitseinrichtung ist alles möglich. Im schlimmsten Fall sogar mit tödlichem Ausgang. Zudem sind regelmäßig Daten – sowohl von Mitarbeiterinnen und Mitarbeitern als auch von Patientinnen und Patienten – aus dem höchstpersönlichen Lebensbereich betroffen.

Die Steigerung der Resilienz vor Cyberangriffen im Gesundheitswesen ist elementare Grundlage für die Sicherheit aller.

Neben dem Bereich Versorgung im Gesundheitswesen ist auch der Öffentliche Gesundheitsdienst (ÖGD) mit seinen Behörden (einschl. HMSI) und Akteuren besonders vor Angriffen zu schützen. Im ÖGD werden z. B. besonders schützenswerte Daten der Gesundheitsberichterstattung oder Daten aus der Krebsregistrierung verarbeitet, gebündelt und gespeichert; zudem sind einige Prozesse und Verfahren besonders schützenswert und sollten vor Angriffen unbedingt sicher sein.

Gegenwart

In einer immer stärker vernetzten Welt spielt Cybersicherheit auch in der Pharma- und Biotech-Branche (insbesondere in der Produktion) sowie auf Ebene der Distribution (Apotheken und pharmazeutischer Großhandel) eine wachsende Rolle. Digitalisierung und Automatisierung sind sehr weit vorangeschritten.

2017 hat der Gesetzgeber die Arzneimittelversorgung zur kritischen Infrastruktur erklärt und damit Teile der Pharmaindustrie hineingenommen. Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) bestimmt, dass Betreiber kritischer Infrastrukturen ihre kritischen IT-Systeme, IT-Komponenten und IT-Prozesse durch angemessene Vorkehrungen nach dem Stand der Technik gegen Störungen der Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität schützen müssen.

Darüber hinaus fördert Hessen mit der Förderrichtlinie „Digitalisierung in der ambulanten medizinischen und pflegerischen Versorgung“ (DIGI-Ambulant) bereits heute besonders Maßnahmen zum Datenschutz und zur Datensicherheit für eine zukunftsfähige Versorgung der Patientinnen und Patienten.

Mit dem Kompetenzzentrum für Telemedizin (KTE) berät, vernetzt und unterstützt das Land Hessen Ärztinnen und Ärzte dabei, Abläufe und Anwendungen zu digitalisieren.

Im Rahmen der Rechtsaufsicht über landesunmittelbare Sozialversicherungsträger und andere Institutionen im Gesundheitswesen (z. B. Gesetzliche Krankenkassen, Kassen(zahn) ärztliche Vereinigungen) prüft das HMSI regelmäßig auch datenschutz- und sicherheitsrelevante Aspekte, wo diese der Rechtsaufsicht anzuzeigen oder von dieser zu genehmigen sind, etwa bei der Beschaffung von IT-Systemen gemäß § 85 Abs. 3a SGB V, bei der Auftragsdatenverarbeitung nach § 80 SGB X oder bei der Genehmigung von Sozialdatenübermittlungen für Forschungsvorhaben nach § 75 SGB X.

Das Thema Patientensicherheit ist in Hessen seit vielen Jahren präsent und genießt einen hohen Stellenwert. Dies drückt sich unter anderem in der seit 2019 für die hessischen Krankenhäuser geltenden Patientensicherheitsverordnung aus. Diese sieht u. a. die Etablierung des Landesbeirates Patientensicherheit vor. Zudem mussten alle hessischen Krankenhäuser einen Patientensicherheitsbeauftragten bestellen. Im Weiteren ist Hessen Mitglied im Aktionsbündnis Patientensicherheit (APS). Es gilt, dass Patientensicherheit nicht ohne Cybersicherheit gedacht werden kann. Vor diesem Hintergrund hat das APS die Handlungsempfehlung „Digitalisierung und Patientensicherheit – Risikomanagement in der Patientenversorgung“ verabschiedet. Diese wendet sich an Angehörige aller Berufsgruppen und Fachdisziplinen, die in der Gesundheitsversorgung tätig sind. Hessen unterstützt die Beachtung dieser Handlungsempfehlung.

Hessen3C berät bei der Umsetzung von Maßnahmen zur Erhöhung der IT- und Cybersicherheit in Krankenhäusern und unterstützt mit konkret auf die Bedarfe von Krankenhäusern abgestimmten Informationsveranstaltungen.

Schwerpunkt / Zielsetzung

Das Gesundheitswesen ist ein wichtiger Gradmesser für das Wohlbefinden in Hessen. Cybersecurity und Datensicherheit können dabei die Schaffung von Rahmenbedingungen unterstützen, die erlauben und ermöglichen, dass Gesundheitsdaten (anonym unter Achtung

etwaiger Persönlichkeitsrechte) erfasst, verarbeitet und zur wissenschaftlichen Auswertung bereitgestellt werden. Der Landesbeirat Patientensicherheit kann sich bei entsprechender Notwendigkeit mit dem Thema Cybersicherheit in Bezug auf Patientensicherheitsthemen befassen. Hierzu kann der Landesbeirat bei entsprechendem Bedarf eine Arbeitsgemeinschaft gründen. Auch die Arbeit des neugegründeten Netzwerks der Patientensicherheitsbeauftragten bietet eine Plattform, um das Thema Cybersicherheit an der Basis aufzugreifen.

Verantwortlichkeit

HMSI

5.2.5 Finanzplatz Hessen

Bedeutung

In Hessen sind mit der Wertpapierbörse FWB und der Derivatebörse Eurex zwei der bedeutsamsten Handelsplätze Europas ansässig. Der Handel vollzieht sich größtenteils elektronisch über das T-7-Handelssystem der Gruppe Deutsche Börse. Dem Thema Cybersicherheit kommt in diesem Zusammenhang eine herausragende Bedeutung zu. Die Sicherstellung der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und deren Verarbeitung ist im vitalen Interesse der Börsen, Handelsteilnehmer und deren Kunden sowie Emittenten. Für den Finanzplatz Hessen sowie die Stabilität des Finanz- und Wirtschaftssystems im Allgemeinen ist eine resiliente Cyberabwehr ebenfalls von erheblicher Bedeutung.

Gegenwart

Nach der „threat landscape" der Europäischen Zentralbank (EZB) für Finanzmarktinfrastruktur ist die Gefahr von Cyberangriffen seit März 2022 als hoch einzustufen. Es ist damit zu rechnen, dass unter anderem staatliche Akteure Finanzmarktinfrastrukturen wie z. B. Handelsplätze attackieren und bestehende Schwachstellen ausnutzen.

Die Hessische Börsenaufsicht stellt im Rahmen ihrer Zuständigkeit nach § 3 Abs. 1 BörsG durch eine laufende Überwachung und anlassbezogene Prüfungen sicher, dass die Börsenträgergesellschaften ihre gesetzlichen Verpflichtungen mit Cybersicherheitsbezug erfüllen (vgl. insbesondere § 5 Abs. 4 Nr. 2, 3 und Abs. 4a BörsG). Bei Verstößen und Missständen trifft sie die notwendigen Maßnahmen zur Abhilfe und ggf. Sanktionierung.

Seit dem 01.01.2022 sind Betreiber von Handelsplätzen wie FWB und Eurex und der Freiverkehr als Kritische Infrastrukturen gemäß Anhang 6 Teil 1 Nr. 1.21 BSI-KritisV anzusehen. Hieraus folgt die Verpflichtung zur Registrierung beim BSI (§ 8b Abs. 3 BSIG) sowie die Pflicht, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen zu treffen (§ 8a Abs. 1 BSIG). Ferner trifft sie die Pflicht zur unverzüglichen Meldung von IT-Störungen an das BSI (§ 8b Abs. 4 BSIG).

Die Gruppe Deutsche Börse führt zur Verbesserung ihrer Cyberresilienz auf freiwilliger Basis ethische Penetrationstests durch, bei denen Angriffe durch Hacker simuliert werden. Diese Attacken dienen dem Ziel, bestehende Schwachstellen zu identifizieren und zu beheben.

Schwerpunkt- und Zielsetzung

Perspektivisch werden die Handelsplätze zusätzliche gesetzliche Pflichten im Bereich der Cybersicherheit erfüllen müssen. Beispielsweise müssen Handelsplätze ab dem 01.05.2023 Systeme zur Angriffserkennung einsetzen (§ 8a Abs. 1a BSIG). Alle zwei Jahre werden Erfüllungsnachweise durch Audits, Prüfungen oder Zertifizierungen verlangt (§ 8a Abs. 3 BSIG). Zukünftig soll Cyberangriffen auch auf EU-Ebene durch die am 16.01.2023 in Kraft getretene Verordnung über digitale Betriebsstabilität (DORA) begegnet werden. Der europäische Finanzsektor soll in die Lage versetzt werden, die Betriebsstabilität im Falle einer schwerwiegenden Störung aufrechtzuerhalten. Die Hessische Börsenaufsicht wird die Einhaltung neuer gesetzlicher Pflichten mit Bezug zur Cybersicherheit durch die Handelsplätze sicherstellen, soweit sie hierfür zuständig ist.

Die Gruppe Deutsche Börse hat gegenüber der Hessischen Börsenaufsicht in Aussicht gestellt, auch zukünftig an freiwilligen Penetrationstests teilnehmen zu wollen und deren Umfang zu erweitern. Die Hessische Börsenaufsicht wird die Behebung von Schwachstellen, die im Rahmen der Tests offenbar werden, begleiten.

Verantwortlichkeit

HMWEVW

5.2.6 Schutz kritischer Weltrauminfrastrukturen

Bedeutung

Neben terrestrischen Infrastrukturen spielen auch Weltrauminfrastrukturen eine zentrale Rolle für Kommunikation und Sicherheit unserer Bürgerinnen und Bürger.

Zahlreiche Anwendungen und Dienste auf der Erde sind nur mittels Weltrauminfrastrukturen realisierbar. Hierzu gehören insbesondere Navigation, Erdbeobachtung, Kommunikation und ein global verfügbares Internet-of-things (IoT) bzw. Internet aus dem Weltraum. Die wachsende gesamtstaatliche Abhängigkeit von Weltrauminfrastrukturen wie Satelliten verdeutlicht zudem ihre Bedeutung für zahlreiche kritische terrestrische Infrastrukturen. So stellen die Dienste des Navigationssystems Galileo eine essentielle Voraussetzung für die Sicherheit des Flugverkehrs, für die Synchronisation von Stromnetzen oder für zuverlässige Finanztransaktionen durch hochpräzise Zeit- und Ortsangaben dar. Erdbeobachtungssatelliten wie die Sentinels des europäischen Erdbeobachtungssystems COPERNICUS liefern wichtige Daten u. a. für präventives und reaktives Krisenmanagement im Zusammenhang mit Naturkatastrophen; Wettersatelliten sichern die Versorgung mit Wetterdaten zur Wettervorhersage und zur Klimamodellierung; Kommunikationssatelliten ermöglichen Rundfunkübertragungen, Internetzugang und Datentransfer. Zudem liefern Satelliten unerlässliche Daten und Dienste für militärische Aufklärung und Operationen.

Weltrauminfrastrukturen müssen nicht nur gegen kosmische oder technische Bedrohungen wie kosmische Strahlung, Weltraumwetter oder Weltraumschrott geschützt werden, um die Verfügbarkeit, Integrität und Authentizität ihrer Dienste sicherzustellen, sondern auch zunehmend gegen Cyberangriffe.

Die große aktuelle Relevanz zeigte sich z. B. am 24. Februar 2022, als der US-amerikanische Betreiber des KA-SAT-Netzwerks, die Firma Viasat, eine Stunde vor dem Überfall Russlands auf die Ukraine einen mutmaßlich von Russland ausgehenden Cyberangriff feststellte. Diese denial-of-service-Attacke führte zu einer teilweisen Unterbrechung des kommerziellen Satelliten-Breitbanddienstes von KA-SAT und verursachte Kommunikationsausfälle und -unterbrechungen bei zahlreichen Behörden, Unternehmen und Nutzern in der Ukraine und in ganz Europa.

