TLP:CLEAR

Informations- und Datensicherheitsstrategie 2023 des Landes Mecklenburg-Vorpommern

I. Herausforderungen und Ziele der Digitalisierung

Die Verwaltungsdigitalisierung ist ein großes Versprechen nicht nur gegenüber der Wirtschaft, sondern insbesondere gegenüber den Bürgerinnen und Bürgern. Ausgehend durch den vom Onlinezugangsgesetz (OZG) getriebenen bürgerorientierten Ansatz erfolgt vor der Digitalisierung der analogen Verwaltungsprozesse eine ganzheitliche Betrachtung, Analyse und Optimierung der Verwaltungsabläufe. Die Bürgerinnen und Bürger mit ihren personenbezogenen und sensiblen Daten stehen nun im Mittelpunkt des zukünftigen Verwaltungshandelns. So werden auf diese Art und Weise deren Antragsverfahren zum einen verständlich, nachvollziehbar und transparent, zum anderen schlanker und komfortabler.

Die Bürgerinnen und Bürger sollen nicht laufen, sondern ihre Daten. Auf die bereits erhobenen oder in der Verwaltung vorliegenden Daten wird ohne ihr Zutun zugegriffen. Dadurch können Verwaltungsverfahren erheblich vereinfacht werden. Über Zugriffsmöglichkeiten auf die in der Verwaltung etablierten Vorgangsräume eröffnen sich neue Teilnahmemöglichkeiten für die Bürgerinnen und Bürger und das in Echtzeit.

Dadurch wandelt sich die einzelne Behörde von einer von außen intransparenten Einrichtung zu einer serviceorientierten und ganzheitlichen öffentlichen Verwaltung. Diese Wandlung zu einer serviceorientierten Verwaltung und die hierdurch bewirkte Erhöhung der Transparenz dürfte die Akzeptanz der Bürgerinnen und Bürger gegenüber der öffentlichen Verwaltung, den Rechtsstaat sowie das Demokratieprinzip nachhaltig erhöhen.

Neben den Effizienz-, Transparenz- und Akzeptanzvorteilen sowie weiteren ökonomischen Chancen erleichtert die Digitalisierung sowohl das Privatleben als auch den beruflichen Alltag. Um die Digitalisierung zu ermöglichen, haben Standardisierung, Automatisierung und Vernetzung stark zugenommen.

Geschlossene Netzwerke und nicht vernetzte Computersysteme wurden durch neue Anforderungen an die Vernetzung, Mobilität und Standardisierung verdrängt. Mit der Mobilität hat sich ebenfalls im Zeitalter der Digitalisierung die Art und Weise des Arbeitens und somit auch das Kommunikationsverhalten stark gewandelt. Diese andauernde Entwicklung führt zu großen Abhängigkeiten von der Informations- und Kommunikationstechnik (IKT) und somit auch zu neuen Risiken. Diese Risiken verstärken sich durch die zunehmende Anzahl von vernetzten Systemen, wodurch ebenfalls die Angriffsfläche deutlich zugenommen hat.

Um diesen Risiken angemessen zu begegnen, sind Informations- und Cybersicherheit sowie der Schutz personenbezogener Daten existenziell wichtige Begleiter der Digitalisierung. Diese sind kein Selbstzweck, sondern tragen deutlich zu einer Erhöhung des Vertrauens und der Akzeptanz bei der Digitalisierung bei. Sie sind jedoch vielmehr, nämlich ein Bürge für die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von schützenswerten Informationen oder Daten. Ein komplexes Thema wird nun noch komplizierter durch ein differenziertes Verständnis von Informationssicherheit, IT-Sicherheit und Datenschutz.

Informationssicherheit schließt neben den technischen auch nicht-technische Aspekte wie organisatorische, physische, personelle und datenschutzrechtliche Aspekte ein. In der Praxis müssen bei der Informationssicherheit die vier Säulen einer Organisation abgesichert werden. Hierbei handelt es sich zusammenfassend um die von einer Organisation eingesetzte IKT, die genutzten Liegenschaften (Gebäude, Räume, usw.), Sensibilisierung des Personals und die Auswahl von externen Dienstleistern.

