LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 6/3493**
6. Wahlperiode **03.12.2014**

UNTERRICHTUNG

durch die Landesregierung

Bürgernahe Verwaltung - papierlose Kommunikation erfordert sichere IT-Strukturen

Zugeleitet mit Schreiben des Chefs der Staatskanzlei vom 1. Dezember 2014 gemäß Beschluss des Landtages vom 16.05.2014 (Drucksachen 6/2928 und 62969); federführend ist das Ministerium für Inneres und Sport.

Inhaltsverzeichnis:

1 Prüfauftrag

Der Landtag hatte in der Sitzung vom 16.05.2014 folgenden Beschluss gefasst[1]:

1. Der Landtag stellt fest,

   a) eine bürgernahe, moderne Verwaltung ist gekennzeichnet von einem einfachen elektronischen Zugang der Bürger zu den Behörden. Der papierlosen Antragsbearbeitung gehört die Zukunft. Sie ermöglicht eine rasche und transparente Erledigung der Anliegen.
   b) die stetig voranschreitende technologische Entwicklung erfordert eine kontinuierliche Betreuung der IT-Systeme in der Verwaltung sowohl des Landes als auch der Kommunen. Daten und Kommunikation müssen effektiv gegen Manipulation, unberechtigten Zugriff und Datenverlust geschützt werden.

2. Die Landesregierung wird gebeten zu prüfen, ob unter Einbeziehung des Städte- und Gemeindetages Mecklenburg-Vorpommern und des Landkreistages Mecklenburg-Vorpommern aufeinander abgestimmte IT-Sicherheitskonzepte, aufbauend auf den Vorgaben der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ erarbeitet werden können, damit die IT-gestützten Geschäftsprozesse in den Kommunen unter besonderer Berücksichtigung der Bürgernähe, der Effektivität und Effizienz des Verwaltungshandels gestärkt werden können.

3. Die Landesregierung wird aufgefordert, den Landtag über entsprechende Prüfergebnisse, insbesondere hinsichtlich möglicher fachlicher, personeller und finanzieller Anforderungen an Land und Kommunen, noch im Jahr 2014 zu unterrichten, gegebenenfalls in Form eines Zwischenberichtes.“

Gemäß diesem Auftrag hat die Landesregierung organisatorische Empfehlungen und mögliche Unterstützungsleistungen zur Erhöhung der Informationssicherheit im Bereich der Kommunalverwaltung geprüft. Dieser Bericht gibt einen Überblick, welche konkreten Maßnahmen im Zuge der Bearbeitung des Prüfauftrags identifiziert wurden und welche personellen und finanziellen Aufwände im Falle der Umsetzung zu berücksichtigen wären.

2 Zusammenfassung

Wie in der Begründung zur Drucksache 6/2928 des Landtags dargelegt worden ist, steigen mit dem zunehmenden Grad der elektronischen Verwaltung auch die Anforderungen an die Sicherheit der Daten. Um die Sicherheitsbelange in geeigneter Weise zu berücksichtigen, können einmalige Investitionen in die IT-Sicherheit allenfalls temporär erfolgreich sein. Die Erarbeitung von aufeinander abgestimmten Sicherheitskonzepten der Landes- und Kommunalverwaltung kann daher lediglich ein erster notwendiger Zwischenschritt sein.

[1] Landtagsdrucksachen 6/2928 und 6/2969.

Die Landesregierung hat dies in der Auslegung des im Abschnitt 1 zitierten Prüfauftrags berücksichtigt und nicht nur geprüft, ob künftig aufeinander abgestimmte Sicherheitskonzepte erarbeitet werden können, sondern zeigt in diesem Bericht die Möglichkeit auf, wie eine geeignete Integration der Kommunalverwaltung in den im „Konzept für den Aufbau und Betrieb eines Informationssicherheitsmanagements in der Landesverwaltung von Mecklenburg-Vorpommern“ beschriebenen Sicherheitsprozess erfolgen könnte. Dies ist aus Sicht der Landesregierung notwendig, damit etwaige Unterstützungsleistungen auch tatsächlich in der notwendigen Weise greifen können. Hierzu ist auch auf der Seite der Kommunalverwaltung zunächst der Aufbau einer Informationssicherheitsorganisation - wie in der Grafik im Abschnitt 4.1.4 dargestellt - erforderlich. Vor diesem Hintergrund enthält der vorliegende Bericht der Landesregierung die nachfolgend genannten organisatorischen Empfehlungen:

1. Die Landesregierung empfiehlt der Kommunalverwaltung, in allen Behörden IT-Sicherheitsbeauftragte zu benennen. Sie werden unter anderem auch als Ansprechpartner für behördenübergreifende Abstimmungen im gemeinsamen Informationssicherheitsprozess benötigt.

2. Die Landesregierung empfiehlt darüber hinaus, eine zentrale Beauftragte beziehungsweise einen zentralen Beauftragten der Kommunalverwaltung für Informationssicherheit (BeKVIS) einzusetzen, um den Informationssicherheitsprozess innerhalb der Kommunalverwaltung zu koordinieren sowie die Interessen der kommunalen Körperschaften zu bündeln und in der ebenenübergreifenden Zusammenarbeit in geeigneter Weise zu vertreten.

3. Die Landesregierung empfiehlt ferner, eine „Lenkungsgruppe für die Informationssicherheit in den Kommunen“ aus Vertretern des eGo-MV, Städte- und Gemeindetags, Landkreistags, Innenministeriums, Büros kooperatives E-Government und der DVZ M-V GmbH als zentrales Steuerungsgremium zur Gewährleistung eines gemeinsamen Basisniveaus für Informationssicherheit in den kommunalen Körperschaften und zur Zusammenarbeit mit der Kommission für Informationssicherheit der Landesverwaltung zu etablieren.

Darauf aufbauend können der Kommunalverwaltung die nachfolgend aufgeführten Unterstützungsleistungen zur Verfügung gestellt werden:

1. Um die Kommunalverwaltung bei der Erstellung, Verwaltung und Fortschreibung von Sicherheitskonzepten entsprechend dem IT-Grundschutz zu unterstützen, bietet die Landesregierung der Kommunalverwaltung die Mitnutzung des bei der DVZ M-V GmbH im Auftrag des Ministeriums für Inneres und Sport betriebenen zentralen Managementsystems für Informationssicherheit (ISMS) an. Die Nutzung eines zentralen ISMS durch die Landes- und Kommunalverwaltung würde zugleich bewirken, dass die Sicherheitskonzepte optimal aufeinander abgestimmt wären und etwaige Unterstützungsleistungen zur Erstellung und Fortschreibung von Sicherheitskonzepten rationell von zentraler Stelle erbracht werden könnten.

2. Um den bestehenden Nachholbedarf bei der Erstellung von Sicherheitskonzepten, insbesondere hinsichtlich der übergreifenden Verfahren, in möglichst kurzer Zeit aufzuarbeiten, könnte die DVZ M-V GmbH mit der Erstellung beziehungsweise Fortschreibung von Muster-Sicherheitskonzepten für diese Verfahren beauftragt werden. Dies würde in enger Abstimmung mit den Verfahrensbetreibern erfolgen.

3. Um bereits zeitnah eine wirksame Erhöhung des Sicherheitsniveaus in den Kommunen zu erreichen, könnten zentrale Unterstützungsleistungen des eGo-MV zur Umsetzung der Sicherheitskonzepte in Anspruch genommen werden.

4. Im Rahmen der Nutzung gemeinsamer zentraler Sicherheitssysteme und IT-Verfahren können die Kommunen Basisleistungen des zentralen Computer-Notfall-Teams der Landesverwaltung wie die Sicherheitsvorfallbehandlung, den Warn- und Informationsdienst und das zentrale Web-Portal mitnutzen.

5. Durch eine Beteiligung der Kommunalverwaltung am Computer-Notfall-Team der Landesverwaltung könnte darüber hinaus erreicht werden, dass die Basisleistungen nicht nur im Rahmen der Nutzung von gemeinsamen zentralen Sicherheitssystemen und IT-Verfahren erbracht werden, sondern vollumfänglich wie dies für die Landesverwaltung erfolgt. In diesem Fall würde die Kommunalverwaltung unter anderem auch in das Informationssicherheitsmanagement der Landesverwaltung und damit in das Meldeverfahren für Sicherheitsvorfälle sowie in das Berichtswesen über durchgeführte proaktive und nachhaltige IT-Sicherheitsmaßnahmen einbezogen werden und zentrale Sensibilisierungs- und Schulungsmaßnahmen mitnutzen können.