Gegenwart

Raumfahrtstrategien der EU und des Bundes betonen die Notwendigkeit, Weltrauminfrastrukturen wirkungsvoll vor Cyberangriffen zu schützen. So bezeichnet die Cybersicherheitsstrategie für Deutschland vom September 2021 weltraumgestützte Infrastrukturen als „Rückgrat der Digitalisierung". Auch die im April 2022 durch die Hessische Landesregierung verabschiedete Hessische Raumfahrtstrategie „Hessen in Space" betont, dass bei der Nutzung von Raumfahrtdaten durch hessische Landesbehörden ein besonderes Augenmerk auf die Cyber- und IT-Sicherheit zu legen ist. Explizit heißt es hier: „Dabei kommt der Ausarbeitung und Einhaltung von Sicherheitsstandards und -konzepten eine herausragende Rolle zu. Wie bei der erdgebundenen Datenverarbeitung hat die hessische Landesverwaltung auch bei der Nutzung von Raumfahrtdaten eine besondere Verpflichtung, die Cyber- und IT-Sicherheit sowie die Unverletzlichkeit der gesicherten Informationen in den genutzten Systemen zu gewährleisten, um die Vertraulichkeit, Verfügbarkeit und Integrität von digital verarbeiteten und gespeicherten Informationen uneingeschränkt aufrecht zu erhalten."

Cybersicherheitsrelevante Aspekte und Sicherheitsanforderungen zum wirkungsvollen Schutz gegen Cyberangriffe und zur Sicherstellung der Integrität der Kommunikation Bodensegment – Satellit sind bereits bei der Entwicklung und dem Bau von Satelliten, Bodenstationen und anderen relevanten System-Komponenten implizit im Sinne des „Security-by-design"-Prinzips mitzudenken. Hier sind in erster Linie die Raumfahrtagenturen (ESA und DLR als deutsches Raumfahrtmanagement) gefragt, entsprechende Spezifikationen in ihre Ausschreibungen mitaufzunehmen, sowie zum anderen die Unternehmen, die Weltrauminfrastrukturen oder Teile von diesen entwickeln und bauen. Darüber hinaus muss die Sensibilisierung zu den Risiken von Cyberbedrohungen bei Bedarfsträgern, Entwicklern, Herstellern und Betreibern von weltraumgestützten Infrastrukturen aktiv gefördert werden.

Schwerpunkt / Zielsetzung

Die Landesregierung wird die stärkere Vernetzung der handelnden Akteure (Wissenschaft, Forschung, Wirtschaft, Behörden, internationale Organisationen) und Intensivierung der Zusammenarbeit mit den zuständigen hessischen Behörden fördern und die Weltrauminfrastrukturen als KRITIS aus Landessicht definieren

Der Schaffung eines öffentlichen und politischen Bewusstseins für sicherheitsrelevante Entwicklungen, Abhängigkeiten und Verwundbarkeiten von Weltrauminfrastrukturen sowie dem Einbringen von hessischen Vorschlägen und Bedarfen bei Rechtssetzungsvorhaben und politischen Initiativen auf Bundes- oder EU-Ebene kommt hierbei große Bedeutung zu.

Verantwortlichkeit

StK – Geschäftsstelle Raumfahrtkoordinator (K 10)
HMdIS – Abteilung VII – Referat VII 13
HMWEVW – Abteilung II – Referat II 4

5.2.7 Cybersicherheit im Luftverkehr

Bedeutung

An den hessischen Flughäfen werden verschiedene Produkte der Informationstechnik eingesetzt, um den Luftverkehr auf mehreren Ebenen (Versorgung, Security, Safety, Flugbetrieb) sicher zu gestalten und abzuwickeln. Ein Cyberangriff auf kritische Informations- und Kommunikationssysteme (KIKS) von Flughäfen kann zu massiven Störungen im Luftverkehr führen.

Die sicheren Lieferketten nach § 9a LuftSiG unterliegen in Hessen der Überwachung durch das Luftfahrtbundesamt.

Gegenwart

Der Flughafen Frankfurt am Main unterliegt den Regelungen aus der KRITIS-Verordnung und wird durch das BSI hinsichtlich der Versorgungssicherheit überwacht.

In Bezug auf Luftsicherheit bestehen für die Flughäfen Frankfurt am Main und Kassel-Calden Anforderungen aus Nr. 1.7 des Anhangs zur der DVO (EU) 2015/1998, die national in Anlage I zum Nationalen Luftsicherheitsprogramm – Grundsätze zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit in Bezug auf Cybersicherheitsmaßnahmen umgesetzt wurden. Die Schutzmaßnahmen richten sich nach BSI-IT-Grundschutz gemäß BSI-Standard 200-2 bzw. gleichwertiger internationaler Standards wie z. B. der ISO 2700X-Familie. Die Flughäfen sind aufgefordert worden, entsprechende Luftsicherheitsprogramme zu entwickeln und dem Hessischen Ministerium für Wirtschaft, Energie, Verkehr und Wohnen (HMWEVW) bzw. dem Regierungspräsidium Kassel zur Zulassung vorzulegen. Darüber hinaus sind die Luftsicherheitsbehörden verpflichtet, eigene Cybersicherheitsmaßnahmen durchzuführen, soweit sie KIKS beim Vollzug von Luftsicherheitsaufgaben betreiben.

Das BSI hat zur Unterstützung der Luftsicherheitsbehörden und der Flughäfen eine Projektgruppe Luftsicherheit eingerichtet. Die hessischen Flughäfen, das HMWEVW und das Regierungspräsidium Kassel sind als Kontaktstelle beim BSI gemeldet.

Cybersicherheitsmaßnahmen zu den flugplatzbetrieblichen Systemen unterliegen den Vorgaben nach VO (EU) 139/2014. Es bestehen bislang IT-spezifische Regelungen für das Management für Luftfahrtdaten und Luftfahrtinformationen sowie in Bezug auf ein Informationssicherheitsmanagementsystem. Eine Erweiterung der Vorgaben durch EU/EASA ist zu erwarten.

Schwerpunkt- und Zielsetzung

In Bezug auf die im Kontext der Luftsicherheit eingesetzten und identifizierten kritischen Informations- und Kommunikationssysteme soll zum 31.12.2024 der BSI-Standard Basisabsicherung erreicht werden.

Die Flughäfen werden weitere nationale und europäische Cybersecurity-Vorgaben in den Bereichen Versorgung, Security, Safety, Flugbetrieb erfüllen und ihre bisherigen Maßnahmen weiterentwickeln müssen. Die hessischen Luftfahrtbehörden werden die Einhaltung neuer gesetzlicher Pflichten mit Bezug zur Cybersicherheit im Luftverkehr durch die Flughäfen sicherstellen, soweit sie dafür zuständig sind.

Die effektive Umsetzung wird durch die hessischen Luftfahrtbehörden selbst sowie externe Stellen des Bundes und der EU-KOM regelmäßig auditiert. Die Behebung von festgestellten Schwachstellen wird von den zuständigen Behörden begleitet.

Verantwortlichkeit

HMWEVW

5.2.8 Cybersicherheit im Straßenverkehr

Bedeutung

In Hessen kreuzen sich nationale, kontinentale und globale Verkehrswege. Die Bedeutung Hessens als Logistikdrehscheibe ist unbestritten. Mit der Osterweiterung der EU ist Hessen ins geografische Zentrum Europas gerückt und bietet beste Voraussetzungen für einen kontinentalen Distributionsstandort. Ist Südhessen mit dem Frankfurter Flughafen auf die kontinentalen und globalen Verkehrsströme ausgerichtet, ist die nördliche Landeshälfte für die nationale Verteilung prädestiniert, denn von hier aus lässt sich jeder Ort Deutschlands über Nacht erreichen. Darum haben sich dort in den vergangenen Jahren zahlreiche Unternehmen mit ihren Umschlagzentren angesiedelt.

Hessen lebt also zu einem guten Teil vom Verkehr. Der Frankfurter Flughafen ist Deutschlands größte Arbeitsstätte, und in Nordhessen beschäftigt die Branche inzwischen mehr als jeden zehnten Arbeitnehmer – eine höhere Dichte an Logistikbeschäftigten gibt es bundesweit nicht. Hessen erbringt Verkehrs- und Logistikleistungen für Deutschland und Europa – auf der Straße, auf der Schiene, und in der Luft.

Mobilitätsunternehmen wie die Lufthansa, die Deutsche Bahn, Fraport, VW und Opel zählen zu den größten Arbeitgebern in Hessen.

Gegenwart

Die Digitalisierung verändert auch die Speditionswelt nachhaltig. In den vergangenen Jahren wurden zahlreiche Internetplattformen gegründet, deren Angebote Frachtenbörsen, Ausschreibungen, Transport Management und Supply Chain Visibility und erste digitale Speditionen als neue Marktteilnehmer, die sämtliche Prozesse des Speditionsgeschäfts von Grund auf digital abbilden wollen, umfasst. So diversifiziert die Speditions- und Logistikbranche durch ihr heterogenes Kunden- und Leistungsspektrum sowie ihre branchenspezifischen Besonderheiten ist, so individuell sind auch die Anforderungen an digitale Lösungen. Anders als in den business to client (B2C)-Märkten haben sich im Business to business (B2B)-dominierten Speditions- und Logistikumfeld mit seinen vielen unterschiedlichen Marktteilnehmern bislang keine dominierenden Plattformanbieter positionieren können. Auch die in der Logistik entstehenden Daten bleiben weithin verteilt, was „Big Data"-Analysen und -Anwendungen schwierig macht.

Der Einfluss der Plattformökonomie auf die Geschäftsmodelle etablierter Speditionen und auf ihre Digitalisierungsdynamik ist Thema bei den Verbänden. Die Zuständigkeit für das Thema Logistik liegt nicht bei den Ländern, sondern beim Bund. Unternehmen aus dem Speditions- und Transportbereich sind eigenständig für ihre Sicherheit im Bereich des Datenschutzes und bei Cyberangriffen verantwortlich.

Schwerpunkt- und Zielsetzung

Hessen ist einer der wichtigsten Verkehrsknotenpunkte in Deutschland und somit attraktiver Standort für viele Unternehmen. Hessen lebt zu einem beträchtlichen Teil vom Verkehr. Deshalb steht die Sicherung der Mobilität für die Landesregierung an vorderster Stelle. So setzt sich die Landesregierung schon heute und auch zukünftig dafür ein, dass Bedarfe an Cybersicherheit für die Speditions- und Logistikbranche in Bundesgesetzgebungsverfahren berücksichtigt werden.

Verantwortlichkeit

HMWEVW

5.2.9 Cybersicherheit in der Verkehrs-/Infrastruktur

Bedeutung

Das hohe Verkehrsaufkommen, die Erfordernisse der Intermodalität sowie der Klimaschutz machen den Einsatz von Verkehrsleitsystemen unerlässlich. Ein Verkehrsleitsystem ist ein elektronisches und kartengestütztes System für die Analyse, Regelung und Optimierung von Verkehrsströmen sowie der Gewährleistung der Verkehrssicherheit. Über Sensoren in, an oder über der Fahrbahn sowie aus Fahrzeugen (Floating Car Data) werden Daten über das aktuelle Verkehrsaufkommen erfasst. Dies bildet die Grundlage für die Steuerung des Verkehrsgeschehens etwa durch Geschwindigkeitsregelung, Tunnel- bzw. Fahrstreifensperrungen oder Schaltungen von Lichtsignalanlagen bzw. Zuflussregelungen.

Hessen Mobil betreibt mit der Tunnelleitzentrale Hessen (TLZ) ein solches System, zwei weitere Zentralen zur Verkehrsbeeinflussung – Verkehrsmanagement- (VMZ)- bzw. Lichtsignalanlagenzentrale Hessen (LZH) – sind in Planung. Weitere Verkehrsmanagementsysteme sind auf kommunaler Ebene in den großen Städten vorhanden. Zunehmend gewinnt die Vernetzung der Akteure im Verkehrssektor an Bedeutung. Der Austausch von Mobilitätsdaten erfolgt hier im Wesentlichen über die „Mobilithek", den Nationalen Zugangspunkt für Mobilitätsdaten gemäß IVS-Richtlinie (Richtlinie 2010/40/EU für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern).

Die Cybersicherheit ist für den Betrieb der Verkehrsleitsysteme bzw. Zentralen von Bedeutung, als dass die Funktionen der darin befindlichen Systeme und damit einhergehend die Sicherheit der Verkehrsteilnehmer/-innen gewährleistet sein muss.

