Landesrechnungshof Nordrhein-Westfalen

Beratung des Landtags nach § 88 Absatz 2 Landeshaushaltsordnung

Informationssicherheit gemeinsam stärken

Gz.: KuP-01.07.02-000010-2023-0003510

Düsseldorf, den 29.11.2023

Inhaltsverzeichnis

1 Informationssicherheit gemeinsam stärken

Der Landesrechnungshof (LRH) regt an, dass der Landtag aus seiner Mitte heraus das E-Government-Gesetz Nordrhein-Westfalen (EGovG NRW) novelliert, um eine stringentere Steuerung der Informationssicherheit durch den Beauftragten der Landesregierung für Informationstechnik (CIO) zu erreichen. Dazu schlägt er insbesondere vor: 1

- Anpassung der §§ 22 und 23 EGovG NRW. Die dort festgelegten Abstimmungsregelungen zwischen dem CIO bzw. dem Ministerium für Heimat, Kommunales, Bau und Digitalisierung (MHKBD) und den Ressorts sollten zu Gunsten des CIO bzw. des MHKBD vereinfacht werden (Benehmen statt Einvernehmen).[1]
- Festschreibung von Kontrollbefugnissen für den CIO hinsichtlich der Informationssicherheit in den Ressorts.

Zudem sollte der Landtag die Landesregierung auffordern, 2

- die Stellung des CIO im Land hierarchisch anzuheben und
- die notwendigen Schritte einzuleiten, um die IT-Infrastruktur bei den Rechenzentren des Landes weitgehend zu zentralisieren.

Der Stand der Informationssicherheit in der Landesverwaltung ist unstreitig kritisch. Nach aktuellem Bericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die Bedrohungslage so hoch wie nie zuvor. Mit Blick auf die Arbeits- und Funktionsfähigkeit der Landesverwaltung besteht Handlungsbedarf. 3

Der LRH hat im März 2023 die Landesregierung zur Gewährleistung der Informationssicherheit in der Landesverwaltung beraten. Aus Sicht des LRH fehlt es insbesondere an hinreichend zentralen Strukturen und einer Steuerung aus einer Hand. Der LRH hat der Landesregierung daher u. a. die Ausweitung der Befugnisse des CIO sowie eine weitgehende IT-Zentralisierung empfohlen. 4

---

[1] Wie auch schon in früheren Entscheidungen des LRH ausgeführt, steht einer Erweiterung ressortübergreifender Kompetenzen die in Art. 55 Abs. 2 der Verfassung für das Land Nordrhein-Westfalen im Rahmen des Ressortprinzips garantierte Organisationshoheit der Ministerien nicht entgegen. Denn die Informationssicherheit gewährleistet, dass die Ressorts die ihnen obliegenden Aufgaben wahrnehmen können. Sie hat also eine rein „dienende“ Funktion (im Gegensatz zu einer „lenkenden“ Funktion). Die Sachkompetenz der Ressorts wird durch aufgabenneutrale Vorgaben (Kommunikations- und Sicherheitsstandards, gemeinsame Anwendungen, gemeinsames Behördennetz) in der Regel nicht berührt (vgl. Rn. 33 der Beratung der Landesregierung zur Gewährleistung der Informationssicherheit [Anlage]).

Obwohl das MHKBD im Rahmen von Gesprächen den Empfehlungen des LRH grundsätzlich zustimmte, sind wesentliche Fortschritte in der Sache bislang nicht erkennbar. Dabei darf es bei diesem wichtigen Thema keinen Stillstand geben. Aus Sicht des LRH ist ein Handeln des Parlaments erforderlich, um die notwendigen strukturellen Veränderungen zur Stärkung der Informationssicherheit im Land anzustoßen. 5

Die Informationssicherheit in der Landesverwaltung muss dringend gestärkt werden. 6

2 Informationssicherheit in der Landesverwaltung kritisch

Die Gewährleistung von Informationssicherheit ist für die Funktionsfähigkeit der Landesverwaltung mit Blick auf die fortschreitende Digitalisierung unverzichtbar. Cyber-Angriffe von außen oder auch Manipulationen von innen können zu schwerwiegenden Systemausfällen führen und erhebliche wirtschaftliche Schäden verursachen. Aufgrund der Abhängigkeit der Funktionsfähigkeit der Landesverwaltung von den eingesetzten IT-Verfahren muss die Herstellung eines angemessenen Sicherheitsniveaus höchste Priorität besitzen. 7

Die öffentliche Verwaltung ist zunehmend Zielscheibe von Hackern. Nach dem aktuellen Lagebericht des BSI für 2023 ist die Bedrohung im Cyberraum so hoch wie nie.[2] Aus den Medien sind zahlreiche Angriffe mit schwerwiegenden Folgen bekannt. Stellvertretend sei hierzu auf einen aktuellen Artikel der Frankfurter Allgemeinen Zeitung vom 06.11.2023 verwiesen.[3] 8

Der Landesregierung ist die Problematik der mangelhaften Beachtung der Anforderungen an die Informationssicherheit auch aus eigenen Quellen bekannt. Dies hat der LRH bei seiner Prüfung zum Notfallmanagement innerhalb der Landesverwaltung festge- 9

---

2 Vgl. BSI – Die Lage der IT-Sicherheit in Deutschland 2023, „Die Bedrohung im Cyberraum ist […] so hoch wie nie zuvor“, Seite 11, Satz 2.