6. Um sich sowohl organisatorisch als auch finanziell zu entlasten und Fragen der IT-Sicherheit und des Datenschutzes nicht allein bewältigen zu müssen, sollten zentral zur Verfügung stehende IT-Verfahren genutzt werden. Da die erzielbaren Synergieeffekte direkt vom Nutzungsgrad abhängig sind, sollte die Nutzung von zentral zur Verfügung stehenden Verfahren und Infrastrukturen verpflichtend vorgeschrieben werden.

Für die vollständige Umsetzung der oben genannten, zentralen Maßnahmen werden Haushaltsmittel in Höhe von jährlich circa 840.000 € benötigt. Mit der Entscheidung der kommunalen Seite, ob und inwieweit sie das Angebot der Landesregierung und die vorgeschlagenen Maßnahmen annimmt, muss zugleich darüber entschieden werden, wie deren Finanzierung sichergestellt werden soll. Hierbei ist zu berücksichtigen, dass die Sicherheit der eigenen IT-Systeme originäre Aufgabe der Kommunen ist. Für die Umsetzung von kooperativen Lösungen und die Umsetzung einheitlicher Standards unterstützt das Land die Kommunen im Rahmen seiner Möglichkeiten. Zusätzliche Haushaltsmittel aus dem Landeshaushalt können hierfür jedoch nicht zur Verfügung gestellt werden.

3 Ausgangssituation

3.1 Ausgangssituation in der Landesverwaltung

Die Landesregierung versteht die Gewährleistung der Informationssicherheit inzwischen nicht nur als wichtige Aufgabe, sondern als einen andauernden Prozess. Dadurch soll erreicht werden, dass die drei Grundwerte der Informationssicherheit - Vertraulichkeit, Verfügbarkeit und Integrität - auch bei sich verändernden Gefährdungslagen bestmöglich geschützt sind. Bei der Einführung, Umsetzung und dem Betrieb von IT-Anwendungen oder IT-Infrastrukturmaßnahmen stehen Fragen der Informationssicherheit regelmäßig im Fokus. Hierbei erweisen sich die konsequente Anwendung der Grundschutzstandards des Bundesamts für die Sicherheit in der Informationstechnik (BSI) sowie der Betrieb eines zentralen GS-Tool-Servers[2] für die Landesverwaltung als effiziente Mittel bei der Umsetzung des IT-Grundschutzes.

Die Landesregierung ist sich der Tatsache bewusst, dass die Informationssicherheit, insbesondere bei übergreifenden IT-Verfahren und zentralen Infrastrukturkomponenten, nur in enger Zusammenarbeit mit allen Beteiligten realisiert werden kann. Um dem Rechnung zu tragen, bestehen seit langem verschiedene ressortübergreifende Sicherheitsteams und Revisionskommissionen. Gleichwohl reichen die bisher getroffenen Maßnahmen fortan nicht mehr aus, um den erheblich gestiegenen Anforderungen an die Informationssicherheit auch künftig gerecht werden zu können Dies hat die Landesregierung bereits erkannt und ist daher derzeit aktiv mit der Umsetzung der vom IT-Planungsrat im März 2013 beschlossenen Informationssicherheitsleitlinie[3] befasst. Im Juni 2014 hat das Kabinett dazu eine gemeinsame IT-Sicherheitsstrategie der Ressorts der Landesregierung beschlossen. In diesem Zusammenhang wurde unter anderem eine „Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern“ (IS-Leitlinie M-V) erlassen, mit der insbesondere Festlegungen für ein landesweit einheitliches Mindestsicherheitsniveau und den Aufbau eines ressortübergreifenden Informationssicherheitsmanagements getroffen wurden. Mit dem ressortübergreifenden Informationssicherheitsmanagement wird in der Landesverwaltung ein kontinuierlicher, übergreifend ausgelegter Prozess zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Anwendungen und IT-Systemen eingeführt. Dieser Prozess beinhaltet alle Verantwortlichkeiten und Aufgaben, mit denen ein angemessenes Sicherheitsniveau erreicht und gehalten wird. Dies betrifft insbesondere Meldepflichten bei Sicherheitsvorfällen, festgelegte Abläufe zur ressortübergreifenden Behandlung von Sicherheitsvorfällen, die Durchführung von Informationssicherheitsrevisionen, regelmäßige Berichtspflichten und die Durchführung von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit in den Behörden. Ein Beauftragter der Landesverwaltung für Informationssicherheit wird den Informationssicherheitsprozess koordinieren und die Einhaltung von ressortübergreifenden Regelungen und Beschlüssen zur Informationssicherheit kontrollieren. Zugleich wird er die zu etablierende Kommission für Informationssicherheit der Landesverwaltung leiten.

[2] Das GS-Tool (Grundschutz-Tool) ist ein Softwaresystem zur werkzeugunterstützten Erstellung von Sicherheitskonzepten nach dem Vorgehensmodell des BSI.

[3] Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung, Beschluss 2013/01 des IT-Planungsrats vom 08.03.2013.

Diese Kommission ist insbesondere für die Erarbeitung und Fortschreibung von IT-Sicherheitsstandards und Regelungen zur Informationssicherheit, die Entwicklung und Überwachung von Kennzahlen zur Bewertung der Informationssicherheit und die Kontrolle der Umsetzung von IT-Sicherheitsmaßnahmen bei übergreifenden Verfahren und zentralen Infrastrukturkomponenten verantwortlich. In der Kommission sind die IT-Sicherheitsbeauftragten der Staatskanzlei und der Ressorts ständig vertreten. Darüber hinaus werden bei den Entscheidungen der Kommission auch der Städte- und Gemeindetag M-V und der Landkreistag M-V beteiligt. An den Sitzungen der Kommission können ferner der Landesbeauftragte für Datenschutz und Informationsfreiheit M-V, der Landesrechnungshof M-V und die Landtagsverwaltung M-V teilnehmen und somit an Entscheidungsfindungen mitwirken.
Als weiteren wesentlichen Schritt sieht die IS-Leitlinie M- V die Schaffung eines Kompetenzzentrums für IT-Sicherheitsfragen vor, welches als CERT M-V[4] etabliert werden und Dienstleistungen zur Behandlung und Vermeidung von Sicherheitsvorfällen zentral für die Verwaltung zur Verfügung stellen soll. Mit dem CERT M-V soll die Landesverwaltung von Mecklenburg-Vorpommern in die Lage versetzt werden, bei IT-Angriffen, IT-Krisen und in Notfällen schnell, effizient und umfassend zu handeln beziehungsweise geeignete Vorsorgemaßnahmen gegen solche Ereignisse zu treffen. Das CERT M-V ist für die Planung und Umsetzung von vorbeugenden, reaktiven und nachhaltigen Maßnahmen im Rahmen des Informationssicherheitsmanagements des Landes zuständig. Es soll das Informationssicherheitsmanagement unter anderem durch die Bereitstellung von Sicherheitsinformationen, die Behandlung von Sicherheitsvorfällen sowie die Sensibilisierung von Beschäftigten unterstützen.
Mit dem Aufbau des CERTs M-V hat die Landesregierung bereits begonnen. Der Pilotbetrieb beginnt Anfang 2015, und der Übergang in den Wirkbetrieb soll Anfang 2017 erfolgen.
Obwohl das Computer-Notfall-Team in erster Linie für Landesverwaltung etabliert wird, sieht das Konzept auch Partizipationsmöglichkeiten für die kommunale Ebene vor. Diese sind in den Darlegungen des Abschnitts 4 mit berücksichtigt.

3.2 Ausgangssituation in der Kommunalverwaltung

Für die nachfolgenden Darlegungen zum Stand der Informationssicherheit in den Kommunen wurden folgende Informationen ausgewertet:

- Landesbeauftragter für Datenschutz und Informationsfreiheit; Elfter Tätigkeitsbericht gemäß § 33 Absatz 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V); 17.03.2014
- Landesrechnungshof M-V; Mitteilungen über die Prüfung der Integrität und Stabilität von IT-Systemen bei Kommunen - System- und Programmprüfung; 19.06.2014
- Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“; IT Sicherheit und Datenschutz in den Kommunen - eine Bestandsaufnahme; 07.05.2014

[4] CERT steht für Computer Emergency Response Team und bedeutet übersetzt Computer-Notfall-Team.