Im Bereich der Dateninfrastruktur stellt der Internetknoten DE-CIX in Frankfurt mit mehr als 13 Terabit pro Sekunde Peak Traffic den weltweit führenden Internet Exchange dar.

Gegenwart

Die TLZ ist zur Gewährleistung der Cybersicherheit mit Sicherheitskonzepten gemäß den Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI) ausgestattet, die IT, die Sicherheitstechnik und die Bauwerke werden regelmäßig geprüft und gewartet. Die IT-Infrastruktur befindet sich darüber hinaus in einer autarken Netzwerkstruktur. Das Personal und alle weiteren Beteiligten werden regelmäßig geschult, zudem finden planmäßige Notfallübungen statt.

Der Internetknoten DE-CIX verknüpft aktuell lokale, regionale und globale Netzwerke und ermöglicht somit den wichtigsten Zugang zum weltweiten Internet. 80 % aller Netzwerke können darüber erreicht werden.

Schwerpunkt- und Zielsetzung

Die VMZ wird zukünftig zusammen mit der LZH sowie der TLZ bei Hessen Mobil und im engen Austausch mit vergleichbaren Einrichtungen auf Bundes- sowie Kommunalebene das zentrale Element im Bereich der intelligenten Verkehrssysteme (IVS) sein.

Bei den geplanten Leitsystemen (LZH, VMZ) werden im Zuge der Errichtung die Aspekte der Cybersicherheit von Beginn an durch die kontinuierliche Abstimmung zwischen Informationssicherheitsbeauftragten, IT-Dezernat und den herstellenden Unternehmen berücksichtigt. Für sämtliche Prozesse, IT-Systeme und Infrastrukturen werden Informationssicherheitskonzepte auf Basis der Informationssicherheitsleitlinie Hessen bzw. BSI-Grundschutz zur Absicherung erstellt und kontinuierlich fortgeschrieben.

Der DE-CIX ist ein Aushängeschild Hessens in die gesamte Welt, für das auch die Hessische Landesregierung eine besondere Verantwortung übernimmt und auch zukünftig notwendige Maßnahmen umsetzen wird.

Verantwortlichkeit

HMWEVW
HMdIS – Abteilung VII – Referat VII 12 (Hessen3C)
HMinD – Abteilung D – Referat D 1

Innovative Forschung und Entwicklung

5.3 Innovative Forschung und Entwicklung

Die Sicherheit der digitalen Welt von morgen liegt in der Hand der Wissenschaft von heute. Technologische Entwicklungen werden von Cyberkriminellen regelmäßig für neue, vielfältige und wandelbare Methoden des Cyberangriffs missbraucht. Um den Angriffsszenarien geeignete technische Sicherheitslösungen und Abwehrmechanismen entgegenstellen zu können, bedarf es optimaler Rahmenbedingungen für innovative Forschung zu Cybersicherheitstechnologien durch Hochschulen und außeruniversitäre Forschungseinrichtungen. Hessen profitiert bereits seit langem von seiner thematisch breit aufgestellten Forschungslandschaft zum Thema Cybersicherheit, deren Stabilität und Ausbau von der Hessischen Landesregierung zum Schutz des Ökosystems weiter forciert wird. Durch das Referat Innovationsmanagement Cybersicherheit im HMdIS werden vielfältige Forschungsbereiche mit den Bedarfen der hessischen Sicherheitsbehörden verknüpft.

5.3.1 Angewandte Forschung

Bedeutung

Cyberkriminelle entwickeln permanent neue Methoden für Cyberangriffe. In diesem Kontext stellt der Wettlauf um die Nutzbarmachung von technologischen Innovationen für die Sicherheit oder kriminelle Zwecke eine ständige Herausforderung dar. Um hier handlungsfähig zu bleiben, muss Cybersicherheit in einem vorausschauenden Prozess gewährleistet werden. Dazu ist es elementar, entlang neuer Forschungserkenntnisse innovative und langfristig funktionierende Schutzmechanismen zu schaffen. Aufgabe der angewandten Forschung ist es, durch aktuelle und spezifische Bedarfe der Praxis begründete Erkenntnisgewinne zu erzielen, die unmittelbar in der praktischen Umsetzung Berücksichtigung finden. Von besonderer Bedeutung sind für die Landesregierung insbesondere die Themen Open Source, sichere Künstliche Intelligenz, Quantencomputing, Internet of Things und Blockchain.

Gegenwart

Mit der „Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz“ (LOEWE) setzt das Land Hessen seit 2008 wissenschaftspolitische Impulse und stärkt damit die hessische Forschungslandschaft, auch im Bereich der Cybersicherheit, nachhaltig.

Das Referat Innovationsmanagement Cybersicherheit des HMdIS wirkt u. a. als Multiplikator zwischen Wissenschaft und Forschung im Bereich Cybersicherheit und den jeweiligen Bedarfsträgern des Innenressorts. Grundlage der Arbeit ist ein systematischer Innovationsprozess: von der anwendungsorientierten Forschung über das Ergebnis bis hin zur Veröffentlichung und Bereitstellung der Ergebnisse für hessische Bedarfsträger.

Zur Förderung von Forschungsprojekten zum Thema IT-Sicherheit existiert die Förderrichtlinie „Cybersicherheitsforschung in Hessen" des HMdIS. Über das Programm werden Forschungsergebnisse im Ökosystem aus Wissenschaft, Bedarfsträgern und strategischer Steuerung hochgradig anwendungsorientiert entwickelt, allgemein verfügbar und nutzbar gemacht. Um gleichzeitig kurzfristige Bedarfslagen zu bedienen, hat Hessen einen „Rahmenvertrag Cybersicherheitsforschung" mit dem Fraunhofer SIT abgeschlossen.

Die Forschungsvorhaben des Landes Hessen werden mit hessischen Hochschulen und Universitäten sowie außeruniversitären Forschungseinrichtungen umgesetzt. Besonders hervorzuheben ist das einzigartige und innovative Kooperationsmodell des Forschungszentrums ATHENE im Zusammenspiel des Fraunhofer SIT, Fraunhofer IGD, der TU Darmstadt sowie der Hochschule Darmstadt, gefördert durch den Bund und das Hessische Ministerium für Wissenschaft und Kunst. ATHENE betreibt Forschung im Bereich der angewandten Cybersicherheit. Das HMdIS steuert mit dem Referat „Innovationsmanagement Cybersicherheit" und dem Hessen3C die explizite Anwendungsorientierung der hessischen Cybersicherheitsforschung. Darüber hinaus richtete die Hessische Landesregierung jüngst das „Zentrum für Angewandtes Quantencomputing" (ZAQC) für die Förderung der Metadisziplin ein, um gemeinsam mit der Wirtschaft Projekte zur Quantentechnologie zu initialisieren. Dazu plant das federführende Fraunhofer-Institut für Graphische Datenverarbeitung (IGD) eine enge Kooperation mit dem Fraunhofer SIT und dem Forschungszentrum ATHENE, insbesondere um eine sichere wirtschaftliche Nutzung von Quantencomputern vorzubereiten (Security-by-Design).

Das ZAQC ist eine der Maßnahmen, die im Rahmen der Hessischen KI-Zukunftsagenda entwickelt werden. Diese Zukunftsagenda gibt „KI made in Hessen" einen strategischen Rahmen, bündelt bestehende Maßnahmen im Bereich KI in Hessen und stellt neue KI-Projekte vor. Sie greift damit eine Schlüsseltechnologie auf, die auch für Fragen der Cybersicherheit von grundlegender Bedeutung ist.

Darüber hinaus startete im Dezember 2019 das Förderprogramm Distr@l, welches mit sei-

nen vier Förderlinien ein Fördersystem darstellt und zielgruppenorientiert auf die Herausforderungen der digitalen Transformation in Wirtschaft und Gesellschaft reagiert und sich komplementär in die Förderlandschaft des Landes einfügt. Dieses breit angelegte Förderangebot mit dem Schwerpunkt auf digitale Innovationen in KMU ermöglicht es auch neue Lösungen und Projektideen im Kontext der Cybersicherheit zu gestalten und umzusetzen.

Zudem profitieren von den Forschungsergebnissen Kommunen und Unternehmen dank eines ebenso effizienten wie praxisorientierten Wissenstransfers. Hier spielt das House of Digital Transformation e. V. (HoDT) eine besondere Rolle. Es vernetzt als Teil der Hessischen Houses of Innovationsstrategie Wirtschaft, Wissenschaft und Politik und hat einen Arbeitsschwerpunkt im Bereich Resilienz und Cybersicherheit.

Schwerpunkt / Zielsetzung

Aktuelle Entwicklungen und technologische Innovationen im Bereich der Cybersicherheit müssen in zukünftige Veränderungsprozesse der Landesverwaltung fortlaufend integriert werden.

Um daran orientierte und langfristig funktionierende Schutzmechanismen zu gewährleisten, setzt die Landesregierung auf eine enge Verzahnung mit Forschungseinrichtungen und –vorhaben in Hessen. So sollen zukünftig insbesondere die Forschungsfelder zu KI-Verfahren und deren Einsatz zur Verbesserung der Cybersicherheit, dem Quantencomputing und zukunftsorientierten Verschlüsselungsverfahren stärker in den Fokus gerückt werden. Die Hessische Landesregierung legt besonderen Wert auf eine nachhaltige Cybersicherheit. Gewonnene Ergebnisse sollen daher in daran anknüpfenden Produktentwicklungen verstetigt werden und im Bereich der Aus- und Fortbildung Anwendung finden.

Verantwortlichkeit

HMinD

HMWK

HMdIS – Abteilung VII – Referat VII 4

5.3.2 Fachkräfte

Bedeutung

Eine Studie des Bitkom e. V. vom 03. Januar 2022 zeigte branchenübergreifend, dass die Zahl freier Stellen für IT-Fachkräfte 2021 in Deutschland im Vergleich zum Vorjahr um 12 % auf 96.000 gestiegen ist.

Der Gewinnung und Bindung von Spezialistinnen und Spezialisten durch Staat, Kommunen und Wirtschaft kommt für die Gewährleistung von Cybersicherheit eine fundamentale Bedeutung zu.

So muss neben Anreizen zur Gewinnung und Bindung von Fachkräften auch durch eine deutlich stärkere Verankerung der Thematik Cybersicherheit in Lehrplänen, in Studien- und Ausbildungsgängen sowie durch die Schaffung neuer Fachausprägungen bereits an einem frühen Punkt angesetzt werden. Die Ausbildung zukünftigen Fachpersonals ist somit ein wesentlicher Baustein, um dem Mangel an Spezialistinnen und Spezialisten nachhaltig entgegenzuwirken.

Gegenwart

Hessen betreibt eine nachhaltige Nachwuchsgewinnung auf allen Ebenen der beruflichen Bildung. In vielen hessischen Lehrplänen der beruflichen Schulen ist das Thema Cybersicherheit schulformübergreifend fest verankert. Im Bereich der dualen Berufsausbildung werden die bundeseinheitlichen Rahmenlehrpläne durch landeseigene Handreichungen zum Thema ergänzt. Schülerinnen und Schüler der beruflichen Schulen sowie Lehrerinnen und Lehrer werden online an Kursen zu Cybersicherheit geschult.

Zudem sind Cybersicherheitsthemen Gegenstand zukunftsweisender Studiengänge der Landesverwaltung in Kooperation mit der Hochschule für öffentliches Management und Sicherheit (HöMS), die Nachwuchskräfte in den Fächern der Cyberkriminalistik und der Digitalen Verwaltung ausbilden und in ihrer Digitalkompetenz stärken. Das Land Hessen und die Hessische Zentrale für Datenverarbeitung (HZD) bieten in vielen Bereichen, beispielsweise Cyberkriminalistik im Fachbereich Polizei, Digitale Verwaltung, Informatik und Software-Technologie, zusammen mit hessischen Hochschulen und Universitäten berufsbegleitende Studiengänge an.

Die hessische Landesverwaltung bietet ihren Beschäftigten attraktive Berufs- und Arbeits-

felder mit vielfältigen Einstiegs- und Entfaltungsmöglichkeiten. Beschäftigte profitieren von einer fairen Bezahlung, einer familienbewussten und an Lebensphasen orientierten Personalpolitik, von Fortbildungsmaßnahmen sowie von einem sicheren Arbeitsplatz.