Während die IT-Sicherheit als Teildisziplin der Informationssicherheit sich ausschließlich auf den Schutz der IKT bezieht, kommt dem Datenschutz durch die vollständig oder teilweise automatisierte Verarbeitung von personenbezogenen Daten eine besondere grundrechtliche Bedeutung zu.

Vom Bund wird die mit der Digitalisierung erforderliche Gewährleistung der Cyber- und Informationssicherheit mit dem im Gesetzgebungsverfahren befindlichen Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0) erneut aufgegriffen. Dieses Gesetz zielt jedoch ausschließlich auf die informations- und kommunikationstechnischen Systeme der Bundesverwaltung sowie auf die Bereiche der Kritischen Infrastrukturen und des Verbraucherschutzes ab.

Die öffentliche Verwaltung und somit auch das Informationssicherheitsmanagement der Landesverwaltung Mecklenburg-Vorpommern stehen aktuell vor mehreren Herausforderungen. Sie müssen unter anderem Antworten finden auf:

- neue und mobile Verwaltungstätigkeiten durch die Digitalisierung der Verwaltungsarbeit einschließlich eines sicheren und ortsunabhängigen Arbeitens,
- neue Arbeitsmodelle und die damit verbundenen Änderungen im Bereich der Organisation (flexible Arbeitszeiten, neue Arbeitsmethoden und Führungsstile sowie Matrixorganisationen usw.),
- neue digitale Technologien und die Gefahr von und durch Konfigurations- oder Bedienfehler,
- die parallele Anwendung von papierbasierten und digitalen Verwaltungsprozessen,
- Veränderungen in den Verwaltungsabläufen sowie Workflows und
- auf die Umstellung der Kommunikation auf digitale und soziale Medien.

Die Gewährleistung der Informationssicherheit für die informations- und kommunikationstechnischen Systeme der öffentlichen Verwaltung auf ein angemessenes Mindestsicherheitsniveau ist nach wie vor eine der größten Herausforderungen der Verwaltungsdigitalisierung.

Traditionelle Sicherheitskonzepte basieren auf einem Perimeterschutz, bei dem zwischen einem sicheren Innen und einem gefährlichen Außen unterschieden wird. Im „neuen Normal“ mit deutlich zunehmenden mobilen informations- und kommunikationstechnischen Systemen lässt sich dieser Strategieansatz nicht mehr anwenden.

Das derzeit in der Landesverwaltung noch vorhandene Sicherheitsniveau ist als Basisschutz mit partiell wirksamen Standard-Sicherheitslösungen zu qualifizieren. Das allein reicht jedoch allenfalls aus, um althergebrachte Cyberangriffe abzuwehren. Ein Basisschutz, der nicht flächendeckend in der Landesverwaltung umgesetzt ist und nicht dem Spiegelbild des neusten Stands der Technik entspricht, ist kein Garant für eine erfolgreiche Abwehr der Angriffe von

morgen. Vielmehr ist eine kontinuierliche Anpassung, Weiterentwicklung und Wirksamkeitsprüfung der Sicherheits- und Schutzmaßnahmen erforderlich.

So muss mit der digitalen Transformation auch eine Transformation in der Informationssicherheit einhergehen, die insbesondere ausgehend vom Schutzbedarf die Umsetzung von angemessenen Sicherheitsanforderungen forciert.

Folgerichtig sind die vorhandenen Strukturen, Zuständigkeiten und Aufgaben im Informationssicherheitsmanagementsystem (ISMS) der Landesverwaltung stetig an die sich ändernden Bedrohungspotenziale anzupassen und weiterzuentwickeln.

II. Informationssicherheit als neue Gemeinschaftsaufgabe

Die Gestaltung einer Informationssicherheitsarchitektur ist eine wesentliche Aufgabe des Staates, denn eine effiziente und nachhaltige Architektur ist unerlässlich für unsere digitale Gesellschaft einschließlich einer handlungsfähigen öffentlichen Verwaltung.