Nach Einschätzung des Landesbeauftragten für Datenschutz und Informationsfreiheit mangelt es in vielen Kommunen an „elementaren Voraussetzungen für die Gewährleistung der Informationssicherheit und des Datenschutzes“[5]. Der Landesrechnungshof stellt dazu in seiner oben genannten Prüfungsmitteilung fest, dass in den Kommunen „IT-Sicherheitskonzepte und Risikoabwägungen für die eingesetzten Verfahren nur vereinzelt vorliegen“ und „ein aktives Risikomanagement nur ansatzweise stattfinden“ würde. Die im Zuge der Prüfung vorgelegten Sicherheitskonzepte wären „teilweise mangelhaft“ gewesen und Serverräume würden „oft nicht den Anforderungen des Bausteins B 2.4 des IT-Grundschutzkataloges des BSI“ entsprechen[6]. Auch der Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“ (eGo-MV) konstatiert in seiner oben genannten Bestandsaufnahme, die IT-Sicherheit in den Kommunen würde „überwiegend stiefmütterlich behandelt“ werden und die Sensibilität für das Thema IT-Sicherheit“ müsse „insbesondere in den Verwaltungsleitungen verbessert werden“. Gleichwohl wären aber „grundlegende Sicherheitsmaßnahmen wie Gebäude-, Raumschutz, Firewall und Virenschutz in allen Verwaltungen vorhanden“ und „Zutritts- und Zugriffsrechte weitgehend aufgabenbezogen zugeordnet“. Auch hätte sich „das Datenschutz- und IT-Sicherheitsniveau in den letzten sechs Jahren“ - zumindest bezogen auf die durch ihn betreuten Kommunen - „wesentlich verbessert“[7].
Der eGo-MV bietet seinen Mitgliedern, aber auch seinen Nichtmitgliedern, in zunehmendem Maße zentrale Lösungen beziehungsweise Infrastrukturen zur Mitnutzung an. Daneben engagiert er sich schon seit 2007 für Unterstützungsleistungen im Bereich Datenschutz. Derzeit nutzen über 50 Verwaltungen die Datenschutzbeauftragten des Zweckverbandes als „behördlichen Datenschutzbeauftragten“ nach § 20 Datenschutzgesetz M-V (DSG M-V). Dabei nehmen die Datenschutzbeauftragten des Zweckverbandes in ihrer Rolle als behördliche Datenschutzbeauftragte alle Aufgaben gemäß dem DSG M-V wahr. Weiterhin verfügt ein Mitarbeiter aus diesem Bereich über die Qualifizierung als IT-Sicherheitsbeauftragter. So bietet der Zweckverband seinen Mitgliedern unter anderem auch ein Rahmensicherheitskonzept an, welches durch die Kommunen als Vorlage für die Erstellung eigener Sicherheitskonzepte verwendet werden kann. Es orientiert sich am BSI-Grundschutz und stellt einen Rahmen dar, nach dem alle zu treffenden Regelungen und Maßnahmen durch die Behörden schriftlich dokumentiert und für die tägliche Arbeit genutzt werden können. Leider haben dieses Angebot bisher nur wenige Mitglieder genutzt. Der Zweckverband plant aber, den Kommunalverwaltungen sowohl weitere Unterstützungsleistungen zur Umsetzung der IT-Sicherheitskonzeptionen als auch die Nutzung eines gemeinsamen IT-Sicherheitsbeauftragten zentral anzubieten. Das daraus sich ergebende Nutzenpotenzial kann den offenkundig bestehenden, akuten Handlungsbedarf, der sich aus der hier beschriebenen Sachlage ergibt, sicherlich nur zum Teil abdecken. Insoweit schlussfolgert auch der Landesrechnungshof in seiner Prüfungsmitteilung: „Die Kommunen sollten prüfen, ob es tatsächlich erforderlich und wirtschaftlich ist, die unterschiedlichsten IT-Systeme selbst zu betreiben“, denn „die Potenziale zur Zusammenarbeit auf dem Gebiet des IT-Betriebs“ und einer „weitergehenden Nutzung des Zweckverbands“ sind „bei Weitem nicht ausgeschöpft“[8].
Entsprechende Überlegungen sind in den Darlegungen des Abschnitts 4 mit berücksichtigt.

---

[5] Landesbeauftragter für Datenschutz und Informationsfreiheit; Elfter Tätigkeitsbericht gemäß § 33 Absatz 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V), Abschnitt 6.4.6; 17.03.2014.

[6] Landesrechnungshof M-V; Mitteilungen über die Prüfung der Integrität und Stabilität von IT-Systemen bei Kommunen – System- und Programmprüfung, Textziffern (6) und (7); 19.06.2014.

[7] Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“; IT Sicherheit und Datenschutz in den Kommunen – eine Bestandsaufnahme; 07.05.2014.

[8] Landesrechnungshof M-V; Mitteilungen über die Prüfung der Integrität und Stabilität von IT-Systemen bei Kommunen – System- und Programmprüfung, Textziffer (150); 19.06.2014.

4 Maßnahmen zur Erhöhung der Informationssicherheit

Angesichts der steigenden Verflechtung der IT-Systeme durch die Nutzung von ebenenübergreifenden Verfahren und gemeinsamen Basiskomponenten beziehungsweise -diensten kann die Informationssicherheit heute allein mit lokal begrenzten Schutzmaßnahmen nicht mehr gewährleistet werden. Stattdessen wird eine stärkere übergreifende Zusammenarbeit immer notwendiger. Diese Erkenntnis spiegelt sich unter anderem in dem Vorhaben zum Aufbau eines Informationssicherheitsmanagements in der Landesverwaltung von Mecklenburg-Vorpommern (ISM M-V) wider, welchem das Kabinett in seiner 21. Sitzung am 10.06.2014 zugestimmt hat. Demnach zählen die kommunalen Körperschaften zur sogenannten sekundären Zielgruppe des CERTs M-V und können dadurch bereits jetzt ausgewählte CERT-Dienste im Hinblick auf zentrale Sicherheitssysteme oder gemeinsame Verfahren kostenneutral mitnutzen. Unabhängig davon hat die Landesregierung den im Abschnitt 1 zitierten Prüfauftrag zum Anlass für weitergehende Überlegungen zur Einbeziehung der Kommunen in das Informationssicherheitsmanagement der Landesverwaltung genommen. Da Informationssicherheit nicht nur eine Frage der Technik ist, sondern auch stark von den organisatorischen und personellen Rahmenbedingungen abhängt, beginnt die nachfolgende Betrachtung zunächst mit grundlegenden organisatorischen Empfehlungen, bevor im Weiteren konkrete Unterstützungsleistungen, die vorrangig auf dem ISM M-V basieren, beschrieben werden.
Ob und inwieweit die Kommunalbehörden diese Maßnahmen aufgreifen werden, ist zum einen davon abhängig, ob der aus Sicht der Landesregierung identifizierte Handlungs- und Unterstützungsbedarf dort ähnlich eingeschätzt wird und zum anderen auch maßgeblich davon, ob zur Finanzierung der Leistungsangebote Haushaltsmittel zur Verfügung stehen werden. Für die Umsetzung von kooperativen Lösungen und die Umsetzung einheitlicher Standards unterstützt das Land die Kommunen im Rahmen seiner Möglichkeiten. Gleichwohl ist zu berücksichtigen, dass die Sicherheit der eigenen IT-Systeme originäre Aufgabe der Kommunen ist.

4.1 Organisatorische Empfehlungen

Um das zur Gewährleistung der Informationssicherheit notwendige Zusammenwirken aller Beteiligten in einem ressortübergreifenden Informationssicherheitsmanagement zu ermöglichen, wird im Bereich der Landesverwaltung gegenwärtig die im „Konzept zum Aufbau und Betrieb eines Informationssicherheitsmanagements in der Landesverwaltung von Mecklenburg-Vorpommern“ (ISM-Konzept) näher beschriebene Informationssicherheitsorganisation aufgebaut. Damit auch im Bereich der Kommunalverwaltung ein angemessenes Sicherheitsniveau ermöglicht werden kann, reichen technische Unterstützungsleistungen, die seitens der Landesverwaltung zur Verfügung gestellt werden, allein nicht aus. Stattdessen ist eine ähnliche Sicherheitsorganisation auch auf der Seite der Kommunalverwaltung erforderlich, um die Aktivitäten untereinander und mit der Landesregierung wie erforderlich abzustimmen und ein koordiniertes Vorgehen zu erreichen.

4.1.1 Ernennung von IT-Sicherheitsbeauftragten

Nach den BSI-Grundschutz-Standards (100-1 und 100-2) soll in jeder Institution eine IT-Sicherheitsbeauftragte beziehungsweise ein IT-Sicherheitsbeauftragter benannt werden, die beziehungsweise der für alle Fragen rund um die Informationssicherheit in der Organisation zuständig ist. Sie beziehungsweise er sollte organisatorisch unabhängig sein und ein unmittelbares Vortragsrecht bei der Behördenleitung haben.

Zu den Aufgaben von IT-Sicherheitsbeauftragten gehört insbesondere:

- die Erstellung von Sicherheitskonzepten zu koordinieren,
- den Realisierungsplan für Sicherheitsmaßnahmen zu erstellen und ihre Umsetzung zu initiieren und zu überprüfen,
- der Leitungsebene über den Status der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- sicherheitsrelevante Vorfälle zu untersuchen und
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und zu koordinieren.