3 Vgl. Frankfurter Allgemeine Zeitung vom 06.11.2023, Seite 18, „So anfällig sind die Länder für Cyberangriffe“.

stellt.[4] Ein ressortübergreifend besetztes IT-Gremium der Landesregierung bewertete in 2021 den Stand der Informationssicherheit in der Landesverwaltung unverändert als kritisch.

Auch der LRH hat in seinen Prüfungen immer wieder z. T. schwere Mängel bei der Informationssicherheit festgestellt. Zuletzt u. a. bei dem zentralen Verfahren zur Bewirtschaftung des Landeshaushaltes.[5] Dabei sind sichere und verfügbare IT-Systeme für die Arbeits- und Funktionsfähigkeit der Landesverwaltung unabdingbar. Die Folgen einer Manipulation oder eines (längerfristigen) Ausfalls können enorm sein. Z. B. könnten bei dem genannten Verfahren zahlungswirksame Vorgänge nicht mehr verbucht werden. Die Verwaltung könnte keine Leistungen mehr beziehen und keine Gelder mehr auszahlen. Dies beträfe Löhne und Gehälter, ebenso wie den Einkauf von Waren und Dienstleistungen, aber auch so scheinbar banale Dinge wie z. B. Kraftstoff für die Fahrzeuge der Sicherheitskräfte. Die gesetzlichen Anforderungen zur Informationssicherheit bei diesem Verfahren sind bis heute nicht vollständig umgesetzt.[6] **10**

Vor diesem Hintergrund hat der LRH am 28.03.2023 die Landesregierung zur Gewährleistung der Informationssicherheit in der Landesverwaltung beraten (siehe Anlage). **11**

3 Beratung der Landesregierung

Der LRH hat in seinem Beratungsbericht aus März 2023 insbesondere die Strukturen zur Gewährleistung der Informationssicherheit in den Blick genommen. Konkret hat der LRH der Landesregierung die Prüfung der folgenden Maßnahmen empfohlen: **12**

---

4 Vgl. Vorlage 18/1511: Jahresbericht 2023 des LRH über das Ergebnis der Prüfungen im Geschäftsjahr 2022, Seiten 95 - 100 (Beitrag 11 „Ohne hinreichende Vorsorge in die Krise – Funktionsfähigkeit der Landesverwaltung in Krisen sicherstellen“).

5 Vgl. Drucksache 18/839: Jahresbericht 2022 des LRH über das Ergebnis der Prüfungen im Geschäftsjahr 2021, Seiten 107 - 113 (Beitrag 5 „IT-Verfahren zur Verwaltung des Landeshaushalts mangelhaft“).

6 Stand: 15.11.2023.

- mehr **zentrale, ressortübergreifende Steuerung** des Informationssicherheitsmanagements durch **Ausweitung der Befugnisse des CIO im EGovG NRW**;
- hierarchische **Anhebung des CIO auf Staatssekretärsebene**;
- weitgehende **Zentralisierung der IT-Infrastruktur** aller Ressorts bei den Rechenzentren des Landes.

Zu den Empfehlungen des LRH an die Landesregierung ist Folgendes kurz zu bemerken: **13**

Mehr zentrale, ressortübergreifende Steuerung, Ausweitung der Befugnisse des CIO und hierarchische Anhebung auf Staatssekretärsebene

Zwar existiert mit dem CIO eine ressortübergreifende Verantwortungsebene für die Informationssicherheit.[7] Für die Umsetzung konkreter Maßnahmen der Informationssicherheit sind aber nach wie vor die Ressorts selbst (bzw. die jeweiligen Behörden und Einrichtungen) verantwortlich. Daher ist das Informationssicherheitsmanagement in der Landesverwaltung im Kern dezentral organisiert. Der CIO hat insoweit nur sehr geringen Einfluss. Er moderiert mehr, als dass er steuert.[8] Landesweite Richtlinien und Priorisierungen zur Informationssicherheit können durch den CIO bzw. das für die Digitalisierung der Landesverwaltung zuständige MHKBD nur in schwergängigen Abstimmungs- und Einvernehmensverfahren mit den Ressorts vorgegeben werden.[9] Daher hat der LRH die Prüfung einer Änderung des EGovG NRW vorgeschlagen. Unter anderem sollten die Entscheidungsbefugnisse des CIO bzw. des MHKBD gegenüber den Ressorts ausgeweitet werden. Damit könnten diese effektiver Verwaltungsvorschriften zu zentralen Standards für die Informationssicherheit erlassen.[10] Auch die Verortung des CIO auf Staatssekretärsebene mit eigenem Vortragsrecht im Kabinett könnte diesbezügliche **14**