Verschiedene staatliche und kommunale Akteure prägen die Informationssicherheitsarchitektur des Landes Mecklenburg-Vorpommern. So gibt es Gefahrenabwehr- und Ordnungsbehörden, Strafverfolgungsbehörden, Nachrichtendienste, privatrechtliche und kommunale IT-Dienstleister sowie den Bereich der stark kommunal geprägten Kritischen Infrastrukturen. Die Zahl der Akteure vervielfältigt sich aus föderalen Gründen und durch die funktionale sowie fachliche Spezialisierung betreten weitere Akteure den Raum der Informations- und Cybersicherheit.

Das im Jahr 2014 durch den Beschluss der Landesregierung gegründete Computersicherheits-Ereignis- und Reaktionsteam Mecklenburg-Vorpommern (CERT M-V) hat in den vergangenen Jahren eine neue Qualität und Quantität von Cyber- beziehungsweise IT-Angriffen auf die informations- und kommunikationstechnischen Systeme und Infrastrukturen der Landes- und Kommunalverwaltung festgestellt. Nicht nur die Häufigkeit von erfolgreichen IT-Angriffen hat sich verändert, sondern auch die Art der Angriffe. Die ausgewählten Ziele heben insgesamt die Bedrohungslage auf ein neues und somit kritisches Niveau.

Heute können auch nicht technisch versierte Täterinnen und Täter in IT-Systeme oder Netzwerke eindringen, weil im Internet, insbesondere im sogenannten Darknet das hierfür notwendige Wissen und die erforderlichen Werkzeuge inklusive Anleitung zur Verfügung stehen. So gibt es spezielle Angebote, die problemlos beschafft und genutzt werden können. Dazu gehören die sogenannten »Crime-as-a-Service«- oder »Malware-as-a-Service«-Angebote, die hoch professionelle IT-Angriffe auf IKT-Systeme und Netzwerke ohne technisches Spezialwissen ermöglichen. Es ist eine neue Ökonomie entstanden, die diese Hackerwerkzeuge professionell entwickelt, vermarktet und die Angreifer bei der Durchführung von Straftaten technisch und organisatorisch unterstützt.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als nationale Cybersicherheitsbehörde und die LandesCERTs im VerwaltungsCERT-Verbund bestätigen dieses neue und andauernde Qualitätsniveau von Cyberbedrohungen. Diese Cyberbedrohungen haben zumeist weltweite und internationale Bezüge, sind extrem dynamisch und kommen in immer

neuen Ausprägungen auf uns zu. Das Allianz Risk Barometer 2020 bekräftigt diese Entwicklung und zählt Cyberbedrohungen zu den weltweiten TOP-Risiken.

Cyberbedrohungen treffen alle Anwendergruppen, die zudem untereinander immer stärker vernetzt sind. Durch diese Vernetzung reichen die Anwender die Bedrohungen auch untereinander weiter, was zu einem Dominoeffekt führen kann. So erleben die LandesCERTs in den letzten Monaten die massenhafte Verbreitung von raffinierten Angriffsmethoden durch organisierte, cyberkriminelle Strukturen, die bis vor einigen Monaten nachrichtendienstlichen beziehungsweise staatlichen Akteuren im Bereich der (Wirtschafts-)Spionage oder Sabotage vorbehalten waren.

Mit dem stufenweisen Aufbau und dem Betrieb eines Informationssicherheitsmanagement-systems (ISMS) in der Landesverwaltung konzentrierte sich die bisherige strategische Zielsetzung im Wesentlichen auf die Initialisierung des Informationssicherheitsmanagements, die Institutionalisierung der Sicherheitsorganisation, die Schaffung grundlegender Regelungen, die Etablierung von Kommunikationskanälen sowie auf die Erhebung des Arbeitsfeldes.

Die inhaltliche Auseinandersetzung mit der bisherigen Zielsetzung und die Wahrnehmung des Themas »Informationssicherheit« als eine Management- beziehungsweise Leitungsaufgabe ist noch nicht lückenlos in der gesamten Landesverwaltung erfolgt.

Allerdings ist eine erkennbare Zunahme der für die Bewältigung dieses umfassenden, komplexen und verantwortungsvollen Aufgabenspektrums erforderlichen personellen und finanziellen Ressourcen in den letzten Jahren punktuell zu verzeichnen. Diesen Prozess gilt es zielgerichtet weiter zu verstetigen, insbesondere mit Blick auf die Schaffung von verpflichtenden, ressortübergreifenden Richtlinien und Sicherheitsstandards (Governance).