Die Landesregierung empfiehlt der Kommunalverwaltung, in allen Behörden IT-Sicherheitsbeauftragte zu benennen. Sie werden unter anderem auch als Ansprechpartner für behördenübergreifende Abstimmungen im gemeinsamen Informationssicherheitsprozess benötigt.

In diesem Zusammenhang ist anzumerken, dass gemäß der Informationssicherheitsleitlinie des IT-Planungsrats diese und andere Vorgaben des IT-Grundschutzes im Falle des Einsatzes von ebenenübergreifenden Verfahren[9] ohnehin schon jetzt für die Kommunalverwaltung[10] gelten. Um die bei den einzelnen Kommunalbehörden anfallenden Personalaufwände mit Hilfe von Synergieeffekten zu minimieren, könnten nach Auffassung der Landesregierung gemeinsame IT-Sicherheitsbeauftragte eingesetzt werden, die optimalerweise beim eGo-MV angesiedelt sein sollten.

[9] Ebenenübergreifende IT-Verfahren sind IT-Verfahren, die über Verwaltungsgrenzen hinweg angeboten beziehnungsweise genutzt werden.

[10] Siehe Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung, Beschluss 2013/01 des IT-Planungsrats vom 08.03.2013, Abschnitt 2 (Geltungsbereich), Absatz 5.

4.1.2 Einsatz eines Beauftragten der Kommunalverwaltung für Informationssicherheit

Im Rahmen des Aufbaus der Informationssicherheitsorganisation der Landesverwaltung von Mecklenburg-Vorpommern wird unter anderem ein Beauftragter der Landesverwaltung für Informationssicherheit (BeLVIS) bestellt, welcher für die Koordinierung des ressortübergreifenden Informationssicherheitsmanagements zuständig ist und die Einhaltung von ressortübergreifenden Regelungen und Beschlüssen zur Informationssicherheit kontrolliert. Darüber hinaus nimmt er folgende Aufgaben wahr:

- Die Abstimmung, Festlegung und Fortschreibung von landeseinheitlichen IT-Sicherheitsstandards und Regelungen zur Informationssicherheit
- Die Leitung der Kommission für Informationssicherheit der Landesverwaltung und strategische Steuerung des CERTs M-V
- Die Vertretung des Landes in der Arbeitsgruppe Informationssicherheit des IT-Planungsrates und im VerwaltungsCERT-Verbund
- Die Leitung des Krisenmanagements bei besonderen IT-Sicherheitslagen
- Die Erstellung von regelmäßigen und anlassbezogenen IT-Sicherheitslageberichten

Wie im Abschnitt 3.1 dargelegt, gehören die Kommunalbehörden aufgrund der Nutzung gemeinsamer zentraler Sicherheitssysteme und IT-Fachverfahren zur sekundären Zielgruppe des CERTs M-V und sind insoweit auch in das Informationssicherheitsmanagement des Landes mit eingebunden. Um sicherzustellen, dass die Interessen der Kommunen in geeigneter Weise vertreten werden, sollte es auf der Seite der Kommunalverwaltung einen ähnlichen Beauftragten oder eine ähnliche Beauftragte geben. Eine solche Beauftragte beziehungsweise ein solcher Beauftragter der Kommunalverwaltung für Informationssicherheit (BeKVIS) könnte beispielsweise beim eGo-MV angesiedelt sein, als zentraler Anlaufpunkt der Kommunalbehörden für alle Fragen der Informationssicherheit dienen und die kommunalen Interessen gegenüber der Landesregierung und dem CERT M-V bündeln. Eine derartige Schnittstelle zwischen der Landes- und der Kommunalverwaltung wäre erst recht erforderlich, wenn die Kommunalverwaltung zusätzliche Unterstützungsleistungen - wie insbesondere im Abschnitt 4.2.5 beschrieben - in Anspruch nehmen wollte.

Die Landesregierung empfiehlt daher, eine zentrale Beauftragte beziehungsweise einen zentralen Beauftragten der Kommunalverwaltung für Informationssicherheit (BeKVIS) einzusetzen, um den Informationssicherheitsprozess innerhalb der Kommunalverwaltung zu koordinieren sowie die Interessen der kommunalen Körperschaften zu bündeln und in der ebenenübergreifenden Zusammenarbeit in geeigneter Weise zu vertreten.

Sofern eine einvernehmliche Verständigung auf eine zentrale Beauftragte beziehungsweise einen zentralen Beauftragten für Informationssicherheit nicht möglich sein sollte, könnte alternativ gegebenenfalls auch die Benennung sowohl einer oder eines Beauftragten für den Landkreistag als auch einer oder eines Beauftragten für den Städte- und Gemeindetag in Betracht gezogen werden.

4.1.3 Bildung einer Lenkungsgruppe für die Informationssicherheit in den Kommunen

Als weitere Maßnahme im Zuge der Umsetzung des ISM-Konzepts wird im Bereich der Landesverwaltung gegenwärtig die im Abschnitt 3.1 bereits erwähnte „Kommission für Informationssicherheit der Landesverwaltung“ gegründet. Diese Kommission ist zuständig für alle Fragen zur IT-Sicherheit, die im Zusammenhang mit dem Einsatz von übergreifenden Verfahren und zentralen Infrastrukturkomponenten gemeinsam abzustimmen und zu klären sind.
Die Aufgaben der Kommission für Informationssicherheit der Landesverwaltung umfassen insbesondere:

- die Mitwirkung bei der Erarbeitung und Fortschreibung von IT-Sicherheitsstandards und Regelungen zur Informationssicherheit in der Landesverwaltung,
- die Entwicklung und Überwachung von Kennzahlen zur Bewertung der Informationssicherheit,
- die Beratung und Mitwirkung bei der Erstellung von IT-Sicherheitskonzepten für ressortübergreifende Verfahren und zentrale Infrastrukturkomponenten,
- die Kontrolle der Umsetzung von IT-Sicherheitsmaßnahmen bei übergreifenden Verfahren und zentralen Infrastrukturkomponenten,
- die Entscheidung über die Änderung von Sicherheitsmaßnahmen mit ressortübergreifenden Auswirkungen.

Der Städte- und Gemeindetag M-V und der Landkreistag M-V werden an den Entscheidungen der Kommission beteiligt, sofern ihre Belange betroffen sind. Sie sind daher als sogenannte „sonstige Mitglieder“ in der Kommission vertreten. Sobald die beziehungsweise der im Abschnitt 4.1.2 beschriebene Beauftragte der Kommunalverwaltung für Informationssicherheit (BeKVIS) eingesetzt sein wird, wird diese beziehungsweise dieser Beauftragte anstelle der kommunalen Spitzenverbände an den Sitzungen der Kommission teilnehmen. Um dieses Mandat in hinreichend autorisierter Weise wahrnehmen zu können - beispielsweise bei der Mitwirkung an der Erarbeitung und Fortschreibung von Sicherheitsstandards, Regelungen zur IT-Sicherheit und Sicherheitskonzepten für übergreifende Verfahren - ist auf der Seite der Kommunalverwaltung ein ähnliches Gremium wie die Kommission für Informationssicherheit der Landesverwaltung erforderlich. Daher sollte eine Lenkungsgruppe für die Informationssicherheit in den Kommunen gebildet werden, der folgende Mitglieder angehören sollten:

- Der eGo-MV/BeKVIS
- Der Städte- und Gemeindetag (StGT MV)
- Der Landkreistag (LKT MV)
- Das Ministerium für Inneres und Sport/BeLVIS
- Das Büro kooperatives E-Government (BkE)
- Die DVZ M-V GmbH

Die Lenkungsgruppe sollte durch den BeKVIS geleitet werden und insbesondere folgende Aufgaben wahrnehmen:

- Die Abstimmung in Angelegenheiten der Zusammenarbeit mit der Kommission für Informationssicherheit der Landesverwaltung
- Die Abstimmung, Festlegung und Fortschreibung von einheitlichen Mindestsicherheitsstandards in den Kommunalbehörden
- Erarbeitung und Fortschreibung von einheitlichen Regelungen zur Informationssicherheit, Muster-Sicherheitsleitlinien und Muster-Dienstanweisungen für die Kommunalverwaltung
- Die Koordinierung der Erstellung und Fortschreibung von IT-Sicherheitskonzepten für IT-Verfahren der Kommunalverwaltung nach dem „Einer-für-Alle-Prinzip“
- Die Koordinierung von gegenseitigen Sicherheitsaudits beziehungsweise Informationssicherheitsrevisionen in den Kommunalbehörden
- Die Durchführung von zentralen Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit für die Kommunalverwaltung

Auf diese Weise könnte ein Steuerungsgremium geschaffen werden, welches maßgeblich dazu beitragen würde, ein gemeinsames Basisniveau für Informationssicherheit im Bereich der Kommunalverwaltung herzustellen und so das Risiko zu minimieren, dass Sicherheitslücken bei einer Behörde über gemeinsame Netzinfrastrukturen und ebenenübergreifende IT-Verfahren die Sicherheit aller beeinträchtigen.