Schwerpunkt / Zielsetzung

Der steigenden Zahl fehlender Fachkräfte, insbesondere im Bereich der Cyber- und IT-Sicherheit, begegnet die Hessische Landesregierung mit einem umfassenden Maßnahmenpaket wie z. B. beim Projekt Verwaltung 4.0. So sollen Cybersicherheitsthemen bereits im Studium und in der Ausbildung, in den Ausbildungsplänen und Curricula fest verankert werden. Durch die regelmäßige Fortschreibung der Lehrinhalte an derzeitige Trends und Entwicklungen im Bereich der Cybersicherheit soll die Aktualität sichergestellt werden.

Zur Gewinnung von bereits ausgebildeten Fachkräften für alle Bereiche der Verwaltung und der Sicherheitsbehörden werden zielgruppenorientierte Personalgewinnungs- und Entwicklungskonzepte erarbeitet. Zudem sollen Einstiegs- und Aufstiegschancen im öffentlichen Dienst der Landesverwaltung für Fachkräfte aus dem Bereich der Cyber- und IT-Sicherheit verbessert werden.

Die Landesregierung prüft die Verbesserung der Rahmenbedingungen für Kooperationen zur Schaffung von weiteren (dualen) Studiengängen mit dem Schwerpunkt Cybersicherheit sowie von Anreizen zur Steigerung der Attraktivität des öffentlichen Dienstes für Fachkräfte der Cyber- und IT-Sicherheit.

Verantwortlichkeit

HKM
HMdF
HZD
HMdJ
HMWK
HMdIS – Abteilung Z – Referat Z 6
HMdIS – Abteilung VII – Abteilungsstab
HöMS
Hessische Landesstelle für Technologiefortbildung (HLfT)

Anwenderinnen und Anwender

5.4 Anwenderinnen und Anwender

Informationssicherheit umfasst weit mehr als nur technische Lösungen und spezifische Organisationsstrukturen. Eine ganz entscheidende Rolle hat hierbei der Mensch. Nur mit einem angemessenen Bewusstsein für Cybersicherheit kann etwa die Auswahl sicherer Softwareprodukte erfolgen und eine digitale Unbedachtheit, insbesondere im Bereich der Kommunikation, abgebaut werden. Dadurch können Einfallstore für Cyberkriminelle im Cyberraum sowohl im privaten als auch bei staatlichen Einrichtungen, bei Wirtschaftsunternehmen oder Forschungsinstituten geschlossen werden. Die Sensibilisierung von Anwenderinnen und Anwendern für Cybersicherheit beginnt bereits in der Schule und setzt sich in einem Prozess des lebenslangen Lernens fort.

5.4.1 Digitalisierung sicher gestalten

Bedeutung

Die Hessische Landesregierung verfolgt mit der Strategie „Digitales Hessen – Wo Zukunft zuhause ist" ein Kernanliegen: Digitalisierung soll dem Menschen dienen und nicht umgekehrt. Die Gewährleistung von Cybersicherheit ist eine Grundvoraussetzung, damit alle Bürgerinnen und Bürger den Mehrwert der Digitalisierung positiv erleben und ihr volles Potenzial ausschöpfen können sowie für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung. Sicherheit im digitalen Raum ist unentbehrlich für den langfristigen Erhalt der Freiheit von Bürgerinnen und Bürgern und nimmt deshalb eine Schlüsselrolle ein.

Gegenwart

Die Digitalisierung durchdringt alle Bereiche des Ökosystems. Dem Ansatz Security-by-Design folgend muss Cybersicherheit bei sämtlichen digitalen Entwicklungen im privaten oder öffentlichen Bereich von Beginn an symbiotisch mitgedacht werden

Mit der Umsetzung des Onlinezugangsgesetzes geht Hessen einen wichtigen Schritt hin zu einer modernen Verwaltung. Die Bedarfe der hessischen Bürgerinnen und Bürger sowie die Nutzerfreundlichkeit der Anwendungen werden dabei in den Mittelpunkt gestellt. Durch Digitalisierung und Vernetzung soll der Zugang zu Verwaltungsdienstleistungen

auch elektronisch angeboten werden. Vor der konkreten Umsetzung und Bereitstellung der Online-Dienstleistungen sind Sicherheitsaspekte zu berücksichtigen. Hierbei muss auch sichergestellt sein, dass die digitalisierten Leistungen von den Verwaltungen ohne zu großen Anpassungsaufwand genutzt werden können und somit insbesondere organisatorische Erleichterungen darstellen, die am Ende auch den entsprechenden Mehrwert für alle Beteiligten haben.

Die Kommunen spielen bei der Digitalisierung der Verwaltungsleistungen eine zentrale Rolle, denn sie sind für die Umsetzung einer Vielzahl der OZG-Leistungen zuständig. Seit Jahren arbeiten sie mit Hochdruck an der Umsetzung des OZG.

Gleichzeitig wurde mit dem Startschuss zum Onlinezugangsgesetz auch die Digitalisierung der dazu erforderlichen internen Verwaltungsprozesse beschleunigt. Auch die Digitalisierung im Sinne von Smart Cities und Smart Regions wird von vielen Kommunen angegangen. Das Land Hessen unterstützt und fördert zahlreiche Projekte in diesem Bereich, wie z. B. die Initiative zur Digitalstadt Darmstadt und die „Digitale Modellbehörde".

Der bewusste Umgang mit digitalen Technologien wird sowohl im Arbeitsumfeld als auch im privaten Bereich immer wichtiger. Auf Grund von technologischem Fortschritt und veränderten Anforderungen sowohl im beruflichen wie privaten Kontext kommt digitalen Kompetenzen eine immer größere Bedeutung zu. Dabei geht es nicht nur um das Bedienen von digitalen Tools und Apps, sondern um ein grundlegendes Verständnis der Technologie, der Chancen und auch Gefahren.

Hessen hat daher die Kampagne „Digitale Kompetenzen stärken" gestartet. Instrumente sind dabei die Webseite „www.wie-digital-bin-ich.de" mit dem darin enthaltenen DigiCheck Kompetenzen sowie einer Plattform zu Angeboten der digitalen Kompetenzstärkung, auch zum Thema IT-Sicherheit.

Schwerpunkt / Zielsetzung

Digitalisierung kann nicht ohne Cyber- und IT-Sicherheit gedacht werden. Diesem Grundsatz folgend legt die Landesregierung die Einbindung des CISO von Beginn an bei allen Digitalisierungsvorhaben der hessischen Landesverwaltung verbindlich fest.

Die Landesregierung setzt sich dafür ein, dass bei der Fortschreibung von Förderrichtlinien für Kommunen der Aspekt der IT-Sicherheit zukünftig mehr Berücksichtigung findet.

Das Informations- und Beratungsangebot der Geschäftsstelle Smarte Region Hessen soll auch im Themenkomplex Cyber- und IT-Sicherheit unter Einbindung von Hessen3C weiter ausgebaut werden.

Verantwortlichkeiten

HMinD

HKM

HMWK

HMdF

HMdIS - Abteilung VII – Referat VII 2

HMdIS - Abteilung VII – Referat VII 3

HMdIS - Abteilung VII – Referat VII 5

HMdIS - Abteilung VII – Referat VII 7

HMdIS - Abteilung VII – Referat VII 9

HMdIS - Abteilung VII – Referat VII 12 (Hessen3C)

5.4.2 Förderung praxisrelevanter Cybersicherheitskompetenzen

Bedeutung

Das Einfallstor für die überwiegende Mehrheit der Sicherheitsvorfälle in Institutionen ist der Mensch. 95 % aller Cybervorfälle gehen auf menschliche Fehler zurück. Unkenntnis, Nachlässigkeit, Gewohnheit, Vertrauen oder Neugierde nutzen Cyberkriminelle tagtäglich für ihre Zwecke aus. Durch gezielte Förderung von Cybersicherheitskompetenzen über alle Lebensphasen hinweg können Risikofaktoren stark minimiert und Schäden für die jeweiligen Betroffenen verhindert werden. Der sichere Umgang mit Technologien bedarf mehr denn je eines Bewusstseins über die, auch bei alltäglichen Anwendungen, im Netz lauernden Gefahren. Diese Grundfertigkeit gilt es, sehr frühzeitig zu vermitteln und durch lebenslanges Lernen im Rahmen von Fort- und Weiterbildungen fortzuentwickeln.

Gegenwart

Bedienstete des Landes Hessen haben die Möglichkeit, an vielfältigen Angeboten, unter anderem einem eLearning, bereitgestellt durch das HMdIS, im Bereich Informationssicherheit teilzunehmen. Bei der inhaltlichen Ausgestaltung arbeitet das Land Hessen mit Bundes- und Landesbehörden sowie Partnern aus Wirtschaft und Wissenschaft zusammen.

Schwerpunkt / Zielsetzung

Die Landesregierung plant den Ausbau der bereits bestehenden Cyber- und IT-Sicherheitsangebote und -schulungen des HMdIS, welche als verpflichtende Maßnahmen von allen Landesbediensteten zu absolvieren sein werden.

Verantwortlichkeiten

HKM
HMWK
HMdIS – Abteilung VII – Referat VII 12 (Hessen3C)
HMdIS – Abteilung VII – Referat VII 3
HMdIS – Abteilung Z – Referat Z 7
HZD
HÖMS
ekom21

5.4.3 Zielgruppenspezifische Awareness

Bedeutung

Cyberkriminalität gehört weltweit zu den Kriminalitätsphänomenen, welche den höchsten finanziellen Schaden verursachen. Die Täterinnen und Täter wählen ihre Opfer nach der größtmöglichen Profitabilität und dem geringsten Aufwand aus. Dies geschieht agil und wird durch aktuelle gesellschaftliche und geopolitische Geschehnisse beeinflusst. Folglich müssen Awareness-Veranstaltungen regelmäßig und an den jeweiligen Zielgruppen orientiert angepasst werden.

Cyberangriffe richten sich am häufigsten gegen KMU aber auch gegen KRITIS- Betreiber sowie Einrichtungen der Landes- und Kommunalverwaltung. Die Einfallstore für Attacken werden dabei oftmals von Beschäftigten geöffnet, denen die notwendige Awareness für Angriffe aus dem Cyberraum fehlt. Daher gilt es, die Beratungs- sowie Präventionsmaßnahmen zur Sensibilisierung an den dort beschäftigten Personen zielgruppenspezifisch auszurichten.

Awareness ist nicht als ein einmaliges Angebot, sondern als Prozess zu betrachten. Die regelmäßige Teilnahme an Beratungsangeboten zu aktuellen Themen sollte deshalb ein fester Bestandteil des Berufslebens sein.

Gegenwart

Das Hessen3C bietet ein breites Angebot an Beratungs- und Präventionsmaßnahmen, das sich an die Landesverwaltung, Kommunen, KRITIS sowie KMU richtet. Durch die Vermittlung aktuellen Wissens über das Vorgehen von Cyberkriminellen sollen die vorgenannten Zielgruppen vor Bedrohungsszenarien geschützt werden, die für sie besonders wahrscheinlich sind. Die entsprechenden Beratungs- und Präventionsangebote sind auf die jeweilige Personengruppe und deren individuelle Situation ausgerichtet. Auch innerhalb der Zielgruppen wird nach Faktoren wie der Funktion und dem Fachwissen differenziert.

Auf kommunaler Ebene werden Beratungs- und Präventionsangebote seitens der ekom21 angeboten.

Auch die Angebote der hessischen Polizei und des Landesamts für Verfassungsschutz Hessen werden fortlaufend evaluiert und an den jüngsten Erkenntnissen ausgerichtet aktualisiert.

Schwerpunkt / Zielsetzung

Um auch weiterhin einen hohen Qualitätsstandard für die Awareness vor Cyberangriffen und deren regelmäßige Aktualität zu gewährleisten, wird die Hessische Landesregierung das Hessen3C in seiner Funktion als Zentralstelle in Hessen stärken, welches seine Beratungsangebote kontinuierlich an aktuelle Cyberbedrohungen anpasst und ausbaut.