Parallel zu diesen Aktivitäten müssen bereits jetzt die Weichen für eine landesspezifische Fort-schreibung der Informations- und Datensicherheitsstrategie gestellt werden. Diese soll verstärkt auf:

- die zentrale Steuerung, Koordinierung und Umsetzung von Sicherheitsstandards,
- die frühzeitige Erkennung sowie die ziel- und zweckgerichtete Reaktionsfähigkeit auf IT-Angriffe (Erhöhung der Widerstands- und Durchhaltefähigkeit),
- die lückenlose Umsetzung von Sicherheitskonzepten,
- die Wirksamkeit und Messbarkeit (Kostencontrolling) von Sicherheitsmaßnahmen und
- die Steigerung der Sensibilität für Informationssicherheit

bis Ende 2023 fokussieren.

Nur unter Berücksichtigung dieser strategischen Ziele kann der starken Stellung des Bundes mit seinem hohen Sicherheitsniveau, das insbesondere durch das BSI geprägt ist, adäquat auf Augenhöhe begegnet und ein einheitliches Mindestsicherheitsniveau erzielt werden. Dieses erfordert insbesondere eine noch intensivere und effizientere Zusammenarbeit aller Beteiligten auf allen Ebenen der öffentlichen Verwaltung.

III. Grundsätze und Handlungsfelder der Informations- und Datensicherheitsstrategie 2023

Um die Gemeinschaftsaufgabe »Verwaltungsdigitalisierung« flankiert mit den Antworten auf die Fragen der Informations- und Cybersicherheit weiterzuentwickeln, bedarf es für das Land Mecklenburg-Vorpommern einer Informationssicherheitsstrategie, die über einen reinen IT-Ansatz und über den Kooperationsgedanken hinausgeht.

Daher sind in der Informationssicherheitsstrategie neben der Informations- und Kommunikationstechnik zusätzlich personelle, physische und organisatorische Aspekte zu berücksichtigen, so dass ein allumfassender, ganzheitlicher und risikobasierter Ansatz umgesetzt wird, um alle relevanten Anforderungen erfüllen zu können. Auf Basis dieses Ansatzes erfolgt eine Risikoermittlung für alle aufgezeigten Aspekte und darauf abgestimmt die Entwicklung geeigneter Sicherheitsmaßnahmen.

Hierbei sind auch die sozialen Voraussetzungen und Auswirkungen von Sicherheitsmaßnahmen mit Blick auf eine Akzeptanz beim Anwender; bei den Landesbediensteten zu berücksichtigen. Abschließend müssen immer die wirtschaftlichen und funktionalen Anforderungen mit den der Informationssicherheit abgewogen werden.

Mit Blick auf die einleitend dargestellten Herausforderungen, strategischen Zielen und den genannten Grundsätzen bedarf es für die Weiterentwicklung der Informationssicherheitsstrategie primär fünf großer Handlungsfelder:

1. die Schaffung eines neuen rechtlichen, organisatorischen und infrastrukturellen Rahmens für die Informationssicherheitsarchitektur des Landes Mecklenburg-Vorpommern,
2. die Weiterentwicklung von zentralen Sicherheitslösungen und -diensten für alle staatlichen und kommunalen Stellen im Land Mecklenburg-Vorpommern für eine gemeinsame, Ebenen-übergreifende Reaktion durch Abwehrmaßnahmen auf IT-Angriffe,
3. die Beseitigung partieller, Silo-getriebener Sicherheitskonzepte und Schaffung eines ganzheitlichen Geltungsbereichs, der sowohl alle staatlichen als auch alle kommunalen Stellen und deren Eigenbetriebe in die Informationssicherheitsarchitektur des Landes integriert,
4. die Berücksichtigung und nachhaltige Integration von Informationssicherheit in allen informations- und kommunikationstechniknahen Projekten staatlicher und kommunaler Stellen mit Blick auf durchgängige Security- und Product-Lifecycle-Modelle (vergleiche Produktlebenszyklusmanagement; Security-by-Design) und
5. die mittelfristige Befähigung zur digitalen beziehungsweise technischen Souveränität staatlicher und kommunaler Stellen und deren IT-Dienstleister als Schlüsselvoraussetzung für ein gesellschaftliches und staatliches souveränes Handeln.