Die Landesregierung empfiehlt daher, eine „Lenkungsgruppe für die Informationssicherheit in den Kommunen“ aus Vertretern des Zweckverbands Elektronische Verwaltung in Mecklenburg-Vorpommern, Städte- und Gemeindetags, Landkreistags, Innenministeriums, Büros kooperatives E-Government und der DVZ M-V GmbH als zentrales Steuerungsgremium zur Gewährleistung eines gemeinsamen Basisniveaus für Informationssicherheit in den kommunalen Körperschaften und zur Zusammenarbeit mit der Kommission für Informationssicherheit der Landesverwaltung zu etablieren.

4.1.4 Struktur der Informationssicherheitsorganisation

Ausgehend von den in den Abschnitten 4.1.1 bis 4.1.3 gegebenen Empfehlungen ergibt sich folgende Struktur der Informationssicherheitsorganisation der Kommunalverwaltung:

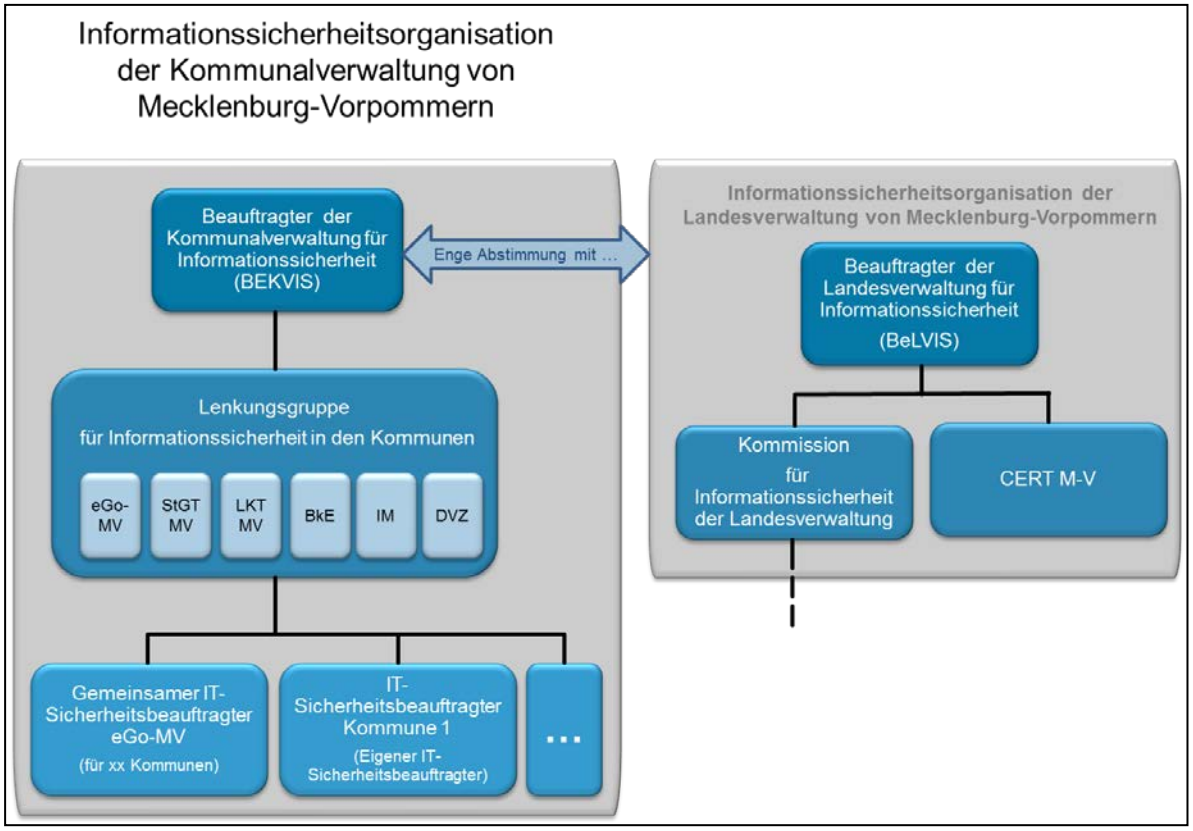

Abbildung 1: Aufbau der Informationssicherheitsorganisation der Kommunalverwaltung des Landes M-V

4.2 Mögliche Unterstützungsleistungen

4.2.1 Mitnutzung des zentralen Managementsystems für Informationssicherheit

Gemäß § 22 Absatz 5 DSG M-V ist für jedes automatisierte Verfahren in einem IT-Sicherheitskonzept festzulegen, in welcher Form die Datenschutzanforderungen umzusetzen sind. Es ist also in diesen Konzepten zu beschreiben, wie durch technische und organisatorische Maßnahmen, die nach dem Stand der Technik und nach der Schutzbedürftigkeit der zu verarbeitenden Daten erforderlich und angemessen sind, der Datenschutz sichergestellt wird. Nach BSI-Grundschutz dient ein Informationssicherheitskonzept „der Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess eines Unternehmens beziehungsweise einer Behörde. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen. Aus diesem Grund muss ein Sicherheitskonzept sorgfältig geplant und umgesetzt sowie regelmäßig überprüft werden.“[11]

[11] Siehe IT-Grundschutz-Kataloge, Maßnahme M 2.195.

Um die Landesverwaltung bei der Erstellung, Verwaltung und Fortschreibung von Sicherheitskonzepten entsprechend dem IT-Grundschutz effizient zu unterstützen, betreibt die DVZ M-V GmbH im Auftrag des Ministeriums für Inneres und Sport ein Managementsystem für Informationssicherheit (ISMS) in Form eines zentralen GS-Tool-Servers, auf dem sowohl die Sicherheitskonzepte der Ressorts als auch die der gemeinsamen zentralen Komponenten und Verfahren gespeichert sind. Durch die im GS-Tool gegebenen Möglichkeiten der Verlinkung, beispielsweise von Systemkomponenten, ermöglicht dies der Landesverwaltung ein hochgradig effizientes Vorgehen bei der Erstellung und Fortschreibung von Sicherheitskonzepten.
Damit auch die Kommunalbehörden fortan von diesen Möglichkeiten profitieren und die daraus sich ergebenden Synergieeffekte nutzen können, bietet die Landesregierung der Kommunalverwaltung die Mitnutzung des ISMS an. Da das BSI die Fortentwicklung des GS-Tools eingestellt hat und die vorliegenden Sicherheitskonzepte daher in absehbarer Zeit auf ein neues ISMS überführt werden, gilt dieses Unterstützungsangebot zugleich für das künftige System.
Die Nutzung eines zentralen ISMS durch die Landes- und Kommunalverwaltung würde zugleich bewirken, dass die Sicherheitskonzepte optimal aufeinander abgestimmt wären und - im Falle von Unterstützungsbedarf bei der Erstellung und Fortschreibung von Sicherheitskonzepten - etwaige Unterstützungsleistungen rationell von zentraler Stelle erbracht werden könnten.

4.2.2 Erstellung von Muster-Sicherheitskonzepten

Vor dem Hintergrund des im Abschnitt 3.2 dargelegten Handlungsbedarfs hinsichtlich der Erstellung von Sicherheitskonzepten bestünde die Möglichkeit - sofern entsprechende Finanzierungsmöglichkeiten gefunden werden - weitergehende Unterstützungsleistungen zur Erstellung von Sicherheitskonzepten zentral zur Verfügung zu stellen. Um diesbezüglich insbesondere hinsichtlich der übergreifenden Verfahren[12] in einem überschaubaren Zeitraum signifikante Fortschritte zu erzielen, könnte die DVZ M-V GmbH mit der Erstellung von Muster-Sicherheitskonzepten für diese IT-Verfahren beauftragt werden. Nach dem Einer-für-Alle-Prinzip würde so beispielsweise zunächst für eine Behörde ein Sicherheitskonzept für ein übergreifendes Verfahren (z. B. BZR/GZR - Bundes-, Gewerbezentralregister; Profil c/s - Fördermittelverwaltung in der Landwirtschaft; ZStV - Zentrales Staatsanwaltschaftliches Verfahrensregister usw.) als Muster erstellt beziehungsweise fortgeschrieben und anschließend als Vorlage für die anderen Behörden zentral zur Verfügung gestellt werden. Die diesbezüglich notwendige Steuerung, welche Sicherheitskonzepte mit welcher Priorität für welche Behörde erstellt werden müssen, sollte durch den Beauftragten der Kommunalverwaltung für Informationssicherheit (BeKVIS) nach Abstimmung mit der Lenkungsgruppe für die Informationssicherheit in den Kommunen erfolgen. Nach erfolgter Bereitstellung der jeweiligen Muster-Sicherheitskonzepte wäre es Aufgabe des BeKVIS zu kontrollieren, ob die erforderliche Nachnutzung in den einzelnen Kommunalbehörden auch tatsächlich und mit der gebotenen Dringlichkeit erfolgt.