Die Hessische Landesregierung strebt die fortdauernde Steigerung der Awareness und zielgruppenorientierte Ausbildung der Bediensteten der Landes- und Kommunalverwaltung an. Hierzu sollen die bestehenden Angebote zielgruppenspezifisch aufbereitet, beworben sowie Multiplikatorinnen und Multiplikatoren auf Landes- und kommunaler Ebene ausgebildet werden.

Verantwortlichkeiten

„Allgemeine Awareness ist die Aufgabe aller Ressorts“
Für die fachliche Ausgestaltung:
HMSI
HMdIS – Abteilung VII – Referat VII 12 (Hessen3C)
HMdIS – Abteilung VII – Referat VII 3
HMdIS – Abteilung Z – Referat Z 7
HMdIS - Landespolizeipräsidium
Landesamt für Verfassungsschutz Hessen
HZD
ekom21

5.4.4 Verbraucherschutz

Bedeutung

In einer komplexen, digitalisierten Welt wird Verbraucherschutz immer wichtiger. Eine ganzheitliche Cybersicherheitsstrategie nimmt die Verbraucherinnen und Verbraucher als wichtige Adressatinnen und Adressaten ihrer Maßnahmen in den Blick.

Die Sicherheitsrisiken, die für die Verbraucherin und den Verbraucher am Endgerät oftmals nicht auf den ersten Blick ersichtlich sind, können weitreichende Folgen nach sich ziehen. Erschwerend kommt beim Kauf von Endgeräten und Software häufig hinzu, dass Preis und Sicherheit in direkter Konkurrenz stehen. Die vielfältigen Anforderungen an die Sicherheit von Hard- und Software können so komplex und undurchsichtig sein, dass sie für die Endverbraucherin und den Endverbraucher unüberwindbare Hürden darstellen.

IT-Sicherheit und Datenschutz sind dabei auch immer Verbraucherschutz.

Gegenwart

Hessen legt großen Wert auf einen selbstbestimmten Umgang mit Personendaten und eine hohe Datensicherheit bei IT-Anwendungen.

Bei der Aufklärung der Bürgerinnen und Bürger arbeitet das Land Hessen eng mit zahlreichen Kooperationspartnern, wie beispielsweise der Verbraucherzentrale Hessen e. V., zusammen. Im Verbraucherschutzportal der Hessischen Landesregierung www.verbraucherfenster.hessen.de werden Nutzerinnen und Nutzer tagesaktuell auch über Themen der IT-Sicherheit informiert. Hintergründe werden durch praktische Tipps ergänzt.

Mit der Anwendung HessenWarn werden insbesondere die Bürgerinnen und Bürger in Hessen regelmäßig über aktuelle Sicherheitsvorfälle informiert und vor möglichen Gefahren im digitalen Raum gewarnt.

Schwerpunkt / Zielsetzung

Die Hessische Landesregierung verfolgt das Ziel, Bürgerinnen und Bürgern den selbstbestimmten und sicheren Umgang mit Daten zu ermöglichen und setzt dazu auf regelmäßige Informationen der Fachdienststellen in Zusammenarbeit mit den Partnereinrichtungen für den Verbraucherschutz in Hessen. Diese sollen zur Steigerung des Bewusstseins für das Thema Cybersicherheit in der hessischen Bevölkerung beitragen.

Verantwortlichkeiten

HMUKLV

HBDI

5.4.5 Digitale Zivilcourage

Bedeutung

Die zunehmende Digitalisierung zwischenmenschlicher Kommunikation ermöglicht die unkomplizierte Vernetzung, die Teilnahme am gesellschaftlichen Diskurs und den schnellen Austausch aller Bürgerinnen und Bürger.

Hate Speech, Fake News und extremistisches Gedankengut stellen eine zunehmende Herausforderung in diesem Kontext dar und können eine Gefahr für demokratische Normen und Werte sein. Ebenso gehören Cybermobbing und das Begehen von Straftaten zur Schattenseite des digitalen Raums.

Anwenderinnen und Anwender können als aktive Gestalterinnen und Gestalter das demokratische Miteinander und den freiheitlichen Diskurs schützen. Digitale Zivilcourage ist hierfür ein zentraler Faktor und schließlich entscheidend für die Förderung eines respektvollen und sicheren Miteinanders in digitalen Räumen.

Einer unkomplizierten und schnellen Schnittstelle zur Unterstützung durch die Gefahrenabwehr-, Sicherheits- und Strafverfolgungsbehörden sowie gemeinnützige zivilgesellschaftliche Einrichtungen und den damit verbundenen Handlungsmöglichkeiten kommt hierbei eine besondere Bedeutung zu.

Gegenwart

Im Rahmen des Aktionsprogramms #HESSENGEGENHETZE, entwickelt um Rechtsextremismus, Gewalt und Hass im Internet entschieden entgegenzutreten, wurde die Meldestelle HessenGegenHetze im Hessen3C eingerichtet. Die Meldestelle arbeitet eng mit der Generalstaatsanwaltschaft Frankfurt am Main (ZIT), dem Bundeskriminalamt (ZMI) und dem Hessischen Landeskriminalamt sowie mit dem Landesamt für Verfassungsschutz Hessen und weiteren Partnern zusammen.

Im Rahmen der Förderrichtlinie „Cybersicherheitsforschung in Hessen" wurde im Zuge des „DeTOx"-Verbundforschungsprojektes, eine Anwendung zur automatisierten Erkennung und Klassifikation von Fake News und Hate Speech mittels Künstlicher Intelligenz entwickelt. Die Meldestelle HessenGegenHetze des Hessen3C arbeitet hier mit der Hochschule Darmstadt und dem Fraunhofer SIT zusammen.

Gefördert durch das Landesprogramm „Hessen – aktiv für Demokratie und gegen Extremismus“ unterstützt das Land Hessen Präventionsprojekte gegen Hass im Netz. Das hessische Landespolizeipräsidium führt in diesem Rahmen Projekttage und -wochen für Schülerinnen und Schüler sowie pädagogische Fachkräfte durch, sodass Medienkompetenz bereits frühzeitig gefördert und Zivilcourage als gesellschaftliche Verantwortung vermittelt wird. Präventive Maßnahmen werden unter anderem auch vom Beratungsnetzwerk Hessen - gemeinsam für Demokratie und gegen Rechtsextremismus, dem Hessischen Informations- und Kompetenzzentrum gegen Extremismus (HKE) und dem Netzwerk gegen Gewalt durchgeführt. Auch die Initiative „Hessen lebt Respekt“ der Hessischen Staatskanzlei umfasst in Zusammenarbeit mit der Landesmedienanstalt Hessen (Respekt digital) die Sensibilisierung für ein respektvolles und verantwortungsbewusstes Handeln im Netz.

Die Initiative #KeineMachtdemHass des Hessischen Justizministeriums zusammen mit Partnern aus Zivilgesellschaft, Medien und Wissenschaft begegnet entschlossen Hass und Hetze im Netz. Mit der App „MeldeHelden“ wird hier eine weitere niedrigschwellige nichtstaatliche Möglichkeit geboten, um auf Inhalte hinzuweisen.

Auch die Beratungsstelle Jugend und Medien Hessen des HKM stellt Kindern und Jugendlichen, Lehrkräften sowie Eltern Informationen, Materialien und Beratungsangebote u.a. zu den Themen Fake News und Hate Speech sowie Cybermobbing zur Verfügung.

Schwerpunkt / Zielsetzung

In Hessen gibt es keinen Platz für Hass und Hetze. Die Hessische Landesregierung steht für ein geschlossenes Vorgehen gegen Hass, Hetze und Extremismus und verfolgt die Bündelung aller Aktivitäten im HMdIS. Der Vernetzung von staatlichen Akteuren, Initiativen und Projekten sowie den Bürgerinnen und Bürgern kommt hierbei eine besondere Bedeutung zu.

Zur Aufklärung und Information über bestehende Handlungsmöglichkeiten soll verstärkt in zielgruppenspezifischen Präventionsangeboten zum Thema „Hass im Netz“ sensibilisiert werden.

Verantwortlichkeit

StK

HMdJ

HKM

HMdIS – Abteilung VII – Referat VII 12 (Hessen3C)

HMdIS – Landespolizeipräsidium

Landesamt für Verfassungsschutz Hessen

5.4.6 Schutz von Kindern und Jugendlichen

Bedeutung

Digitale Medien prägen heute das Aufwachsen von Kindern und Jugendlichen wie in keiner Generation zuvor. Die Nutzung des Internets durch Kinder und Jugendliche hat sich sehr schnell entwickelt. Sie verfügen heute über eigene Internet-Zugänge und onlinefähige Geräte. Das Internet ist für sie selbstverständlicher Lebensraum, sie verbringen einen großen Teil des Tages online. Immer mehr Kinder und Jugendliche machen so auch negative Erfahrungen. Beleidigungen, Hasskommentare und systematisches Mobbing zählen zu den größten Risiken. Auch sexuell motivierte Belästigungen und Übergriffe sind alltägliche Erfahrung von Kindern und Jugendlichen, vor allem in Social Media-Diensten und Online-Spielen.

Gegenwart

Strukturen für die Regulierung von Gewalthandeln, die in der analogen Welt selbstverständlich sind, existieren im Internet bisher nur in Ansätzen. Weltweit werden deshalb Regelungen diskutiert und beschlossen, mit denen Betreiber von Online-Diensten zu größerer Vorsorge für den Schutz von Kindern und Jugendlichen verpflichtet werden. Letztlich entscheidend ist die Durchsetzung. Hier gibt es nach wie vor Defizite.

In Hessen sowie in ganz Deutschland gibt es bereits zahlreiche Initiativen und Projekte, die am Schutz von Kindern und Jugendlichen vor (sexualisierter) Gewalt mitwirken. Im Rahmen des Beteiligungsprozesses zum hessischen Aktionsplans zum Schutz von Kindern und Jugendlichen vor sexualisierter Gewalt wurden zahlreiche Maßnahmen-Empfehlungen gegeben, die dazu beitragen sollen, diese Initiativen und Projekten miteinander zu vernetzen, weiterzudenken und zusätzliche Ansatzpunkte zu identifizieren.

Das Netzwerk gegen Gewalt Hessen ist die Gewaltpräventionsinitiative der Hessischen Landesregierung. Es wurde mit der Aufgabe initiiert, Akteurinnen und Akteure der Gewaltprävention, wie Behörden, Schulen, Einrichtungen der Jugendhilfe, Eltern, Vereine, private Initiativen und engagierte Menschen in Hessen zu vernetzen.

Für die landesweite operative Tätigkeit ist die zentrale Geschäftsstelle zuständig. Hessenweit ist das Netzwerk durch sieben regionale Geschäftsstellen in den jeweiligen Polizeipräsidien vertreten, die auch Ansprechpartner für Kommunen und Landkreise sind. Unmittelbare Zielgruppe der Maßnahmen sind Kinder, Jugendliche und Heranwachsende.

Das Thema „Sexualisierte Gewalt“ bearbeitet das Netzwerk gegen Gewalt als eines von mehreren Themen in der Gewaltprävention.

So wurde gemeinsam mit dem Hessischen Innenministerium durch die hessische Polizei beispielsweise ein hessenweites Beratungstelefon zur Prävention und Aufklärung über die Verbreitung von Kinder- und Jugendpornografie eingerichtet, an das sich u.a. Eltern oder junge Menschen vertrauensvoll an die Präventionsexperten der hessischen Polizei wenden können.

Schwerpunkt / Zielsetzung

Ziel ist, sexualisierte Gewalt gegen Kinder und Jugendliche im Netz möglichst von Anfang an zu verhindern. Deshalb hat die Prävention, beispielsweise durch ziel- und altersgruppengerechte Sensibilisierung und Medienerziehung sowie durch die Qualifizierung pädagogischer Fachkräfte, eine besondere Bedeutung.

Zur Umsetzung und Implementierung präventiver Maßnahmen, wurde die „Projektgruppe zum Schutz unserer Kinder“, unter der künftigen Schwerpunkt-Marke „GEMEINSAM SICHER – FÜR KINDER UND JUGENDLICHE“ der Dachmarke „GEMEINSAM SICHER IN HESSEN“ durch die hessische Polizei eingerichtet.