IV. Maßnahmen der Landesregierung

Ausgangspunkt aller Handlungsfelder bildet ein rechtlicher Rahmen, der mit dem Gesetz zur Neuordnung und Förderung der Informationssicherheit im Land Mecklenburg-Vorpommern (Informationssicherheitsgesetz Mecklenburg-Vorpommern – ISichG M-V) geschaffen werden soll.

Durch den Geltungsbereich dieses Gesetzes soll der ganzheitliche Ansatz der Informations- und Datensicherheitsstrategie über alle öffentlichen Stellen im Land erreicht werden. Der Gesetzesentwurf soll organisatorische Regelungen in folgenden Bereichen treffen:

a) Ausstattung des/ der Beauftragten der Landesverwaltung für Informationssicherheit (BeLVIS) mit ressortübergreifenden Sicherheitsrichtlinien- und Standardisierungskompetenzen. Darüber hinaus soll der/ die BeLVIS mit Prüf- und Kontrollbefugnissen sowie mit Weisungsbefugnissen bei besonderen IT-Sicherheitslagen oder -vorfällen ausgestattet werden.
b) Die Informationssicherheitsorganisation der Landesverwaltung soll mit angemessenen personellen Ressourcen in den Ministerien und der Staatskanzlei sowie in den größeren nachgeordneten Behörden und anderen Einrichtungen der Landesverwaltung ausgestattet werden.
c) In der Kommunalverwaltung soll eine dem Land vergleichbare Informationssicherheitsorganisation angestrebt werden.

Die ressortübergreifenden Sicherheitsrichtlinien und -standards sollen in der Kommission für Informationssicherheit (KofIS) gemeinsam erarbeitet, einvernehmlich beschlossen und vom BeLVIS in Kraft gesetzt werden.

Anschließend sind weiterführend Prüf- und Kontrollbefugnisse des/ der BeLVIS erforderlich, um die Einhaltung und Umsetzung der ressortübergreifenden Sicherheitsrichtlinien und -standards zu gewährleisten. Dies gilt insbesondere bei der Nutzung von zentralen (ressortübergreifenden) Diensten, Fachverfahren, Systeme und Infrastrukturen. In diesem Kontext soll die Weisungsbefugnis des/ der BeLVIS bei besonderen IT-Sicherheitslagen oder bei ressortübergreifenden Sicherheitsvorfällen greifen. Diese Befugnisse gelten nicht für behördenspezifische Fachverfahren, Systeme oder Infrastrukturen.

Der neu geschaffene rechtliche Rahmen bildet zusätzlich die Voraussetzung für den adäquaten Ausbau von (zentralen) Sicherheitslösungen und -diensten zur Stärkung der Detektions- und Reaktionsfähigkeit durch die Sicherheitsteams bei IT-Angriffen.

IV.1 Stärkung der Sicherheitsteams: Verbesserung der Detektions- und Reaktionsfähigkeit

Das CERT M-V ist als unabhängige und neutrale Stelle für viele Fragen der Informationssicherheit weiterzuentwickeln und seine Zielgruppe auf die Kommunalverwaltung auszuweiten. Das bedeutet, dass die bisherige Bereitstellung von CERT-Basisdiensten auf Grundlage der Unterteilung zwischen primärer und sekundärer Zielgruppe aufgehoben wird.

Als Voraussetzung ist im Zusammenhang mit dem Informationssicherheitsgesetz in der Kommunalverwaltung eine Informationssicherheitsorganisation aufzubauen, die eng mit dem CERT M-V zusammenarbeitet.

Neben seinen bisherigen koordinierenden und beratenden Aufgaben- und Tätigkeiten soll das CERT M-V in das Modell eines internen CERTs mit reaktiven und agierenden Aufgaben und Tätigkeiten überführt werden. Hierzu ist es erforderlich dem CERT M-V im Rahmen seines neuen Mandats erweiterte Rechte und Befugnisse einzuräumen.

