Landesrechnungshof Mecklenburg-Vorpommern

Landesrechnungshof Mecklenburg-Vorpommern, Mühlentwiete 4, 19059 Schwerin

gemäß Verteiler
nur per E-Mail

Bearbeiter: Steffen Wirks
Telefon: +49 (0) 385 74 12 -113
Fax: +49 (0) 385 74 12 -100
E-Mail: swirks@lrh-mv.de
Ihr Zeichen:
GZ:

Rundschreiben Nr. 1/2020 des Landesrechnungshofes Mecklenburg-Vorpommern

Grundsatzpapier zum Informationssicherheitsmanagement

Allgemeines

Der Landesrechnungshof Mecklenburg-Vorpommern informiert in unregelmäßigen Abständen über Themen von über den Einzelfall hinausgehender Bedeutung durch Rundschreiben. Adressat der Rundschreiben sind alle Stellen der öffentlichen Verwaltung in Mecklenburg-Vorpommern, die vom Landesrechnungshof geprüft werden können. Der Versand erfolgt ausschließlich elektronisch, die Rundschreiben werden auch auf der Homepage des Landesrechnungshofes zur Verfügung gestellt[1].

Der Landesrechnungshof wird die in seinen Rundschreiben mitgeteilten Feststellungen und Wertungen seiner künftigen Prüfungstätigkeit zugrunde legen und bei den geprüften Stellen als bekannt voraussetzen. Er bittet deshalb die Empfänger, in geeigneter Weise sicherzustellen, dass die Rundschreiben allen Beschäftigten bekannt gemacht werden.

1 Grundsatzpapier Informationssicherheitsmanagement

Die Rechnungshöfe des Bundes und der Länder hatten im Oktober 2015 ein Grundsatzpapier veröffentlicht. Dieses wird nun in einer aktualisierten Fassung vorgelegt und ersetzt

[1] Http://www.lrh-mv.de/Veröffentlichungen/Rundschreiben/.

das bisherige Dokument. Es steht auf der Homepage des Landesrechnungshofes zur Verfügung.[2]

1.1 Grundsatz der Wirtschaftlichkeit

Die Rechnungshöfe betonen in der aktualisierten Fassung die Notwendigkeit der Wirtschaftlichkeit des Informationssicherheitsmanagements.

Einerseits ist die Aufrechterhaltung der Funktionsfähigkeit der Verwaltung durch den Schutz der Verfügbarkeit, Integrität und Vertraulichkeit der Systeme und Informationsbestände ein Gebot der Wirtschaftlichkeit. Aktuelle Beispiele zeigen, dass erfolgreiche Angriffe z. B. durch Ransomware[3] oder APT[4] eine Verwaltung für längere Zeit lahmlegen können.

Neben dem Reputationsverlust gehen mit erfolgreichen Angriffen volkswirtschaftliche Schäden einher, wenn Genehmigungen nicht erteilt und Geldleistungen nicht ausgezahlt werden können. Zudem verursacht die Wiederherstellung des ursprünglichen Zustands außerplanmäßige Ausgaben zu Lasten der Haushalte. Auch der mögliche dauerhafte Verlust von Daten stellt ein finanzielles Risiko dar.

Die Verletzung von Dienst- oder Privatgeheimnissen durch das Ausspähen von Daten kann strategische oder operative Ziele der öffentlichen Verwaltung gefährden und birgt das Risiko von Schadensersatzansprüchen.

Sicherheitslücken in IT-Systemen, die der Auszahlung von Geldleistungen dienen, ermöglichen betrügerische Handlungen zu Lasten des Haushalts. Die daraus resultierenden Zahlungen ohne Rechtsgrund sind rechtswidrig und damit zugleich unwirtschaftlich. Informationssicherheit ist die Grundlage für Kassensicherheit.

[2] Grundsatzpapier der Rechnungshöfe des Bundes und der Länder zum Informationssicherheitsmanagement (Mai 2020); https://www.lrh-mv.de/Veröffentlichungen/Gemeinsame-Dokumente-der-Rechnungshöfe.