[12] Mit „übergreifenden Verfahren“ sind hier sowohl jene Verfahren gemeint, die innerhalb derselben Ebene, aber behördenübergreifend oder ebenenübergreifend genutzt werden, als auch gleiche Verfahren, die lokal in mehreren Behörden im Einsatz sind.

4.2.3 Umsetzung von Sicherheitskonzepten

Das Vorliegen von Sicherheitskonzepten ist erst dann unmittelbar mit der erforderlichen Erhöhung des Sicherheitsniveaus verbunden, wenn die darin beschriebenen Sicherheitsmaßnahmen, die im Übrigen nach dem Prinzip der Angemessenheit und Wirtschaftlichkeit auszuwählen sind, in die Praxis umgesetzt wurden. Diese Umsetzung muss zeitnah durchgeführt werden, kann aber mitunter von größerer Komplexität sein und muss daher sorgfältig geplant werden. Auch sind gegebenenfalls Abhängigkeiten und Prioritäten je nach Gefährdungslage zu berücksichtigen und Verantwortlichkeiten für die Durchführung, Kontrolle und Revision festzulegen.
Da die übergreifenden Verfahren naturgemäß von mehreren Behörden genutzt werden, liegt es nahe, dass zentrale Unterstützungsleistungen zur Umsetzung von Sicherheitskonzepten zielführend sind und zu Synergien führen müssen. Hier bietet es sich an, das diesbezügliche Angebot des eGo-MV – wie im Abschnitt 3.2 erwähnt – aufzugreifen. Die notwendige Steuerung sollte durch den BeKVIS im Zusammenwirken mit den IT-Sicherheitsbeauftragten der Kommunalbehörden erfolgen.

4.2.4 Mitnutzung des CERTs M-V

In der vom Landeskabinett im Juni 2014 erlassenen „Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern“ (IS-Leitlinie M-V) wird die Zusammenarbeit bei der Abwehr von IT-Angriffen als eine der grundlegenden Säulen des Vorgehens bei der Umsetzung der gemeinsamen IT-Sicherheitsstrategie hervorgehoben. Dabei kommt dem im Aufbau befindlichen CERT M-V eine Schlüsselstellung zu, denn es sorgt für einen effizienten Informationsaustausch zwischen allen Beteiligten und das notwendige Zusammenwirken der IT-Sicherheitsbeauftragten der Ressorts mit dem CERT im gemeinsamen Informationssicherheitsprozess. Hierfür stellt das CERT verschiedene Dienstleistungen zur Verfügung, die in zentral finanzierte Basisleistungen und individuell zu finanzierende Zusatzleistungen untergliedert werden. Im Rahmen der Nutzung gemeinsamer zentraler Sicherheitssysteme und IT-Verfahren stehen folgende Basisleistungen des CERTs auch den kommunalen Körperschaften zur Verfügung:

Behandlung von Sicherheitsvorfällen (an gemeinsamen zentralen Sicherheitssystemen und IT-Verfahren)
Die Behandlung von Sicherheitsvorfällen beinhaltet die Reaktion auf Anfragen und Berichte sowie die Analyse von Sicherheitsvorfällen und Einleitung entsprechender Gegenmaßnahmen. Zu den Gegenmaßnahmen zählen insbesondere: - Maßnahmen zum Schutz der betroffenen oder von Angreifern bedrohten Systeme und Netzwerke, - Ausarbeitung von Lösungen und Migrationsstrategien anhand von relevanten Hinweisen oder Warnmeldungen, - Suche nach möglichen Angriffen auf weitere Ziele, - Ausarbeitung von Reaktions- oder Abhilfestrategien, - Hilfe per Telefon, E-Mail, Fax oder auf sonstige Weise (Dokumentation) bei der Wiederherstellung nach einem Sicherheitsvorfall, - Koordinierung der Gegenmaßnahmen.

Alarmmeldungen
Dieser Dienst umfasst die Erfassung, Aufbereitung und Weiterleitung von Informationen, in denen ein Angriffsversuch gemeldet und beschrieben wird. Dazu gehören auch Meldungen über kompromittierte Systeme der Zielgruppen (z. B. durch Schadsoftware) und die Empfehlung kurzfristiger Maßnahmen für den Umgang mit den dadurch entstehenden Problemen.
Warn- und Informationsdienst (WID)
Der Warn- und Informationsdienst informiert über mögliche Angriffe, Warnmeldungen zu neu festgestellten Sicherheitslücken sowie neue Angriffswerkzeuge und Entwicklungen. Auf Basis solcher Bekanntgaben können die Zielgruppen ihre Systeme und Netzwerke vor neu erkannten Problemen schützen, bevor diese ausgenutzt werden.
Technologieüberwachung
Das CERT überwacht und beobachtet neue technische Entwicklungen, Aktivitäten von Angreifern und zugehörige Trends, um zukünftige Risiken leichter erkennen zu können. Dieser Dienst umfasst die Lektüre von sicherheitsspezifischen Mailinglisten und Websites sowie von aktuellen Zeitungs- und Zeitschriftenartikeln zu den Themenbereichen Wissenschaft, Technologie, Politik und Staatswesen, um sicherheitsrelevante Informationen für die Systeme und Netzwerke der Zielgruppen zu extrahieren. Aus dieser Dienstleistung können Bekanntgaben, Richtlinien oder Empfehlungen hervorgehen.
Monitoring von gemeinsamen zentralen Sicherheitssystemen
Das CERT nutzt Sensorik-Systeme mit entsprechenden Auswertungsverfahren, überwacht die entsprechenden Protokolle und wertet die Informationen unterschiedlicher Quellen in einer ganzheitlichen Betrachtung aus. So können z. B. durch das Feststellen von Abweichungen vom Normalzustand kompromittierte Systeme schnell und zuverlässig erkannt und die Betroffenen darüber unmittelbar informiert werden.
Wissensmanagement
Das CERT M-V stellt eine umfassende und übersichtliche Sammlung von nützlichen Informationen, die zur Erhöhung der Sicherheit beitragen, auf einem zentralen Web-Portal zur Verfügung.

Darüber hinaus können folgende weitere technische Unterstützungsleistungen in Form von individuell zu finanzierenden Zusatzleistungen in Anspruch genommen werden:

- Eine über die übliche Beweissicherung hinausgehende IT-Forensik[13] (unter anderem forensische Analysen)
- Sicherheitsanalysen beziehungsweise Penetrationstests[14]
- Technische Audits und Informationssicherheitsrevisionen
- Risikoanalysen
- Sicherheitsbewertungen und Produktbewertungen

Die konkrete Ausgestaltung dieser Dienstleistungen hängt von den Anforderungen der jeweiligen Behörde ab. Dadurch können auch die dafür zu entrichtenden Entgelte im Übrigen nur einzelfallbezogen kalkuliert werden.

[13] Die IT-Forensik befasst sich mit der Spurensuche auf elektronischen Datenträgern.
[14] Bei einem Penetrationstest geht es um die umfassende Prüfung der Sicherheit von Systembestandteilen und Anwendungen.

4.2.5 Beteiligung am CERT M-V

Um zu erreichen, dass die im vorherigen Abschnitt beschriebenen Basisleistungen des CERTs nicht nur im Rahmen der Nutzung von gemeinsamen zentralen Sicherheitssystemen und IT-Verfahren erbracht werden, sondern vollumfänglich wie dies für die Landesverwaltung erfolgt, müsste das CERT M-V personell aufgestockt werden. Sofern hierfür Finanzierungsmöglichkeiten gefunden werden, wäre die Erbringung der im Abschnitt 4.2.4 beschriebenen Dienste dann für die Kommunalbehörden nicht mehr auf zentrale Sicherheitssysteme und Verfahren beschränkt. Darüber hinaus würden folgende weitere Dienstleistungen zur Verfügung stehen:

Sensibilisierung des Sicherheitsbewusstseins
Das CERT M-V unterstützt bei der Information und der Sensibilisierung der Beschäftigten durch Maßnahmen wie Informationsveranstaltungen und Kampagnen zu sicherheitsrelevanten Themen.
Ausbildung/Schulung
Dieser Dienst beinhaltet die Durchführung von Workshops, Schulungskursen und Lernprogrammen zu sicherheitsrelevanten Themen. Hierzu zählen unter anderem Informationen über Richtlinien, die Nutzung von Formularen für die Berichterstattung über Sicherheitsvorfälle, geeignete Reaktions- beziehungsweise Gegenmaßnahmen, Werkzeuge für die Reaktion auf Sicherheitsvorfälle, Methoden zur Prävention und sonstige Informationen, die zur Vermeidung, Erkennung und Meldung von und Reaktion auf Computersicherheitsverletzungen erforderlich sind.
Unterstützung der Notfallvorsorge
Das CERT M-V nutzt die gewonnenen Erfahrungen, um bei der Konzeptionierung von Vorsorgeplänen für Notfälle, Krisen und Katastrophen zu unterstützen. Gleichzeitig beinhaltet dieser Dienst auch die Unterstützung der IT-Sicherheitsbeauftragten bei der Durchführung von Notfallübungen.