In diesem Zusammenhang sind ebenfalls die datenschutzrechtlichen Rahmenbedingungen für das CERT M-V zu schaffen. Diese sind im Rahmen mit der Sicherheitsvorfallbehandlung erforderlich, weil die fehlende Einwilligung der Betroffenen nicht dazu führen darf, dass die Ursachenanalyse und somit die Ableitung von ad-hoc Sicherheitsmaßnahmen aus datenschutzrechtlichen Gründen verwehrt bleibt.

Des Weiteren muss das CERT M-V für eine zeitgerechte Erkennung von IT-Angriffen mit neuen, unterstützenden sowohl staatlichen als auch kommunalen Einheiten, wie beispielsweise durch Security Operation Center (SOC) bei den IT-Landes- und Kommunaldienstleistern (RZ-Betreibern) und/ oder durch IT-Forensik-Einheiten unterstützt werden.

Dieses setzt voraus, dass alle öffentlichen Stellen, die IT-Landesverwaltungsdienstleisterin sowie alle kommunalen IT-Dienstleister in die rechtssichere Lage versetzt werden müssen, IT-Angriffe auf ihre eigenen informations- und kommunikationstechnischen Systeme und Infrastrukturen detektieren und abwehren zu dürfen. Die Aufgabe zur Detektion und zur Reaktion von IT-Angriffen sollen interne Security Operation Center wahrnehmen, deren Befugnisse zum Schutz der Landes- und der Kommunalverwaltung erweitert werden müssen. Sicherheitsrelevante Protokoll- oder Ereignisdaten sollen länger als bisher gespeichert und vermehrt auch unpseudonymisiert verarbeitet werden dürfen.

In diesem Kontext fällt dem CERT M-V die herausgehobene Aufgabe zu, alle wesentlichen sicherheitsrelevanten Daten zu aggregieren und somit revolvierend ein ganzheitliches IT-Sicherheitslagebild der öffentlichen Verwaltung des Landes erstellen zu können.

Das aufgezeigte Ziel soll über eine Akkreditierung durch eine Trusted-Introducer-Zertifizierung[1] bestätigt werden.

IV.2 Meldepflichten, Standardisierung und Kontrollbefugnisse

Ebenso wird die Landesregierung die Meldepflichten bei Sicherheitsvorfällen und die Verpflichtung zur Einhaltung beziehungsweise Umsetzung von Mindestsicherheitsstandards bei der gemeinsamen Nutzung von informations- und kommunikationstechnischer Systeme und Infrastrukturen ausweiten.

Durch das Informationssicherheitsgesetz wird die »Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung Mecklenburg-Vorpommern« (IS-Leitlinie M-V) auf eine höhere Stufe der Rechtsnormen gehoben. Der/ die BeLVIS soll durch das Informationssicherheitsgesetz umfangreiche Kontroll- und Prüfbefugnisse zur Einhaltung und Umsetzung der Mindestsicherheitsstandards gegenüber allen Behörden und anderen Einrichtungen der Landesverwaltung erhalten. Von den Kontroll-, Prüf- und Weisungsbefugnissen werden ebenfalls die IT-Dienstleister erfasst.

[1] Eine Trusted-Introducer-Zertifizierung bestätigt den Reifegrad eines Computer Emergency Response Teams (CERT) nach standardisierten Kriterien; vgl. https://www.trusted-introducer.org.

Analoge Befugnisse für die Kommunalverwaltung soll auch der/die Beauftragte der Kommunalverwaltung für Informationssicherheit (BeKVIS) für die kommunalen Stellen erhalten.

IV.3 Vernetzung von Sicherheitskonzepten

Mit der Verwaltungsdigitalisierung verschwinden die föderalen Grenzen. Bürgerinnen und Bürger nutzen Verwaltungsdienstleistungen über Portallösungen oder mobile Apps, die nicht zwingend im eigenen Bundesland entwickelt und betrieben werden müssen. Die steigende Vielzahl, die Komplexität und die Vernetzung der IT-Systeme der öffentlichen Verwaltung zur Erbringung von digitalen Verwaltungsdienstleistungen machen es erforderlich, auch die jeweiligen Sicherheitskonzepte miteinander zu vernetzen. Für eine über die föderalen Grenzen hinausgehende aktive Zusammenarbeit, insbesondere mit dem BSI und mit spezialisierten Sicherheitsexperten anderer Bundesländer auf dem Gebiet der Informationssicherheit, bedarf es einer Rechtsgrundlage.