---

7 So hat die Landesregierung mit der Informationssicherheitsleitlinie aus 2015 sowie der Festschreibung der Koordinierungsfunktion des CIO im EGovG NRW beim Informationssicherheitsmanagement in der Landesverwaltung grundsätzlich zentrale Strukturen unter ihrer Gesamtverantwortung eingerichtet. Vgl. Rn. 22 der Beratung der Landesregierung zur Gewährleistung der Informationssicherheit (Anlage).

8 Vgl. Rn. 22 der Beratung der Landesregierung zur Gewährleistung der Informationssicherheit (Anlage).

9 Vgl. Rn. 23 - 25 der Beratung der Landesregierung zur Gewährleistung der Informationssicherheit (Anlage).

10 Vgl. Rn. 29 der Beratung der Landesregierung zur Gewährleistung der Informationssicherheit (Anlage).

Entscheidungen beschleunigen.[11] Zudem würden umfassende Kontrollbefugnisse des CIO den Stand der Informationssicherheit in den Ressorts für die Landesregierung transparent machen. Aus Sicht des LRH würde dies einen erhöhten Umsetzungsdruck in den Ressorts erzeugen.[12]

Zentralisierung der IT-Infrastruktur

Eine zentralisierte IT erzeugt nicht nur stringente Steuerungsmöglichkeiten der Informationssicherheit, sondern schafft auch Synergien. Es ist unwirtschaftlich, wenn vergleichbare IT-Dienste von mehreren Behörden und Einrichtungen des Landes separat betrieben werden. Dies schließt die mehrfache Umsetzung vergleichbarer Informationssicherheitsmaßnahmen ein. Darüber hinaus wirkt eine Zentralisierung dem Fachkräftemangel entgegen. Auch die Koalitionsvereinbarung von CDU und GRÜNEN 2022-2027 sieht eine Zusammenführung der Rechenzentren des Landes zu einem Rechenzentrumsverbund vor.[13] **15**

Rezeption des Beratungsberichts

Der Beratungsbericht wurde von den Ressorts unterschiedlich aufgenommen. Das MHKBD stimmte der Analyse und den Empfehlungen des LRH im Rahmen von Gesprächen inhaltlich grundsätzlich zu. Einzelne Ressorts äußerten sich nach Auskunft des MHKBD im Hinblick auf eine Zentralisierung der Steuerung der Informationssicherheit und der IT-Infrastruktur skeptisch. Der LRH hat keine Stellungnahme der Landesregierung zu seinem Beratungsbericht erhalten. Substantielle Fortschritte in der Sache sind für den LRH bislang nicht erkennbar. Aus Sicht des LRH sollte daher der Landtag handeln. **16**

---

11 Vgl. Rn. 30 der Beratung der Landesregierung zur Gewährleistung der Informationssicherheit (Anlage).

12 Vgl. Rn. 34 der Beratung der Landesregierung zur Gewährleistung der Informationssicherheit (Anlage).

13 Vgl. Rn. 35 - 37 der Beratung der Landesregierung zur Gewährleistung der Informationssicherheit (Anlage).

4 Handlung des Parlaments erforderlich

Bereits im Juni 2021 hat der LRH den Landtag zur Prüfung „Programm ‚Digitale Verwaltung Nordrhein-Westfalen' – Initiierung, Management und Finanzierung" beraten (siehe Vorlage 17/5319). Unter anderem hat der LRH dem Landtag damals vorgeschlagen, auf eine Stärkung des CIO in seinen Rechten und Befugnissen hinzuwirken. Zudem sollte das Abstimmungsverfahren des CIO mit den Ressorts bei der Steuerung und Koordinierung der Informationstechnik zu Gunsten des CIO deutlich vereinfacht werden. Dazu muss u. a. das EGovG NRW entsprechend angepasst werden.[14] Der Landesregierung hat der LRH in diesem Zusammenhang empfohlen, den CIO mindestens auf Staatssekretärsebene zu verorten und für ihn ein eigenes Vortragsrecht im Kabinett vorzusehen. Inhaltliche Beschlüsse zur Umsetzung der Empfehlungen des LRH hat die Landesregierung seither nicht getroffen. **17**

Der LRH empfiehlt die Stärkung des CIO auch mit Blick auf das vorliegende Thema „Informationssicherheit". Darüber hinaus hält er eine weitgehende Zentralisierung der IT bei den Rechenzentren für zielführend. **18**