Die Projektgruppe hat u.a. zum Ziel, gemeinsam mit vielen Kooperations- und Netzwerkpartnern, folgende drei Projekte hessenweit umzusetzen:

- „Brich-Dein-Schweigen“
  (entwickelt vom PP Südhessen, Schwerpunkt Prävention von Hands-on-Delikten),
- „Digital Native“
  (entwickelt vom PP Osthessen, Schwerpunkt Hands-off-Delikte) und
- MeKoKi - Medienkompetenz in Kindertagesstätten
  (entwickelt vom Netzwerk gegen Gewalt im HMdIS, Schwerpunkt Aufbau von Medienkompetenz im Umgang mit sozialen Medien/Internet).

Ungeachtet dessen werden in Hessen seit dem 01.10.2020, um den gestiegenen Fallaufkommen begegnen zu können, alle Sexualstraftaten gegen Kinder und Jugendliche in der BAO FOKUS (Besondere Aufbauorganisation Fallübergreifende Organisationsstruktur gegen Kinderpornografie und sexuellen Missbrauch) gebündelt bearbeitet. Ziel war und ist die Intensivierung der Bekämpfung in den Phänomenbereichen Kinder- und Jugendpornografie, sowie

des sexuellen Missbrauchs von Kindern und Jugendlichen. Hierunter fallen sämtliche Sexualstraftaten gegen Kinder und Jugendliche gemäß §§ 174 bis 184c StGB.

Die Struktur, Organisation und Prozesse wurden in der BAO FOKUS seit Bestehen ständig überprüft und den herausfordernden Anforderungen im Hinblick auf Qualität und Quantität regelmäßig überprüft und angepasst.

Vor dem Hintergrund, dass hinter jeder kinderpornographischen Darstellung ein aktuell noch real stattfindender Missbrauch stecken kann, den es unmittelbar zu unterbinden gilt („Gefahrenüberhang"), wurde bei der BAO FOKUS eine Clearingstelle eingerichtet.

Ein weiterer wesentlicher Baustein der BAO FOKUS im Kontext der Gefahrenabwehr bzw. Prävention, ist die dort angesiedelte Handlungskonzeption Personenpotential KOPTER-HE (KOntrolle Pädokriminieller TätER-Hessen). Hier liegt der Fokus auf der Befassung mit pädokriminellen Tätern, deren intensive Betrachtung und Bewertung ihres Rückfallrisikos weitere Straftaten in diesem Deliktbereich verhindern soll.

Die intervenierende Bekämpfung sexualisierter Gewalt im Internet setzt darüber hinaus eine nachhaltige und ganzheitliche Strategie voraus, eine gute Koordination der Akteurinnen und Akteure sowie regelmäßige Überprüfungen der Wirksamkeit ergriffener Maßnahmen. Neben Präventions- und Interventionsmaßnahmen sind auch die Ursachen sexualisierter Gewalt im Netz aufzuspüren und zu beseitigen.

Verantwortlichkeit

HMdIS
HMdJ
HKM
HMSI
HMinD

Vernetzung und Kooperation

5.5 Vernetzung und Kooperationen

Die Investition in die Vermittlung praxisrelevanter Cybersicherheitskompetenzen im Bildungssektor führt nicht nur zu einer Erhöhung der persönlichen Resilienz jeder und jedes Einzelnen, sondern dient gleichzeitig der Förderung zukünftiger Fachkräfte. Nur wenn staatliche Institutionen bzw. die politischen Verantwortungsträgerinnen und Verantwortungsträger in die Schulbildung zum Thema Cybersicherheit investieren, kann eine stabile Basis für die Resilienz von Anwenderinnen und Anwendern gegen Cyberkriminelle geschaffen und Interesse für Cybersicherheit geweckt werden. Letzteres generiert den Kreis der zukünftigen Fachkräfte, die zum Teil in die Wissenschaft eintreten und als innovative Impulsgeber die Forschung und Entwicklung weiter vorantreiben. Von den erzielten Ergebnissen profitieren wiederum alle Gemeinschaften, indem beispielsweise durch neue Softwareprodukte die Schutzlevel von IT-Systemen verbessert werden können.

Dies ist nur eines der zahlreichen Szenarien, welches deutlich macht, dass sich eine solide Sicherheit der einzelnen Gemeinschaften im Cyberraum nur über ihr wechselseitiges Zusammenwirken entfalten kann. Vernetzung, Kooperation, Austausch und Wissenstransfer sind dafür entscheidend, die Potenziale der Wechselbeziehungen auszuschöpfen. Je stärker die Wechselbeziehungen ausgeprägt sind, desto höher ist das zu erreichende Niveau an Sicherheit im Ökosystem Cybersicherheit.

5.5.1 Öffentlich-private Partnerschaften

Bedeutung

Die Mehrheit der hessischen KMU ist über Verbände organisiert oder ist Mitglied bei der Industrie- und Handelskammer (IHK) oder Handwerkskammer (HWK). Die Vernetzung der KMU mit diesen und weiteren (privaten) Institutionen stellt einen wichtigen Eckpfeiler in der effektiven Kommunikation mit ihnen dar. Hier können unter anderem in der Präventionsarbeit, aber auch für die fachliche Fortbildung, Synergien genutzt werden, um künftigen Cybersicherheitsbedrohungen gemeinsam entgegenzuwirken.

Gegenwart

Zur Steigerung der Reichweite von Sensibilisierungsmaßnahmen für die KMU in Hessen kooperiert das Hessen3C mit dem TÜV Hessen.

Über die Mitgliedschaft in der Allianz für Cybersicherheit des BSI ist das Land Hessen einer Kooperationsplattform zwischen Unternehmen, Verbänden, Behörden und Organisationen zum Austausch von Informationen zu aktuellen Bedrohungslagen und praxisnahen Cybersicherheitsmaßnahmen beigetreten.

Die Geschäftsstelle Smart Region bringt mit Unterstützung verschiedener Ressorts Start-Ups, Kommunen sowie nationale und internationale Expertinnen und Experten aus Wirtschaft und Wissenschaft zu Fragen der Cybersicherheit in unterschiedlichen Foren zusammen.

Schwerpunkt / Zielsetzung

Im Kampf gegen Cyberangriffe liegt die Stärke in der Gemeinschaft. Die Hessische Landesregierung fördert den Zusammenschluss sowie den Ausbau und die Verfestigung von Partnerschaften zwischen öffentlicher Verwaltung und Privatwirtschaft.

Um die Vernetzung der öffentlichen Verwaltung mit den handelnden und verantwortlichen Personen der KMU sicherzustellen, sollen der CERT-Austausch weiter ausgebaut und der Aufbau eines CISO-Netzwerks realisiert werden.

Verantwortlichkeit

HMinD
HMdIS – Abteilung VII – Referat VII 12 (Hessen3C)
HMdIS – Abteilung VII – Referat VII 13
HMdIS – Abteilung Z – Referat Z 6

5.5.2 Cybersicherheit gemeinsam mit Partnern

Bedeutung

Cybersicherheit ist die Grundvoraussetzung für eine erfolgreiche Digitalisierung sowie den Erhalt der Wettbewerbsfähigkeit Hessens und seiner Unternehmen. Cyberangriffe entwickeln sich dynamisch fort und machen nicht vor Ländergrenzen halt. Daher ist Vernetzung mit Partnern im Land und länderübergreifend unabdingbar. So können Bedrohungen frühzeitig erkannt, gemeinsam bewältigt sowie Präventionsstrategien entwickelt, ausgebaut und weitergeführt werden.

Gegenwart

Zur Vernetzung mit dem nationalen Forschungszentrum für angewandte Cybersicherheit (ATHENE) auf höchster Ebene wurde mit dem Beirat Cybersicherheit unter Leitung des hessischen Innenstaatssekretärs ein impulsgebendes, output- fokussiertes Cybersicherheitsnetzwerk einberufen. Der Beirat erkennt wesentliche Entwicklungen und Bedarfe frühzeitig und berät programmatisch. Wissenschaftliche Erkenntnisse werden im Beirat gebündelt und mit den spezifischen Bedarfen der Praxis verknüpft.

Im länderübergreifenden Kontext haben Baden-Württemberg und Hessen eine Kooperation zur Stärkung der Cybersicherheit vereinbart. Gegenstand dessen ist eine Intensivierung der Zusammenarbeit. Die Kooperationsvereinbarung nennt als Handlungsfelder einen intensiveren Erkenntnis- und Wissenstransfer bei länderübergreifenden Cyberlagen, eine gegenseitige Unterstützung bei der Aus- und Fortbildung von Cybersicherheitsexpertinnen und -experten sowie die Beratung und Unterstützung bei strategischen Fragestellungen und operativen Anforderungen.

Darüber hinaus findet im Rahmen der Zusammenarbeit mit Bayern und Baden-Württemberg ein regelmäßigerer Informationsaustausch zu Phänomenen und zur Lageentwicklung im Cyberraum statt.

Schwerpunkt / Zielsetzung

Um Bedrohungen rechtzeitig identifizieren und Schaden gemeinsam abwenden zu können sowie Präventionsstrategien zu entwickeln, wird die Hessische Landesregierung das landesweite und länderübergreifende Partnernetzwerk ausweiten. Hessen steht seinen Partnern mit dem fachlichen Know-how unterstützend zur Seite und profitiert gleichermaßen von diesem Austausch. Dies gilt es nachhaltig, durch regelmäßige gemeinsame Übungen zur Cyber- und IT-Sicherheit und gegenseitige Hospitationen zum Informationsaustausch, zu stärken.

Verantwortlichkeit

HMdIS – Abteilung VII – Referat VII 12 (Hessen3C)

HMdIS – Abteilung VII – Referat VII 4

5.5.3 Nationale und internationale Zusammenarbeit und Kooperationen

Bedeutung

Die digitale Vernetzung führt dazu, dass marktführende Softwareanwendungen weltweit genutzt werden. In der Folge sind die Ausnutzung von Schwachstellen sowie der bestmögliche Schutz davor als globale Herausforderung zu verstehen. Dabei sind alle Verwaltungsebenen, unabhängig davon, ob kommunal, national, europäisch oder multinational, gleichermaßen gefordert. Umso wichtiger ist es, eine Vielzahl an Cybersicherheitspartnern im nationalen und internationalen Bereich zu gewinnen und gemeinsam Schutz- und Abwehrmechanismen zur Bekämpfung von Cyberangriffen zu erarbeiten.

Eine Zusammenarbeit zwischen Bund, Ländern und Kommunen, in Ergänzung zu den jeweils bestehenden Zuständigkeiten, ist bei der Begegnung von Cybersicherheitsvorfällen essenziell. So können gesammelte Erfahrungen als Best-Practice und / oder Lessons-Learned in die zukünftige Bewältigung einfließen. Aus organisatorischer Sicht können somit Synergien unter Vermeidung von Doppelstrukturen erzeugt werden.

Gegenwart

Die Innenministerkonferenz (IMK) hat in ihrer 211. Sitzung vom 04. bis 06.12.2019 in Lübeck die Umwidmung der seit 2011 bestehenden „länderoffenen Arbeitsgruppe Cybersicherheit" in die „Länderarbeitsgruppe Cybersicherheit" (LAG CS) beschlossen. Unter dem Vorsitz Hessens arbeiten seither alle Länder in der Arbeitsgruppe zusammen.

Die Aufgaben der LAG CS umfassen die Abstimmung der Länder zu den Themen des Nationalen Cyber-Sicherheitsrates (NCSR) und die Berichterstattung an die IMK sowie den Erfahrungsaustausch und die Vernetzung zu allen Aspekten von Cybersicherheit. Dies gilt insbesondere für die Bereiche der Sicherheitsbehörden, der Wissenschaft, der Kommunen und der Wirtschaft. Des Weiteren liegen die Abstimmung, die Unterstützung und die Koordination von Initiativen und Maßnahmen zur Erhöhung der Cybersicherheit sowie die Sicherstellung eines kontinuierlichen wissenschaftlichen Inputs aus der Cybersicherheits-Forschung in der Verantwortung der LAG CS.

Aspekte der Cybersicherheit im Bereich der Verwaltung von Bund und Ländern werden durch die AG Informationssicherheit des IT-Planungsrates behandelt.