[3] Schadsoftware, die die Nutzung von Rechnern oder Daten blockieren und für die Freigabe ein Lösegeld fordert. Auch nicht erfolgreiche Angriffe können zu finanziellen Schäden führen, da als Sofortmaßnahme bei einer erkannten Bedrohung die betroffenen Netzwerksegmente und IT-Systeme abgeschaltet werden müssen. 2019 gab es mehrere Angriffe auf Kommunalverwaltungen, Universitäten und Kliniken.

[4] Advanced Persistent Thread (fortgeschrittene andauernde Bedrohung). Angriff auf ein Netzwerk, bei dem sich eine unautorisierte Person Zugriff auf ein Netzwerk verschafft, um sich dort möglichst lange unerkannt aufzuhalten. Die Angriffe dienen in der Regel dem Diebstahl von Daten. Da der Angreifer tief in das System eindringt und versucht Zugriff auf alle verfügbaren Bereiche der IT-Infrastruktur zu erlangen, kann die Bedrohung häufig nur durch umfangreiche Ersatzbeschaffungen und Neuinstallationen bekämpft werden. Ein Beispiel für erfolgreiche APT sind der Angriff auf das Netzwerk des Deutschen Bundestages und das Berliner Kammergericht.

Die angestrebte Digitalisierung in der Verwaltung ist von der Akzeptanz digitaler Lösungen durch Bürger und Unternehmen abhängig. Dazu müssen diese darauf vertrauen können, dass ihre Daten sicher übertragen, verarbeitet und gespeichert werden. Berichte über erfolgreiche Angriffe auf IT-Systeme und Informationsbestände könnten dieses Vertrauen untergraben und dazu führen, dass digitale Lösungen nicht genutzt werden. Akzeptanzprobleme bei digitalen Lösungen erfordern zusätzlichen Verwaltungsaufwand für die Bearbeitung von Verwaltungsvorgängen (Scannen von Papierpost, Drucken und Versenden von Dokumenten in Papierform) und erhöhen die Kosten des Verwaltungshandelns. Um die Wirtschaftlichkeit des Verwaltungshandelns zu gewährleisten, ist eine hohe Nutzungsquote bei den digitalen Lösungen anzustreben.

Andererseits unterliegt das Informationssicherheitsmanagement selbst auch dem Gebot der Wirtschaftlichkeit gem. § 7 LHO bzw. § 43 Abs. 4 Kommunalverfassung M-V. Das heißt, das notwendige Sicherheitsniveau und die dafür notwendigen Maßnahmen sind am tatsächlichen Schutzbedarf und der Gefährdungslage auszurichten.

Alle Maßnahmen des Informationssicherheitsmanagements müssen geeignet sein, das angestrebte Sicherheitsniveau zu erreichen und den Schutzbedarf zu gewährleisten. Jede ungeeignete Maßnahme ist zugleich auch unwirtschaftlich.

Aus mehreren geeigneten Maßnahmen sind diejenigen auszuwählen, die mit dem geringsten Mitteleinsatz realisiert werden können. Vor Investitionen in technische Maßnahmen zur Informationssicherheit ist im Rahmen einer Wirtschaftlichkeitsbetrachtung die wirtschaftlichste Lösung zu ermitteln. Dies setzt voraus, dass zuvor die Anforderungen vollständig erhoben und definiert wurden.

Bereits bei der Planung von IT-Architekturen sollten diese so gestaltet werden, dass der technische Aufwand und damit die Kosten für ihre Absicherung minimiert werden.

Durch organisatorische Maßnahmen der Informationssicherheit sollte der Aufwand für technische Lösungen ebenfalls minimiert werden.

1.2 Fragenkatalog

Die Rechnungshöfe haben als Teil des Dokuments einen Fragenkatalog erarbeitet. Die Fragen können durch den Landesrechnungshof bei seinen Prüfungen als Prü-

fungsmaßstab herangezogen werden. Die Verwaltungen können den Fragebogen für eine Selbstüberprüfung verwenden.