Auch wenn das MHKBD der Einschätzung des LRH inhaltlich grundsätzlich folgt, sind in der Sache jedoch kaum Fortschritte erkennbar. Eine angekündigte Novellierung des EGovG NRW hat das MHKBD bisher nicht auf den Weg gebracht. Auch die ausbleibende Reaktion der Landesregierung auf den Beratungsbericht des LRH zur Informationssicherheit lässt vermuten, dass die Landesregierung sich mit der Thematik nicht mit dem gebotenen Nachdruck beschäftigt. Dies ist jedoch zur Gewährleistung der Funktionsfähigkeit der Landesverwaltung zwingend angezeigt. **19**

Vor diesem Hintergrund hat der LRH entschieden, seinen Beratungsbericht an die Landesregierung (siehe Anlage) nunmehr auch dem Landtag zuzuleiten. Der LRH regt an, dass der Landtag aus seiner Mitte heraus das EGovG NRW anpasst, um eine verstärkte **20**

---

[14] Um den CIO mehr Kompetenzen einzuräumen, sollte u. a. § 22 EGovG NRW angepasst werden. Der CIO sollte bei der Steuerung und Koordinierung der Informationstechnik in der Landesverwaltung künftig nicht mehr auf das Einvernehmen des Ministerpräsidenten und der Ressorts angewiesen sein. Stattdessen sollte er seine Entscheidungen im Benehmen mit den Genannten treffen können.

ressortübergreifende Steuerung der Informationssicherheit zu erreichen. Dabei sollten insbesondere die Befugnisse des CIO ausgeweitet werden. Zudem sollte der Landtag die Landesregierung auffordern, eine weitgehende IT-Zentralisierung anzustreben (siehe Rn. 1 f.).

Anlage

Beratung der Landesregierung durch den LRH nach § 88 Absatz 2 Landeshaushaltsordnung zur Gewährleistung der Informationssicherheit in der Landesverwaltung vom 28.03.2023 **21**

gez.
Prof. Dr. Mandt
Präsidentin

gez.
Kisseler
Vizepräsident

gez.
Dr. Hähnlein
Direktor beim LRH

gez.
Dr. Lascho
Direktor beim LRH

gez.
Zelljahn
Direktor beim LRH

gez.
Dr. Rohde
Leitender Ministerialrat

gez.
Krüger
Leitende Ministerialrätin

Anlage

Landesrechnungshof Nordrhein-Westfalen

Beratung der Landesregierung nach § 88 Absatz 2 Landeshaushaltsordnung

zur

Gewährleistung der Informationssicherheit in der Landesverwaltung

Gz.: KuP-01.07.02-000010-2023-0000687

Düsseldorf, den 28.03.2023

Abkürzungsverzeichnis*

BSI	Bundesamt für Sicherheit in der Informationstechnik
CIO	Beauftragte/r der Landesregierung für Informationstechnik
CISO	Chief Information Security Officer
EGovG NRW	E-Government-Gesetz Nordrhein-Westfalen
EGov-Rat	E-Government-Rat
EPOS.NRW	Einführung von Produkthaushalten zur Outputorientierten Steuerung – Neues RechnungsWesen
Informationssicherheitsleitlinie NRW	Leitlinie zur Informationssicherheit der Landesverwaltung Nordrhein-Westfalen
ISMS	Informationssicherheitsmanagementsystem
KG InfoSic	Koordinierungsgruppe Informationssicherheit
Landes-CISO	Informationssicherheitsbeauftragte/r der Landesverwaltung
LRH	Landesrechnungshof
Ressort-CISO	Informationssicherheitsbeauftragte/r der Ressorts
Rn.	Randnummer(n)

* Abkürzungen, soweit nicht allgemein bekannt oder aus sich heraus ohne Weiteres verständlich.

1 Informationssicherheit in der Landesverwaltung – wie aus Anspruch Wirklichkeit werden kann

Der Stand der Informationssicherheit in der Landesverwaltung ist unstreitig kritisch. Dies wiegt schwer. Das Risiko schwerwiegender Sicherheitsvorfälle ist so hoch wie nie. Deshalb muss die Landesregierung unverzüglich ein angemessenes Sicherheitsniveau für die IT-Verfahren des Landes herstellen. Hierfür muss sie die Strukturen zur Informationssicherheit auf den Prüfstand stellen. 1

Aus Sicht des Landesrechnungshofs (LRH) sollte die Landesregierung erwägen, insbesondere das Informationssicherheitsmanagement deutlich stärker als bisher als zentral gesteuerten Prozess zu etablieren. Insoweit sollte sie in Betracht ziehen, die Kompetenzen der/des Beauftragten der Landesregierung für Informationstechnik (CIO) auszuweiten. Dazu schlägt der LRH die Prüfung einer Änderung des E-Government-Gesetzes Nordrhein-Westfalen[1] (EGovG NRW) sowie eine hierarchische Anhebung der CIO-Rolle auf Staatssekretärsebene vor. Zudem sollte die Landesregierung eine weitgehende IT-Zentralisierung prüfen. 2