Überdies würde die Kommunalverwaltung im Falle der Beteiligung am CERT M-V in das Informationssicherheitsmanagement der Landesverwaltung einbezogen werden. Damit wären folgende Maßnahmen verbunden:

- Einbeziehung in das Meldeverfahren für Sicherheitsvorfälle
- Einbeziehung in das Berichtswesen über durchgeführte proaktive IT-Sicherheitsmaßnahmen wie
  - Bekanntgaben von Sicherheitswarnungen,
  - Bekanntgaben von Berichten anderer Sicherheitsinstitutionen,
  - Stand des Einsatzes von Monitoring- beziehungsweise Sensorik-Systemen,
  - weitere proaktive IT-Sicherheitsmaßnahmen.

- Einbeziehung in das Berichtswesen über durchgeführte nachhaltige IT-Sicherheitsmaßnahmen wie
  - durchgeführte Sensibilisierungsmaßnahmen,
  - durchgeführte Schulungsmaßnahmen,
  - durchgeführte Notfallübungen,
  - durchgeführte Informationssicherheitsrevisionen (mit Ergebnisdarstellung),
  - Durchgeführte Sicherheitsanalysen (z. B. Penetrationstests),
  - Weitere nachhaltige IT-Sicherheitsmaßnahmen.
- Mitnutzung von zentralen Sensibilisierungs- und Schulungsmaßnahmen

4.2.6 Nutzung zentral zur Verfügung stehender IT-Verfahren

Durch die Nutzung von zentral zur Verfügung stehenden IT-Verfahren können sich einzelne Behörden sowohl organisatorisch als auch finanziell entlasten und Fragen der IT-Sicherheit oder des Datenschutzes gemeinsam bewältigen. Kommunalbehörden, welche die zentral vom eGo-MV angebotenen Verfahren nutzen, werden dies zu schätzen wissen, insbesondere wenn nicht nur der technische Betrieb, sondern auch der fachliche Support von diesem geleistet wird, wie dies beim Verfahren „Elektronisches Personenstandswesen“ der Fall ist.
Hinsichtlich der IT-Sicherheit liegt der Vorteil der Nutzung zentraler Verfahren, die durch den eGo-MV oder die DVZ M-V GmbH angeboten werden, insbesondere darin, dass der Betrieb in zertifizierten Rechenzentren erfolgt und die IT-Grundschutzanforderungen damit beim Verfahrensbetreiber standardmäßig berücksichtigt werden. Da die erzielbaren Synergieeffekte direkt vom Nutzungsgrad abhängig sind und dessen Anstieg exponentielle Auswirkungen auf die Einsparmöglichkeiten haben dürfte, sollte die Nutzung von zentral zur Verfügung stehenden Verfahren und Infrastrukturen verpflichtend vorgeschrieben werden. Die Notwendigkeit und Dringlichkeit einer solchen Regelung ergibt sich aktuell erst recht vor dem Hintergrund der Auswirkungen des E-Government-Gesetzes des Bundes, des Verwaltungsverfahrensgesetzes M-V und des Gesetzes zur Förderung des elektronischen Rechtsverkehrs, weil die Mehraufwände, die entstehen könnten, wenn parallele Lösungen für Systeme zur rechtssicheren Kommunikation, rechtssicheren Aktenführung und beweiswerterhaltenden Speicherung von Dokumenten aufgebaut würden, in diesem Zusammenhang eine ganz andere Dimension erhielten. Da es sich hierbei nicht vordergründig um eine ganz andere Dimension in wirtschaftlicher, sondern vor allem in sicherheitsrelevanter Hinsicht handelt, sollte die Steuerung, welche zentral zur Verfügung stehenden Verfahren verpflichtend in den Kommunalbehörden genutzt werden müssen, durch die Lenkungsgruppe für die Informationssicherheit in den Kommunen erfolgen. Sobald dieses Gremium derartige Beschlüsse gefasst hat, könnte es zu deren Umsetzung Muster-Dienstanweisungen herausgeben, die von den einzelnen Kommunalbehörden übernommen und entsprechend in Kraft gesetzt werden müssten.

5 Kosten

5.1 Personalkosten

Nachfolgend sind die zusätzlich benötigten Stellen zur Umsetzung der im Abschnitt 4 dargelegten Maßnahmen zur Erhöhung der Informationssicherheit in der Kommunalverwaltung aufgelistet. Die Werte stellen den schätzungsweise anfallenden Mindestbedarf dar.
Die individuell bei den einzelnen Kommunalbehörden in diesem Zusammenhang anfallenden Personalaufwände sind in der Tabelle nicht berücksichtigt, weil es sich hierbei um Pflichtaufgaben handelt, die derzeit bereits bestehen. Dies trifft auch für die von den jeweiligen IT-Sicherheitsbeauftragten wahrzunehmenden Aufgaben zu.

Bezug auf Abschnitt	Maßnahme	Vollzeit-einheiten (VZE)	Bemerkungen
4.1.1	Ernennung von IT-Sicherheitsbeauftragten	3	Personalbedarf, wenn der eGo-MV gemeinsame IT-Sicherheitsbeauftragte für die Kommunen stellen würde
4.1.2	Einsatz eines Beauftragten der Kommunalverwaltung für Informationssicherheit	1,5	Personalbedarf für den Beauftragten der Kommunalverwaltung für Informationssicherheit
	Summe:	**4,5**	
	Personalkosten[15]	**415.000 €**	

Tabelle 1: Übersicht über den Personalaufwand

Mithin müssten dem eGo-MV zur Umsetzung der Maßnahmen 4,5 Stellen zusätzlich zur Verfügung gestellt werden. Werden zur Ermittlung der entsprechend zu berücksichtigen Personalkosten die Personalkostensätze der Entgeltgruppe E 12 zugrunde gelegt, betragen die hierfür benötigten Haushaltsmittel insgesamt **415.000 €** pro Jahr.

5.2 Sachkosten

Sachkosten sind lediglich für die Mitnutzung des zentralen Managementsystems für Informationssicherheit, die Erstellung von Muster-Sicherheitskonzepten und den Fall einer Beteiligung der Kommunalverwaltung am CERT M-V zu berücksichtigen. Kosten, die für individuell zu finanzierende Zusatzleistungen, wie in Abschnitt 4.2.4 beschrieben, anfallen würden, sind vom jeweiligen Einzelfall abhängig, individuell zu beauftragen und daher nicht berücksichtigt. Ebenso unberücksichtigt sind die Kosten für die Nutzung zentral zur Verfügung stehender IT-Verfahren, weil auch diese individuell zu finanzieren sind.

[15] Gemäß Gebührenerlass 2014/2015 des Finanzministeriums beträgt der Personalkostensatz einer Stelle der Entgeltgruppe E12 pro Jahr 92.265 €.

Die nachfolgende Tabelle gibt Auskunft über die schätzungsweise anzusetzenden Beträge:

Bezug auf Abschnitt	Maßnahme	Sachkosten in € pro Jahr	Bemerkungen
4.2.1	Mitnutzung des zentralen Managementsystems für Informationssicherheit (ISMS)	25.000	Mittelbedarf für die Nutzung des zentralen ISMS der Landesverwaltung durch die Kommunalverwaltung
4.2.2	Erstellung von Muster-Sicherheitskonzepten	100.000	Mittelbedarf, wenn die DVZ M-V GmbH circa 3 - 6 Mustersicherheitskonzepte im Jahr erstellen würde
4.2.5	Beteiligung am CERT M-V	300.000	Mittelbedarf, wenn die CERT-Kopfstelle in der DVZ M-V GmbH die Dienstleistungen für die Kommunen mit erbringen würde[16]
	Summe:	**425.000**	

Tabelle 2: Übersicht über die Sachkosten

Mithin sind zur Umsetzung der Maßnahmen jährlich circa **425.000 €** erforderlich.