Hessen und Niedersachsen vertreten die Interessen der Länder auf Bundesebene im Nationa-

len Cyber-Sicherheitsrat (NCSR). Der NCSR fungiert als strategischer Ratgeber der Bundesregierung und bringt Vertreterinnen und Vertreter aus Bund, Ländern, Kommunen, Wirtschaft und Wissenschaft zusammen, um sich zu den für Deutschland im Bereich Cybersicherheit wesentlichen Themen auszutauschen und zukunftsweisende Impulse zu geben.

Seit Herbst 2021 ist das Hessen CyberCompetenceCenter (Hessen3C) des HMdIS eine von zwei Partnereinrichtungen auf Landesebene im Nationalen Cyber-Abwehrzentrum (Cyber-AZ).

Das Cyber-AZ ist im Bereich der Cyberabwehr die Kooperations-, Kommunikations- und Koordinationsplattform der relevanten (Sicherheits-)Behörden unterschiedlicher Ressorts und Ebenen des Bundes. Es koordiniert relevante Informationen zwischen beteiligten Behörden und Partnern und tauscht Schutzmaßnahmen zur Gewährleistung von Cybersicherheit in Deutschland aus.

Durch die Kooperationsvereinbarung des Landes Hessen mit dem BSI wurde die gegenseitige Unterstützung bei gemeinsamen Projekten, in der Fortbildung, bei Übungen zum IT-Krisenmanagement sowie beim Wissenstransfer zwischen BSI und Hessen festgeschrieben. Damit hat die Zusammenarbeit eine neue Qualitätsstufe erreicht.

Das Thema Cybersicherheit wird aufgrund seiner querschnittlichen Relevanz auch in weiteren Gremien und Fachministerkonferenzen (Kultusministerkonferenz, Justizministerkonferenz, etc.) behandelt, die sich mit ressortspezifischen Fragestellungen befassen.

Ein von der Landesregierung unterstütztes südhessisches Konsortium unter Koordination des House of Digital Transformation e. V. (HoDT) und mit den weiteren Mitgliedern Fraunhofer-Institut für Sichere Informationstechnologie SIT, GSI Helmholtzzentrum für Schwerionenforschung in Darmstadt, Hessisches Zentrum für Künstliche Intelligenz hessian.AI, Mittelstand-Digital Zentrum Darmstadt sowie TechQuartier erhält seit 2023 für das Projekt EDITH – „Enabling Digital Transformation in Hesse“ für zunächst drei Jahre eine Förderung der Europäischen Kommission. Der Fokus des Hubs wird u.a. auf Cybersicherheit gelegt. Eine Vernetzung mit anderen europäischen Hubs ist eines der Ziele des Programms.

Schwerpunkt / Zielsetzung

Hessen ist einer der wichtigsten Wirtschaftsstandorte in Deutschland. Die Hessische Landesregierung wird daher sicherstellen, dass diese Interessen bei zukünftigen Gesetzgebungs-

verfahren auf nationaler und europäischer Ebene sowie geplanten Maßnahmen des Bundes, hinsichtlich aller Cyber- und IT-Sicherheitsfragen berücksichtigt werden und wird die notwendigen Impulse geben.

Die Hessische Landesregierung setzt sich dafür ein, dass Hessen festes Mitglied im Cyber-AZ wird und als solches weiterhin die Cybersicherheit in Deutschland aktiv mitgestaltet. Eine verstärkte Vernetzung Hessens in allen beratenden und richtungsweisenden Gremien der nationalen Cybersicherheitsarchitektur wird angestrebt.

Mit der geplanten Gründung eines Hessischen Cybersicherheitsrats (HCSR) soll ein Gremium eingerichtet werden, welches die Aspekte der Cyber- und IT-Sicherheit auf Ebene der Entscheidungsträgerinnen und Entscheidungsträger der beteiligten Institutionen berät, Maßnahmen beschließt und Impulse zur Fortentwicklung der hessischen Cybersicherheitsstrategie setzt.

Verantwortlichkeit

Ressorts in den Fachministerkonferenzen
HMdIS – Abteilung VII, Referat VII 12 (Hessen3C)
HMdIS – Abteilung VII, Abteilungsstab
HMinD

Controlling

6. Controlling

Durch den Kabinettsbeschluss vom 04.09.2023 hat die vorliegende Cybersicherheitsstrategie für die gesamte hessische Landesverwaltung und die Ressorts verbindlichen Charakter. Die Frist bis zur Fortschreibung der Strategie beträgt maximal fünf Jahre.

Die bestehenden Zuständigkeiten der Ressorts bleiben von der Cybersicherheitsstrategie unberührt.

Zur Umsetzung, Erreichung und Fortschreibung der Ziele erstellen die verantwortlichen Ressorts in eigener Zuständigkeit und in Koordinierung durch das HMdIS einen landesweiten Umsetzungsplan, der alle erforderlichen Maßnahmen beinhaltet. Dieser Umsetzungsplan ist anhand der S.M.A.R.T.-Methode zu erarbeiten.

Über den ressortübergreifenden Umsetzungsstand der Cybersicherheitsstrategie informiert der Hessische Minister des Innern und für Sport den Landtag in jährlichem Zyklus. Dazu berichten die Ressorts nach Aufforderung dem Hessischen Ministerium des Innern und für Sport über die in ihrer Verantwortlichkeit liegenden Entwicklungen und getroffenen Maßnahmen.

Die Entwicklungen im digitalen Raum sind hochdynamisch und erfordern daher eine flexible Möglichkeit der inhaltlichen Anpassung der Cybersicherheitsstrategie. Notwendige Änderungen vor der nächsten Fortschreibung werden mit den Ressorts abgestimmt und in der digitalen Version der Cybersicherheitsstrategie auf der Webseite des Hessischen Ministeriums des Innern und für Sport vorgenommen.

Glossar

7. Glossar

Awareness

Awareness beschreibt das Bewusstsein einer Person oder Organisation für bestimmte Risiken, Bedrohungen oder Chancen. Im Bereich der IT-Sicherheit ist Awareness besonders wichtig, um die Nutzerinnen und Nutzer von Computersystemen auf die Gefahren von Cyberangriffen und anderen Bedrohungen aufmerksam zu machen und sie dazu zu bewegen, sich sicherheitsbewusst zu verhalten. Awareness-Kampagnen können Schulungen, Informationstafeln oder E-Mail-Newsletter umfassen.

Blockchain

Blockchain ist eine dezentrale, verteilte Datenbank, die Informationen in einer Kette von Blöcken speichert und durch kryptografische Verfahren gesichert ist. Die Blockchain-Technologie ermöglicht sichere Transaktionen und ist damit insbesondere für die Verwaltung digitaler Währungen wie Bitcoin von Bedeutung.

Chief Information Security Officer

Ein Chief Information Security Officer (CISO) ist eine Führungskraft, die für die Informationssicherheit in einem Unternehmen oder einer Behörde / Landesverwaltung verantwortlich ist. Der CISO entwickelt IT-Sicherheitsstrategien, koordiniert die Umsetzung von Sicherheitsmaßnahmen und stellt sicher, dass alle Mitarbeiterinnen und Mitarbeiter in Sicherheitsfragen geschult und sensibilisiert sind.

Computer Emergency Response Team

Ein Computer Emergency Response Team (CERT) ist eine Gruppe von Experten, die darauf spezialisiert sind, auf IT-Sicherheitsvorfälle zu reagieren und sie zu untersuchen. CERTs können beispielsweise in Unternehmen oder Behörden eingerichtet werden, um auf Sicherheitsvorfälle wie Hacking oder Malware-Infektionen zu reagieren.

Cyber- (als Teilwort)

Cyber bezieht sich auf „die von Computern erzeugte virtuelle Scheinwelt", eine nicht real betretbare Welt. Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann.

Cyberangriff

„Ein Cyberangriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyberraum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen."[1]

Cyberangriffe können enorme Tragweite haben, wie zahlreiche öffentlich bekanntgewordene Angriffe etwa auf Industrieanlagen, Kliniken, Verfassungsorgane und Behörden, Medien, Hochschulen und andere Einrichtungen zeigen. Unterschiedliche Akteure – etwa staatliche / nichtstaatliche – können unterschiedliche Motivationen und Ziele haben.

Cybercrime

Cybercrime bezieht sich auf kriminelle Aktivitäten, die im Zusammenhang mit Computersystemen oder dem Internet stattfinden, wie z. B. Hacking, Betrug oder Identitätsdiebstahl. Cybercrime ist ein wachsendes Problem, da immer mehr Bereiche des täglichen Lebens digitalisiert werden und Kriminelle neue Möglichkeiten finden, um an vertrauliche Daten oder Geld zu gelangen.

Cyberintelligence

Cyberintelligence bezieht sich auf die Sammlung, Analyse und Verbreitung von Informationen über Cyberbedrohungen, um Sicherheitsrisiken zu erkennen und zu minimieren. Cyberintelligence kann von Regierungsbehörden, Unternehmen oder unabhängigen Organisationen durchgeführt werden und umfasst die Überwachung von Netzwerken, die Analyse von Malware und die Verfolgung von Angriffen. Ziel ist es, frühzeitig auf Bedrohungen zu reagieren und effektive Schutzmaßnahmen zu ergreifen.

1 Gemäß Glossar der Allianz für Cyber-Sicherheit, https://www.allianz-fuer-cybersicherheit.de.

Cybermobbing

Cybermobbing bezeichnet das absichtliche Schikanieren, Bedrohen oder Bloßstellen einer Person oder Gruppe über das Internet oder andere digitale Medien. Cybermobbing kann über soziale Netzwerke, Messaging-Apps, Online-Forums oder andere Plattformen stattfinden. Es kann schwerwiegende Folgen für die Opfer haben, wie z. B. psychische Belastungen.

Cyberraum

Der Cyberraum oder das Cyberspace bezeichnet den virtuellen Raum, der durch das Internet und andere digitale Netzwerke geschaffen wird. Im Cyberraum werden Informationen ausgetauscht, Dienste angeboten und Transaktionen durchgeführt. Da der Cyberraum nicht an geografische Grenzen gebunden ist, können Bedrohungen und Angriffe aus beliebigen Teilen der Welt erfolgen.

Cybersicherheit

Cybersicherheit umfasst dem Verständnis der LAG Cybersicherheit nach alle Aspekte der Sicherheit in der Informations- und Kommunikationstechnik sowie den Schutz gesellschaftlich relevanter Prozesse vor Cyberangriffen im gesamten Cyberraum. Hierbei handelt es sich um die Gesamtheit der mit dem Internet und vergleichbaren Netzen verbundenen Informationstechnik. Besondere Bedeutung hat dabei der Schutz der kritischen Infrastrukturen.

Cybersicherheitsarchitektur

Ein angemessenes Niveau der Cybersicherheit erfordert eine angemessene Cybersicherheitsarchitektur. In einer ganzheitlichen Cybersicherheitsarchitektur sind alle Akteure, Prozesse und Einrichtungen des Bundes und der Länder, die koordiniert mit der Herstellung und Aufrechterhaltung eines angemessenen Cybersicherheitsniveaus befasst sind, eingeschlossen.

Cyberspionage

Sie bezeichnet den „heimliche[n] Zugriff auf Computersysteme von Staaten, Organisationen oder Firmen zum Zweck der Spionage“.[2]

Damit beschreibt Cyberspionage solche Cyberangriffe, die speziell auf das Erbeuten von

2 Duden, https://www.duden.de/rechtschreibung/Cyberspionage.

Informationen abzielen. Laut BMI „[zeigen] Nachhaltigkeit und Zielauswahl von Cyberangriffen deutlich den Versuch, Politik und Bundesverwaltung strategisch auszuspionieren.[3]“ Siehe auch „Cyberangriff“.

Datenschutz

Datenschutz bezieht sich auf den Schutz personenbezogener Daten, die von Unternehmen, Behörden oder Organisationen erhoben, gespeichert oder verarbeitet werden. Ziel des Datenschutzes ist es, die Privatsphäre und die Rechte der betroffenen Personen zu schützen, indem angemessene Sicherheitsmaßnahmen ergriffen werden, um den Missbrauch oder die unbefugte Weitergabe von Daten zu verhindern.