2 Prüfungserfahrungen

Bei Prüfungen hat der Landesrechnungshof insbesondere festgestellt, dass:

- notwendige Dokumentationen nicht vorhanden, nicht aktuell oder unvollständig waren,
- notwendige Regelungen, Prozesse und Maßnahmen nicht den Anforderungen der jeweiligen Vorschriften in ihrer aktuellen Fassung genügten,
- das Sicherheitskonzept nicht mehr den tatsächlichen Gegebenheiten (der IT-Infrastruktur und den Geschäftsprozessen) entsprach,
- im Sicherheitskonzept aufgeführte Maßnahmen noch nicht umgesetzt waren,
- es bei Verfahren mit Nutzern auch außerhalb der Landesverwaltung (z. B. Kommunen) an Vorgaben für die Gewährleistung von Informationssicherheit fehlte,
- bei der Beauftragung von Dienstleistern nicht alle Vorgaben des Grundschutzkompendiums zum Outsourcing umgesetzt wurden und
- Zertifizierungen nicht geprüft wurden.

Jede Änderung in der IT-Infrastruktur oder in den Geschäftsprozessen muss eine Überprüfung und ggf. Anpassung des Sicherheitskonzepts auslösen.

Die Umsetzung der Maßnahmen des Informationssicherheitsmanagements muss bei allen Nutzern durchgesetzt werden.

Bei der Nutzung von Dienstleistern sind die Vorgaben des BSI zum Outsourcing sowie die der DS-GVO zur Auftragsverarbeitung umzusetzen. Bei Zertifizierungen sind deren Geltungsbereich, die Gültigkeit sowie die Umsetzung etwaiger Auflagen des Zertifizierers zu prüfen.

Gemäß des BSI-Grundschutzkompendiums ist das Standard-Datenschutzmodell (SDM) der Datenschutzbehörden des Bundes und der Länder umzusetzen, um die Gewährleistungsziele des Datenschutzes zu erreichen.

Der Landesrechnungshof empfiehlt, ein IT-gestütztes Änderungs- und Dokumentationsmanagement einzuführen. Dieses kann die Transparenz und Nachvollziehbarkeit des Informationsmanagements verbessern, den manuellen Aufwand verringern und dadurch die Wirtschaftlichkeit erhöhen. Die Modellierung des Informationsverbundes und der technischen und organisatorischen Maßnahmen sowie die Dokumentation des Umsetzungsstandes sollten ebenfalls IT-gestützt erfolgen.

3 Weitere Rundschreiben des Landesrechnungshofes

3.1 Rundschreiben des Landesrechnungshofes Nr. 2/2016: Informationssicherheitsmanagement

Das Rundschreiben bleibt weiterhin gültig unter der Maßgabe, dass dort zitierte Rechtsvorschriften und Dokumente in ihrer jeweils aktuellen Fassung anzuwenden sind. Dies gilt insbesondere für die IT-Grundschutzstandards des BSI 200-1, 200-2 und 200-3 anstelle der dort zitierten 100-1, 100-2 und 100-3 sowie das Grundschutzkompendium anstelle der Grundschutzkataloge.

Zu dem im Abschnitt 5.2 für Gemeinden und Amtsverwaltungen empfohlenen „Informations-Sicherheits-Management-System in 12 Schritten (ISIS 12)“ ergänzt der Landesrechnungshof seine Ausführungen mit dem Hinweis, dass die Nutzung eine kostenpflichtige Lizenzierung erfordert.

3.2 Rundschreiben des Landesrechnungshofes Nr. 1/2019: Ordnungsmäßigkeit des Einsatzes von Informationstechnik

Der Landesrechnungshof hat in dem Rundschreiben ausgeführt, welche Rechtsnormen und sonstigen Regelungen sowie Empfehlungen einzuhalten sind. Weiterhin hat er Grundsätze für die im Rahmen von Informationssicherheitsmanagement und Datenschutz erforderlichen Dokumentationen aufgestellt. Das Rundschreiben enthält Hinweise zum Outsourcing und der Auftragsverarbeitung.

Das Rundschreiben bleibt weiterhin gültig und wird demnächst in einer überarbeiteten Fassung veröffentlicht werden.

gez. Dr. Johannsen gez. Fuhrmann

gez. Dr. Zitscher