Die Informationssicherheit ist seit 1998 im Kern dezentral organisiert. Die Verantwortung liegt im Wesentlichen bei den jeweiligen Behörden und Einrichtungen des Landes. Hier kann aus Sicht des LRH ein bedeutendes Problem liegen. Die stark zunehmende Digitalisierung in der Landesverwaltung hat mit zahlreichen, auch ressortübergreifend[2] eingesetzten IT-Systemen einen hohen Vernetzungsgrad erreicht. Dadurch erhöht sich die Anfälligkeit der IT-Systeme für Angriffe von innen und außen. Informationssicherheit ist unteilbar: Ein schwaches Glied in der Kette kann potenziell das gesamte System gefährden. Damit ist eine im Kern dienststellenbezogene Ausrichtung des Informationssicherheitsmanagements aufgrund der fehlenden Sicht auf die Gesamtarchitektur der IT- 3

---

1 Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen vom 08.07.2016 (E-Government-Gesetz Nordrhein-Westfalen – EGovG NRW), GV. NRW. Ausgabe 2016 Nr. 22 vom 15.07.2016, S. 551, zwischenzeitlich aktualisiert, zuletzt durch Artikel 1 des Gesetzes vom 01.02.2022 (GV. NRW. S. 122), in Kraft getreten am 19.02.2022.

2 Z. B. das Landesverwaltungsnetz, Systeme der elektronischen Verwaltungsarbeit (E-Akte, E-Laufmappe), das IT-Verfahren zur Verwaltung des Landeshaushalts etc.

Landschaft nicht mehr sachgerecht. Mit Blick auf diesen Befund fordern die Rechnungshöfe des Bundes und der Länder ein zentrales Informationssicherheitsmanagement mit Befugnissen zum Durchgriff in die Ressortverantwortlichkeiten.[3]

Erste richtige Schritte wurden gemacht. In 2015 und 2016 wurden eine Informationssicherheitsleitlinie erlassen sowie das EGovG NRW verabschiedet. Darin wurde mit der/dem CIO auch eine ressortübergreifende Verantwortungsebene für die Informationssicherheit geschaffen. Die/Der CIO moderiert jedoch mehr, als dass sie/er steuert. Landesweite Richtlinien und Priorisierungen zur Informationssicherheit können nur in schwergängigen Abstimmungs- und Einvernehmensverfahren mit den Ressorts vorgegeben werden. Auch dezentrale IT-Strukturen in der Landesverwaltung erschweren eine stringente Steuerung der Informationssicherheit. **4**

Was fehlt? Aus Sicht des LRH mangelt es an hinreichenden zentralen Strukturen und einer Steuerung aus einer Hand. Der vorliegende Bericht will einen Beitrag dazu leisten, wie dieser Zustand überwunden werden kann. **5**

[3] Vgl. Grundsatzpapier zum Informationssicherheitsmanagement der Rechnungshöfe des Bundes und der Länder, S. 9 (abrufbar unter: https://lrh.nrw.de/index.php/veroeffentlichungen/gemeinsame-veroeffentlichungen-der-rechnungshoefe-des-bundes-und-der-laender).

2 Informationssicherheit ist unverzichtbar

Die Gewährleistung von Informationssicherheit ist für die Funktionsfähigkeit der Landesverwaltung mit Blick auf die fortschreitende Digitalisierung unverzichtbar. Cyber-Angriffe[4] von außen oder auch Manipulationen von innen können zu schwerwiegenden Systemausfällen führen und erhebliche wirtschaftliche Schäden verursachen. Aufgrund der Abhängigkeit der Funktionsfähigkeit der Landesverwaltung von den eingesetzten IT-Verfahren muss die Herstellung eines angemessenen Sicherheitsniveaus höchste Priorität besitzen. 6

Nach aktueller Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist die Gefährdungslage im Cyber-Raum in Deutschland so hoch wie nie.[5] Vergleichbares gilt nach Feststellungen des Ministeriums des Innern und des Landeskriminalamts auch für NRW.[6] Die Lage wird von Oberstaatsanwalt Markus Hartmann, Leiter der Zentral- und Ansprechstelle Cybercrime mit Sitz in Köln, wie folgt bewertet: „Die Kriminellen greifen jedes Ziel an, das angreifbar ist. Also überall dort, wo sich Sicherheitslücken finden und die Verteidigungsstrategie nicht gut funktioniert“.[7] Diese Einschätzungen werden durch verschiedene, öffentlich bekannt gewordene IT-sicherheitsrelevante Vorfälle deutlich unterstrichen.[8] Z. B. wurde im Oktober 2022 der 7

---

4 Angriffe über den virtuellen Raum der weltweit vernetzten IT-Systeme mit dem Ziel der Beeinträchtigung von IT-Systemen.