Digitalisierung

Digitalisierung bezeichnet den Prozess der Umstellung von analoger auf digitale Technologien und Prozesse. Im Kontext der IT-Sicherheit bedeutet Digitalisierung, dass immer mehr Bereiche des täglichen Lebens digitalisiert werden, was neue Möglichkeiten für Cyberangriffe und andere Bedrohungen schafft. Gleichzeitig bietet die Digitalisierung jedoch auch Chancen für die Entwicklung neuer IT-Sicherheitslösungen und -technologien.

Dokumentenmanagementsystem

Ein Dokumentenmanagementsystem (DMS) ist ein System zur Verwaltung und Archivierung von Dokumenten in digitaler Form. Ein DMS ermöglicht es Unternehmen und Organisationen, Dokumente sicher und effizient zu speichern, zu organisieren und zu teilen. Ein geeignetes DMS sollte auch sicherheitsrelevante Aspekte wie Zugangskontrollen und Verschlüsselungstechniken berücksichtigen.

Fake News

Fake News bezeichnen falsche oder irreführende Informationen, die online oder in anderen Medien verbreitet werden. Fake News können absichtlich gestreut werden, um politische Ziele zu erreichen oder Desinformation zu verbreiten. Fake News können auch zur Verbreitung von Malware oder anderen Cyberbedrohungen verwendet werden.

3 BMI, https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/cyberspionage/cyberspionage-node.html.

Hate Speech

Hate Speech bezeichnet die Verwendung von beleidigenden, diffamierenden oder diskriminierenden Aussagen oder Ausdrücken gegenüber bestimmten Personen oder Gruppen aufgrund ihrer Rasse, Religion, Sexualität oder anderen Merkmalen. Hate Speech ist ein Problem in den sozialen Medien und anderen Online-Plattformen und kann zu einer Verbreitung von Hass und Gewalt führen.

Informations- und Kommunikationstechnologien

Informations- und Kommunikationstechnologien (IKT) beziehen sich auf die technischen Werkzeuge, Anwendungen und Systeme, die zur Verarbeitung, Speicherung und Übertragung von Daten und Informationen genutzt werden. IKT umfasst eine Vielzahl von Technologien wie Computer, Netzwerke, mobile Geräte, Software, Cloud-Services und das Internet. Die Sicherheit von IKT ist von entscheidender Bedeutung, da sie einen großen Einfluss auf die Wirtschaft, Gesellschaft und individuelle Privatsphäre hat.

Informationssicherheit

„Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwender ziehen in ihre Betrachtungen weitere Grundwerte mit ein.“[4]

Informationssicherheitsleitlinie

Eine Informationssicherheitsleitlinie ist ein Dokument, das die Richtlinien, Ziele und Verantwortlichkeiten für die Informationssicherheit in einem Unternehmen oder einer Organisation festlegt. Eine Informationssicherheitsleitlinie dient als grundlegende Richtlinie für das Informationssicherheitsmanagement und beschreibt die Maßnahmen, die zur Umsetzung der Informationssicherheitsstrategie erforderlich sind.

4 BSI, IT-Grundschutz-Kompendium, Edition 2021, Glossar, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.html?nn=12856.

Informationssicherheitsmanagementsystem

Ein Informationssicherheitsmanagementsystem (ISMS) ist ein umfassender Ansatz für das Management der Informationssicherheit in einem Unternehmen oder einer Organisation. Ein ISMS umfasst Prozesse, Richtlinien und Verfahren, um die Risiken im Zusammenhang mit der Verarbeitung, Speicherung und Übertragung von Daten und Informationen zu bewerten und geeignete Schutzmaßnahmen zu ergreifen. Ein ISMS umfasst auch die Überwachung, Bewertung und Verbesserung der Informationssicherheitsprozesse im Laufe der Zeit.

Internet of Things

„IoT steht für Internet of Things, also das Internet der Dinge. Im Gegensatz zu „klassischen" IT-Systemen umfasst das Internet der Dinge „intelligente" Gegenstände, die zusätzliche „smarte" Funktionen enthalten. Diese Geräte werden in der Regel an Datennetze angeschlossen, in vielen Fällen drahtlos, und können sogar oft auf das Internet zugreifen und darüber erreicht werden."[5]

IT-Krisenmanagement

IT-Krisenmanagement bezieht sich auf die Planung, Vorbereitung und Reaktion auf unvorhergesehene Ereignisse oder Katastrophen, die die IT-Infrastruktur und -Systeme eines Unternehmens oder einer Organisation betreffen können. IT-Krisenmanagement umfasst Maßnahmen wie Notfallpläne, Back-up- und Wiederherstellungsoptionen sowie eine schnelle Reaktion auf Bedrohungen, um die Geschäftskontinuität zu gewährleisten.

IT-Planungsrat

Der IT-Planungsrat ist ein Gremium in Deutschland, das sich aus Vertretern der Bundesregierung und der Länder zusammensetzt. Der IT-Planungsrat ist für die Koordination der IT-Strategien und -Projekte der Bundesregierung und der Länder verantwortlich und spielt eine wichtige Rolle bei der Förderung der IT-Sicherheit und des Datenschutzes in der öffentlichen Verwaltung.

5 Gemäß Glossar der Allianz für Cyber-Sicherheit, https://www.allianz-fuer-cybersicherheit.de.

IT-Sicherheit

„IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls."[6]

Kritische Infrastruktur

Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Regelungen für diese Bereiche sind auf allen Ebenen (EU, Bund, Länder, Kommunen) in der jeweiligen Zuständigkeit zu treffen. Entsprechend können/sollten diese Themen in Cybersicherheitsstrategien der jeweiligen Ebene aufgegriffen und in der Folge gegebenenfalls rechtlich abgesichert werden. Dabei sollte auf eine geeignete Verzahnung der jeweiligen Verwaltungsebenen und Zuständigkeitsbereiche geachtet und widersprüchliche/konkurrierende Doppeladressierung vermieden werden.

Beispielsweise bestehen auf EU-Ebene Regelungen in der NIS-Richtlinie[7], die per Umsetzungsgesetz[8] auf Bundesebene umgesetzt wurden.

Daneben wurde mit dem IT-Sicherheitsgesetz[9] (als Artikelgesetz) seitens des Bundes bereits 2009 der Bereich der Kritischen Infrastrukturen geregelt und in der BSI-KritisV näher bestimmt.[10]

6 BSI, IT-Grundschutz-Kompendium, Edition 2021, Glossar, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.html?nn=128568.
7 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.
8 Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.
9 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17.07.2015, 2021 Fortschreibung als Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme.
10 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz.

Die Kritischen Infrastrukturen werden dabei in der Regel näher unterteilt. Die Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) aus dem Jahr 2009 beispielsweise definiert neun Sektoren der Kritischen Infrastrukturen:

- Energieversorgung
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Staat und Verwaltung
- Medien und Kultur

Alle Organisationen aus diesen Sektoren zählen unabhängig von ihrer Größe zu den Kritischen Infrastrukturen (KRITIS).

Eine landes- und kommunalrechtliche Normierung und Umsetzung – samt Verzahnung mit der föderalen Ebene – könnte auch Bereiche unterhalb der Schwellenwerte des Bundes umfassen, beispielsweise wenn eine hohe Bedeutung für das Gemeinwesen vorläge. Solche Bereiche werden in Anlehnung an die KRITIS-Definition gemäß BSI-KritisV gelegentlich als „Sub-KRITIS" bezeichnet.

Künstliche Intelligenz

Künstliche Intelligenz (KI) bezieht sich auf Technologien und Anwendungen, die es Computern und Maschinen ermöglichen, menschenähnliche Fähigkeiten wie Spracherkennung, Bilderkennung und Entscheidungsfindung zu erlangen. KI wird in verschiedenen Anwendungen eingesetzt, wie z. B. in der Medizin, der Automobilindustrie, der Finanzwirtschaft und der IT-Sicherheit, um Prozesse zu optimieren und Entscheidungen zu treffen.

Mobile Incident Response Team

Mobile Incident Response Teams (MIRT) sind spezialisierte Teams, die in Notfällen schnell reagieren können, um IT-Sicherheitsvorfälle zu untersuchen und zu beheben. MIRT sind mobil

und können bei Bedarf an den Ort des Vorfalls reisen, um schnell und effektiv zu handeln.

Ökosystem

Ein Ökosystem bezeichnet die Gesamtheit der Beziehungen und Interaktionen zwischen verschiedenen Akteuren und Elementen in einem bestimmten Bereich. Im Kontext der IT-Sicherheit kann ein Ökosystem verschiedene Akteure wie Regierungen, Unternehmen, IT-Sicherheitsanbieter und Nutzer umfassen, die alle zusammenarbeiten, um die IT-Sicherheit zu verbessern und Bedrohungen zu minimieren. Ein Ökosystem kann auch die verschiedenen Technologien, Anwendungen und Systeme umfassen, die in einem bestimmten Bereich eingesetzt werden.

Open Source

Open Source bezieht sich auf Software, die unter einer Open-Source-Lizenz veröffentlicht wird und somit für die Öffentlichkeit frei verfügbar und zugänglich ist. Open-Source-Software wird oft von einer Community von Entwicklern und Nutzern weiterentwickelt und verbessert. Die Verwendung von Open-Source-Software kann Vorteile wie höhere Sicherheit, Flexibilität und niedrigere Kosten bieten.

OSINT

OSINT steht für Open-Source-Intelligence und bezieht sich auf die Verwendung von öffentlich zugänglichen Informationen und Datenquellen, um Informationen und Erkenntnisse zu gewinnen. OSINT wird oft von Geheimdiensten, Strafverfolgungsbehörden und Unternehmen verwendet, um Informationen zu sammeln und Bedrohungen zu identifizieren.

Quantencomputing

Quantencomputing ist eine Technologie, die auf der Quantenmechanik basiert und es Computern ermöglicht, Berechnungen mit einer Geschwindigkeit und Effizienz durchzuführen, die mit herkömmlichen Computern nicht möglich sind. Quantencomputer werden als potenziell bahnbrechend für verschiedene Anwendungen wie Kryptographie, künstliche Intelligenz und Materialwissenschaften angesehen. Quantencomputing stellt jedoch auch eine Herausforderung für die IT-Sicherheit dar, da die Verschlüsselung von Daten auf herkömmlichen Computern möglicherweise nicht mehr ausreichend sicher ist, wenn Quantencomputer weit verbreitet sind.

Security-by-default

Security-by-default ist ein Ansatz für die IT-Sicherheit, bei dem die Sicherheitsfunktionen standardmäßig in IT-Systemen, Geräten und Anwendungen aktiviert und voreingestellt sind. Dies soll sicherstellen, dass die IT-Systeme von Anfang an sicher und geschützt sind, ohne dass der Nutzer zusätzliche Einstellungen vornehmen muss.

Security-by-design

Security-by-design ist ein Ansatz für die Entwicklung von IT-Systemen, bei dem die IT-Sicherheit von Anfang an in den Entwicklungsprozess integriert wird. Dabei werden die Sicherheitsaspekte bereits in der Konzeptions- und Designphase berücksichtigt, um sicherzustellen, dass das IT-System von Anfang an sicher ist und keine Schwachstellen aufweist.

Smarthome-Geräte

Smarthome-Geräte sind Geräte und Systeme, die in Privathaushalten eingesetzt werden, um den Komfort und die Effizienz zu verbessern. Smarthome-Geräte können von einem Smartphone oder einem anderen Gerät aus gesteuert werden und umfassen oft Geräte wie Thermostate, Beleuchtungssysteme, Türschlösser und Überwachungskameras. Die IT-Sicherheit von Smarthome-Geräten ist von großer Bedeutung, da Schwachstellen und Angriffe auf diese Geräte das persönliche Leben und die Privatsphäre der Nutzer gefährden können.

SOCMINT

SOCMINT steht für Social Media Intelligence und bezieht sich auf die Verwendung von sozialen Medien zur Informationsbeschaffung und Erkenntnisgewinnung. SOCMINT wird oft von Geheimdiensten, Strafverfolgungsbehörden und Unternehmen verwendet, um Informationen zu sammeln und Bedrohungen zu identifizieren.

Impressum

Hessisches Ministerium des Innern und für Sport
Friedrich-Ebert-Allee 12
65185 Wiesbaden
Telefon: (0611) 353 – 0
E-Mail: poststelle@hmdis.hessen.de
Web: https://innen.hessen.de

HESSEN