5.3 Gesamtkosten

Aus den in den Abschnitten 5.2 und 5.3 vorgenommenen Betrachtungen ergeben sich die jährlich insgesamt zu berücksichtigenden Gesamtkosten wie folgt:

Personalkosten: 415.000 €
Sachkosten: 425.000 €
Gesamtkosten: **840.000 €**

Diese Mittel sind bisher weder im Landeshaushalt noch in den kommunalen Haushalten veranschlagt worden. Mit der Entscheidung der kommunalen Seite, ob und inwieweit sie das Angebot der Landesregierung und die vorgeschlagenen Maßnahmen annimmt, muss zugleich darüber entschieden werden, wie deren Finanzierung sichergestellt werden soll.

[16] Es würde ein Dienstleistungsvertrag geschlossen werden, der die Bereitstellung von 2 VZE zum Preis von 250.000 € und die Finanzierung der zusätzlich auf die Kommunen entfallenden CERT-Sachkosten beinhaltet.

6 Anhang

6.1 Begriffsdefinitionen

Informationssicherheitsmanagement

Das Informationssicherheitsmanagement (kurz ISM) wird im BSI-Standard 100-1 beschrieben, der im Wesentlichen auf dem ISO 27001-Standard aufbaut und die Empfehlungen des ISO Standards 27000 und ISO 27002 berücksichtigt. Nach der Definition des Bundesamts für die Sicherheit in der Informationstechnik (BSI) ist das ISM:

„… jener Teil des allgemeinen Risikomanagements, der die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Anwendungen und IT-Systemen gewährleisten soll. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.“

Zum Management der Informationssicherheit gehören insoweit alle Aufgaben und Aktivitäten, mit denen ein angemessenes Sicherheitsniveau erreicht und gehalten wird. In diesem Zusammenhang ist beispielsweise die regelmäßige Durchführung von Informationssicherheitsrevisionen ein unerlässliches Instrument, um den erreichten Stand der Informationssicherheit und die Effizienz der gewählten Sicherheitsstrategie zu bewerten, zu beurteilen und zu verbessern.
Verantwortlich für die Informationssicherheit in einer Behörde ist die jeweilige Behördenleitung. Die Verantwortung für die Landesverwaltung von Mecklenburg-Vorpommern wird durch den IT-Beauftragten der Landesverwaltung wahrgenommen.

Sicherheitsvorfall

Selbst bei Umsetzung aller konzipierten Sicherheitsmaßnahmen kann in der Praxis nicht ausgeschlossen werden, dass Sicherheitsvorfälle auftreten. Wird auf solche Situationen nicht angemessen und unverzüglich reagiert, können sich daraus unter Umständen große Schäden bis hin zu Notfallsituationen entwickeln. Um Maßnahmen zur Behandlung von Sicherheitsvorfällen planen zu können, muss zunächst definiert werden, was ein Sicherheitsvorfall ist.
Ein Sicherheitsvorfall ist jedes Vorkommnis, bei dem die Grundwerte der Informationssicherheit

- Vertraulichkeit (Schutz vor unbefugter Preisgabe),
- Verfügbarkeit (Schutz vor Verlust und Ausfall)
- Integrität (Schutz vor Manipulation oder Verfälschung),

von Daten beziehungsweise IT-Systemen in unzulässiger Weise verletzt werden.
Sicherheitsvorfälle sind somit Vorkommnisse,

a) die einen Verstoß gegen die geltenden Sicherheitsrichtlinien darstellen, wie z. B:
   - Weitergabe von Passwörtern,
   - Manipulation von IT-Geräten (APC, Notebooks, Netzwerkdruckern, Etagenkopierern usw.),
   - Zutritt von Unbefugten zu Server- oder Verteilerräumen,
   - Anschluss privater Geräte (z. B. USB-Sticks) an APC,

b) die einen Verstoß gegen relevante gesetzliche Vorschriften oder Verwaltungsvorschriften (z. B. DSG M-V) darstellen, wie z. B.:
   - unrechtmäßige Speicherung und Auswertung von Personendaten,
   - ungeeigneter Umgang mit vertraulichen Informationen,

c) die die Sicherheit von Daten, Netzen und IT-Systemen des Landes in einer Weise beeinträchtigen, welche den im jeweiligen IT-Sicherheitskonzept festgelegten Schutzbedarf verletzt, wie z. B.:
   - Fehlerhaft eingerichtete Zugriffsmöglichkeiten auf Informationen,
   - Computerviren, Schadsoftware,
   - Unbefugtes Kopieren von Datenbeständen,

d) die die vorhanden Sicherheitsmechanismen oder Sicherheitssysteme ganz oder teilweise außer Funktion setzen, wie z. B.:
   - Umgehen von Firewalls,
   - Deaktivieren von Virenscannern auf den APC,

e) die darauf hinweisen, dass ein Vorfall nach a) bis d) versucht wurde oder bevorsteht, wie z. B.:
   - unerklärliches Systemverhalten,
   - verdächtige Einträge in Protokolldateien der Server und Firewalls.

CERT (Computer Emergency Response Team)

Ein CERT ist, nach der Definition der europäischen IT-Sicherheitsbehörde ENISA (European Network and Information Security Agency):

„Ein Team von IT-Sicherheitsexperten beziehungsweise -sachverständigen, deren Hauptaufgabe darin besteht, auf Computersicherheitsverletzungen zu reagieren. Dieses Team bietet die zu ihrer Behandlung notwendigen Dienstleistungen und unterstützt seine Klientel bei der Wiederherstellung nach derartigen Sicherheitsverletzungen.“

Ein solches Computer-Notfallteam ist somit in der Lage, IT-Sicherheitsvorfälle in einer Organisation abzuschwächen oder zu verhindern sowie Informationen angemessenen Schutz zu bieten.
Im Wesentlichen können die zu erbringenden Leistungen eines CERTs in folgende drei Bereiche unterteilt werden:

- Reaktive CERT-Leistungen, die konkrete Maßnahmen infolge aktueller sicherheitsrelevanter Vorkommnisse beinhalten und der Unterstützung von Betroffenen dienen.
- Proaktive CERT-Leistungen, die auf die Verbesserung der Sicherheit ausgerichtet sind und der Vermeidung von Vorfällen dienen.
- Nachhaltige CERT-Leistungen, die auf den Erfahrungen bei der Erbringung von reaktiven und proaktiven CERT-Leistungen beruhen und der Nachhaltigkeit des Sicherheitsmanagements dienen.

Daraus abgeleitet sind die wesentlichen Aufgaben eines CERTs:

- Die sachkundige Behandlung von Sicherheitsvorfällen, was insbesondere die Unterstützung von Betroffenen bei der raschen Wiederherstellung ihrer Systeme und die zentrale Koordinierung aller notwendigen Aktivitäten nach Sicherheitsvorfällen sowie die Sicherstellung und Aufbewahrung von Beweisen (Forensik) beinhaltet.
- Der Betrieb eines Warn- und Informationsdienstes, was insbesondere die Auswertung und Verteilung von sicherheitsrelevanten Informationen und die Beobachtung von Entwicklungen im Bereich der Informationssicherheit beinhaltet.
- Die Unterstützung der Notfallvorsorge durch Wissensvermittlung und Sensibilisierung des Sicherheitsbewusstseins, was insbesondere die Durchführung von Notfallübungen, Workshops und Schulungen zu sicherheitsrelevanten Themen beinhaltet.

In Deutschland wurden erste Computer-Notfallteams bereits in den neunziger Jahren eingerichtet (CERT Universität Karlsruhe, CERT des Deutschen Forschungsnetzes). Seitdem ist eine große Zahl von CERTs hinzugekommen. Im Bereich der öffentlichen Verwaltung gibt es auf Bundesebene unter anderem das CERT-Bund im BSI, in dem auch das Bürger-CERT angesiedelt ist. Seit 2002 sind inzwischen mehr als 30 Teams aus den verschiedensten Bereichen im Deutschen CERT-Verbund organisiert.

6.2 Abkürzungsverzeichnis

APC	Arbeitsplatzcomputer
BeLVIS	Beauftragter der Landesverwaltung für Informationssicherheit
BeKVIS	Beauftragter der Kommunalverwaltung für Informationssicherheit
BMI	Bundesministerium des Innern
BSI	Bundesamt für die Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
CERT M-V	CERT Mecklenburg-Vorpommern
DSG M-V	Datenschutzgesetz Mecklenburg-Vorpommern
DVZ M-V GmbH	DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
eGo-MV	Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern
GS-Tool	Grundschutz-Tool des BSI
IT	Informationstechnik
IS-Leitlinie	Informationssicherheitsleitlinie
ISM	Informationssicherheitsmanagement
ISM-Konzept	Konzept für den Aufbau und Betrieb eines Informationssicherheits-managements in der Landesverwaltung von Mecklenburg-Vorpommern
IS-Richtiline	Informationssicherheitsrichtlinie
ISMS	Managementsystem für die Informationssicherheit
M-V	Mecklenburg-Vorpommern
VZE	Vollzeiteinheit
WID	Warn- und Informationsdienst