5 Vgl. Pressemitteilung des BSI vom 25.10.2022, abrufbar unter: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/221025_Lagebericht.html#:~:text=Vizepr%C3%A4sident%20des%20BSI%20%2C%20Dr.,gegen%20IT%20%2DSicherheitsvorf%C3%A4lle%20ger%C3%BCstet%20haben.

6 Vgl. Bericht zur Cybersicherheit in Nordrhein-Westfalen 2021, abrufbar unter https://www.cybersicherheit.nrw/system/files/media/document/file/cybersicherheitsbericht2021.pdf: „Bereits im Jahr 2020 war ein Anstieg der Fallzahlen im Bereich Cybercrime zu beobachten, dieser Trend setzte sich auch im Jahr 2021 fort.“; vgl. Lagebild Cybercrime 2021, abrufbar unter: https://polizei.nrw/sites/default/files/2022-12/221028_Lagebild_CC_2021.pdf: Gesamtschaden i. H. v. 24,2 Millionen € und rd. 24 Prozent mehr Cybercrime-Fälle als in 2020.

7 Zitiert nach Rheinischer Post vom 10.12.2022: Hacker: Cyberangriffe auf Städte und Universitäten in NRW (rp-online.de), die hervorhebt, dass „(es) Kriminelle Hacker … aktuell besonders auf Kommunen, staatliche Organisationen und Unternehmen in NRW abgesehen (haben)“.

8 Z. B. musste sich das Universitätsklinikum Düsseldorf in NRW 2020 aufgrund eines Cyber-Angriffs insgesamt 13 Tage von der Notfallversorgung abmelden und wurde vom Rettungsdienst nicht angefahren. Vgl. Pressemitteilung des Universitätsklinikums Düsseldorf vom 12.10.2020, abrufbar unter: https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/wieder-normale-patientenzahlen-nach-it-ausfall.

In 2021 wurde im Landkreis Anhalt-Bitterfeld (Sachsen-Anhalt) nach einem Cyber-Angriff der Katastrophenfall ausgerufen. Hier wurden von den Angreifern auf Servern gespeicherte Daten verschlüsselt und Dienstleistungen der Verwaltung waren nicht mehr verfügbar. Vgl. Nachricht des MDR Sachsen-Anhalt vom 02.02.2022, abrufbar unter: https://www.mdr.de/nachrichten/sachsen-anhalt/dessau/bitterfeld/cyberangriff-katastrophenfall-anhalt-bitterfeld-aufgehoben-100.html.

Rhein-Pfalz-Kreis Opfer eines Hackerangriffs. Hierzu war in der Süddeutschen Zeitung zu lesen[9]: „Auch in Ludwigshafen ging erst mal gar nichts mehr. Wie so ein Hackerangriff ausgehen kann, lässt sich dort beobachten: Erst nach fünf Wochen konnten die Mitarbeiterinnen und Mitarbeiter in ihre Büros zurück, erst dann liefen die Telefone wieder.“ Ende 2022 wurde die Universität Duisburg-Essen das Ziel von Cyber-Angriffen.[10] Die IT-Infrastruktur der Universität sei dabei fast vollständig lahmgelegt worden. U. a. hätten die unbekannten Täter erbeutete Daten ins Darknet[11] gestellt, weil die Hochschule kein Geld an die Erpresser zahlen wollte. Als weiteres Beispiel für die deutschlandweit bestehende Bedrohungslage sei auf einen Vorfall Ende 2022 in der Stadt Potsdam hingewiesen. Dort musste die Stadt nach Hinweisen von Sicherheitsbehörden auf einen möglicherweise bevorstehenden Hackerangriff ihre Systeme vorsorglich abschalten. Sie konnte dementsprechend z. B. Dienstleistungen für Bürger nicht erbringen.[12]

Die bestehende Gefährdungslage und der Umgang mit den Herausforderungen der Informationssicherheit sind auch Thema im Landtag NRW. Die Fraktion der CDU und die Fraktion BÜNDNIS 90/DIE GRÜNEN fordern in einem Antrag[13] die Entwicklung einer neuen Strategie zur Informationssicherheit. Der Landtag soll die Landesregierung u. a. beauftragen zu prüfen, wie ein kontinuierlicher Prozess zur Überprüfung, Umsetzung und Weiterentwicklung von Sicherheitsmaßnahmen eingerichtet werden kann. Zudem soll die IT-Grundschutz-Methodik des BSI flächendeckend umgesetzt werden. **8**

In 2022 konnten nach einem Cyber-Angriff gegen das Suhler Rathaus (Thüringen) sämtliche Ämter der Stadtverwaltung nicht mehr arbeiten. Vgl. Nachricht des MDR Thüringen vom 11.03.2022, abrufbar unter: https://www.mdr.de/nachrichten/thueringen/sued-thueringen/suhl/hackerangriff-rathaus-polizei-100.html.