Eine gesetzliche Regelung ist insbesondere dann erforderlich, wenn zur gemeinsamen Abwehr von Cyber- beziehungsweise IT-Angriffen dauerhaft sicherheitsrelevante Daten ausgetauscht und hierfür Dienstleistungen in Anspruch genommen werden.

V. Ausblick

In der gegenwärtigen Informationssicherheitsarchitektur des Landes begegnet die Landesregierung den Bedrohungen aus dem Cyberraum durch Maßnahmen der präventiven und passiven Abwehr von Cyber- beziehungsweise IT-Angriffen. Für die Landesregierung ist dieser präventive Ansatz, beispielsweise durch die Sensibilisierung von Landes- und Kommunalbeschäftigen, ein wichtiger Baustein.

Im Bereich des passiven Ansatzes bilden die privatrechtlichen landes- und kommunalen IT-Dienstleister, beispielsweise durch Härtung eigener informations- und kommunikationstechnischer Systeme oder durch den Einsatz von Firewalls, einen zentralen und wirksamen Baustein eines ganzheitlichen Informationssicherheitsansatzes.

Dennoch sind Cyber- beziehungsweise IT-Angriffe vorstellbar gegen die die Maßnahmen der präventiven und passiven Abwehr alleine keinen hinreichenden Schutz bieten können. Das gilt solange, wie Informations- und Kommunikationstechnik fehlerbehaftet ist und somit Angriffe erst möglichen. Dies kann beispielweise bei gezielten staatlichen Angriffen, bei Cyberspionage- oder Sabotageoperationen der Fall sein. Um nach der Detektion derartiger Angriffe weitergehende Möglichkeiten der Abwehr zu haben, kann das Ergreifen von aktiven Maßnahmen notwendig sein.

Mit aktiver Abwehr sind solche Maßnahmen zu verstehen, die auf fremde informations- und kommunikationstechnische Systeme einwirken, um somit einen bevorstehenden IT-Angriff zu verhindern oder einen solchen zu beenden. In Deutschland sind für Maßnahmen der (digitalen) Gefahrenabwehr grundsätzlich die Länder zuständig.

Cyber- beziehungsweise IT-Angriffe stellen jedoch vielfach eine länderübergreifende Gefahr dar und haben zunehmend eine internationale Dimension. Es ist zudem auch ein äußerst hohes technisches Know-how erforderlich, das effektiv nur an bestimmten Stellen in

Deutschland vorhanden ist oder aufgebaut werden kann. Dem Bund stehen nach geltendem Verfassungsrecht nur in bestimmten Bereichen gefahrenabwehrrechtliche Sonderzuständigkeiten zu, wie zum Beispiel bei der Bahnsicherheit. In anderen Bereichen kann der Bund aufgrund der Landeszuständigkeit selbst bei einem bedeutenden, komplexen oder länderübergreifenden IT-Angriff, die eines nationalen Handelns bedarf, nicht selbst gefahrenabwehrend tätig werden. Diese bestehende Zuständigkeitsaufteilung wird der aktuellen und der sich absehbar weiter verschärfenden Bedrohungslage nicht gerecht. Cyberbedrohungen in Deutschland können somit dauerhaft und nachhaltig nicht begegnet werden. Vor diesem Hintergrund ist im Rahmen des Gesetzgebungsverfahrens zu prüfen, wie die Zusammenarbeit von Bund und Ländern bei der Cyberabwehr strukturell neu geordnet werden kann.

In der Gesamtsicht soll mit den aufgezeigten Grundsätzen, den fünf Handlungsfeldern sowie den hieraus abgeleiteten und umzusetzenden (Sicherheits-)Maßnahmen den Bürgerinnen und Bürger signalisiert werden, dass Informationssicherheit, Datensicherheit und Datenschutz einen hohen Stellenwert bei der Digitalisierung in der Landes- und Kommunalverwaltung besitzen.

Die konkrete Umsetzung der genannten Maßnahmen soll in einem Umsetzungsplan aufgezeigt werden, der neben den maßnahmenbezogenen Zuständigkeiten auch die strategische Zeitplanung bis 2024 enthalten soll.