Auch Berichte über Cyber-Gefahren im Zusammenhang mit der aktuellen internationalen Konfliktlage verdeutlichen die Bedeutung des Themas Informationssicherheit. Vgl. Pressemitteilung des BSI zur Lageeinschätzung, abrufbar unter: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220225_Angriff-Ukraine-Statement.html.

9 Vgl. Bericht der Süddeutschen Zeitung „Wenn Hacker alles lahmlegen“, Ausgabe Donnerstag/Freitag, 5./6. Januar 2023, Nr. 4.

10 Vgl. Bericht des WDR vom 20.01.2023, abrufbar unter: https://www1.wdr.de/nachrichten/ruhrgebiet/uni-duisburg-essen-normalzustand-nach-hackerangriff-fuer-sommer-geplant-100.html.

11 Teil des Internets, der nicht auf herkömmliche Weise auffindbar ist. Die Kommunikation wird verschlüsselt und die Urheber der Inhalte sowie seine Besucher bzw. Konsumenten wollen möglichst anonym bleiben. (Quelle: BSI).

12 Vgl. Bericht ZEIT ONLINE vom 03.01.2023, abrufbar unter: https://www.zeit.de/digital/2023-01/cybersicherheit-potsdam-internet-sicherheit.

13 Vgl. Drucksache 18/2543 vom 17.01.2023. Vgl. in diesem Zusammenhang auch den Antrag der Fraktion der FDP vom selben Tag (Drucksache 18/2564).

3 Informationssicherheit nicht ausreichend gewährleistet

Der LRH hat sich mit der Gewährleistung einer angemessenen Informationssicherheit seit 2002 in verschiedenen Prüfungen auseinandergesetzt[14]. Zuletzt waren dies die Prüfungen des IT-Verfahrens zur Verwaltung des Landeshaushalts (EPOS.NRW[15])[16] und des Notfallmanagements innerhalb der Landesverwaltung. Die dabei gewonnenen Erkenntnisse zeugen davon, dass die Belange der Informationssicherheit in der Praxis noch nicht richtig priorisiert werden. **9**

Der LRH hat bei seinen oben in Bezug genommenen Prüfungen immer wieder eine mangelhafte Umsetzung der in der Landesverwaltung zu beachtenden Empfehlungen des BSI festgestellt. Insbesondere war in den geprüften Stellen kein ausreichendes Informationssicherheitsmanagementsystem (ISMS) etabliert. Ein ISMS beinhaltet Regelungen zur Steuerung der Informationssicherheit einer Institution. Der Informationssicherheitsprozess muss geplant, umgesetzt, kontrolliert und regelmäßig optimiert werden. Die geprüften Stellen haben in ihren Stellungnahmen die Einschätzungen des LRH zur Informationssicherheit im Wesentlichen anerkannt. Auch im Rahmen der jüngst durchgeführten Prüfung des Notfallmanagements innerhalb der Landesverwaltung haben die geprüften Stellen den Feststellungen und Bewertungen des LRH zur Informationssicherheit nicht widersprochen. Teilweise stimmten sie der Empfehlung des LRH ausdrücklich zu, dass die Informationssicherheit bzw. die Umsetzung des IT-Grundschutzes zu priorisieren sei. **10**

Die beim IT-Verfahren EPOS.NRW festgestellten gravierenden Sicherheitsmängel sind ein besonders deutliches Beispiel für die unzulängliche Priorisierung der Informationssicherheit. Denn hier wurden erste Teilsysteme bereits 2010 in Betrieb genommen und **11**

---

14 Z. B. Orientierungsprüfung IT-Sicherheit (Jahresbericht 2003, S. 79 ff.), Prüfung der IT-Services und IT-Schulungen in der Landesverwaltung (Jahresbericht 2005, S. 110 ff.), IT-Einsatz beim Sondervermögen Bau- und Liegenschaftsbetrieb NRW sowie beim Landesbetrieb Wald und Holz NRW (Jahresbericht 2010, S. 114 ff.) und IT-Einsatz in den Hochschulen (Jahresbericht 2016, S. 86 ff.), jeweils abrufbar unter https://lrh.nrw.de.

15 EPOS.NRW ist der Name des Programms zur Reform des Haushalts- und Rechnungswesens in Nordrhein-Westfalen. Die Abkürzung EPOS.NRW bedeutet: Einführung von Produkthaushalten zur Outputorientierten Steuerung – Neues RechnungsWesen.

16 Jahresbericht 2022, S. 107 ff., abrufbar unter https://lrh.nrw.de.

die landesweite Einführung Ende 2019 abgeschlossen. Trotzdem war das Informationssicherheitskonzept des IT-Verfahrens nach Mitteilung der für das Verfahren zuständigen Stelle auch Anfang 2023 noch nicht vollständig umgesetzt. Das fällt aus Sicht des LRH erheblich ins Gewicht. Dieses IT-Verfahren hat für die Landesverwaltung eine herausragende Bedeutung. Mit ihm werden jährlich rd. 95 Milliarden €[17] verwaltet und die Zahlungsvorgänge der Landesverwaltung verbucht. Bei dem System handelt es sich um eine für die Funktionsfähigkeit der Landesverwaltung kritische Infrastruktur, die besonders zu sichern ist.[18]

12 Der Landesregierung ist die Problematik der mangelhaften Beachtung der Anforderungen an die Informationssicherheit auch aus eigenen Quellen bekannt. Dies hat der LRH bei seiner Prüfung Notfallmanagement innerhalb der Landesverwaltung festgestellt. Im Mai 2021 bewertete eine Vorlage in dem ressortübergreifend besetzten Gremium E-Government-Rat (EGov-Rat)[19] den Stand der Informationssicherheit in der Landesverwaltung unverändert als kritisch. Grundlegende Sicherheitsmaßnahmen hätten noch nicht umgesetzt werden können. Zur Vermeidung von schwerwiegenden Sicherheitsvorfällen und einer Gefährdung der Digitalisierung der Landesverwaltung müsse u. a. ein deutlich höherer Arbeitszeitanteil für die Informationssicherheit durch die hierfür Verantwortlichen aufgewendet werden. Dafür, dass die Landesregierung im Bereich der Informationssicherheit Handlungsbedarf sieht, spricht im Übrigen, dass sie erst kürzlich eine IT-Steuerungsgruppe auf der Ebene der Staatssekretärinnen und Staatssekretäre eingesetzt hat. Diese soll sich offenbar auch mit Fragen der Informationssicherheit beschäftigen.[20] Einzelheiten bleiben insoweit bislang aber unklar.

---

17 Stand 21.12.2022, vgl. Gesetz über die Feststellung des Haushaltsplans des Landes Nordrhein-Westfalen für das Haushaltsjahr 2023, GV. NRW. 2022 S. 1137.

18 Die Folgen einer Manipulation oder eines (längerfristigen) Ausfalls von EPOS.NRW können enorm sein, da ggf. zahlungswirksame Vorgänge nicht mehr verbucht werden könnten. Die Verwaltung könnte keine Leistungen mehr beziehen und keine Gelder mehr auszahlen. Dies beträfe Löhne und Gehälter, ebenso wie den Einkauf von Waren und Dienstleistungen, aber auch so scheinbar banale Dinge wie z. B. Kraftstoff für die Fahrzeuge der Sicherheitskräfte.

19 Der EGov-Rat ist unter dem Vorsitz der/des CIO auf Ebene der Abteilungsleitungen der Ministerien eingerichtet (vgl. § 13a Gemeinsame Geschäftsordnung für die Ministerien des Landes Nordrhein-Westfalen). Er berät und entscheidet u. a. bei ressortübergreifenden Angelegenheiten im Zusammenhang mit der Umsetzung des EGovG NRW sowie der Informationstechnik.

20 Vgl. Drucksache 18/3426 vom 07.03.2023.

4 Regelungen zur Informationssicherheit

Für die Behörden und Einrichtungen der Landesverwaltung ist bei der Umsetzung von Maßnahmen zur Informationssicherheit bereits seit 1998 der Einsatz der Methodik des BSI zum IT-Grundschutz[21] vorgeschrieben.[22] 13

Am 23.06.2015 hat die Landesregierung darüber hinaus die Leitlinie zur Informationssicherheit der Landesverwaltung NRW (Informationssicherheitsleitlinie NRW)[23] beschlossen. Sie trat am 01.07.2015 in Kraft. Danach obliegt die Gesamtverantwortung für die Informationssicherheit zur Gewährleistung einer ordnungsgemäßen und sicheren Aufgabenerledigung den Mitgliedern der Landesregierung im Rahmen des in Artikel 55 der Landesverfassung verankerten Ressortprinzips. Für die Umsetzung geeigneter Maßnahmen im Sinne der Leitlinie sind die Leiterinnen und Leiter der Behörden und Einrichtungen des Landes verantwortlich.[24] 14

Gemäß der Informationssicherheitsleitlinie NRW besteht die Sicherheitsstrategie der Landesregierung darin, mit wirtschaftlichem Ressourceneinsatz ein höchst mögliches Maß an Sicherheit zu erreichen. Dazu soll ein ressortübergreifendes ISMS etabliert werden. Dieses hat sich an der IT-Grundschutz-Methodik des BSI zu orientieren. Auf dieser Grundlage sollen die Ressorts eigene ISMS aufbauen, dazu gehört auch die Benennung von Informationssicherheitsbeauftragten im jeweiligen Geschäftsbereich.[25] Für diese ressortübergreifenden und -internen Maßnahmen hatte die Landesregierung (parallel mit der Inkraftsetzung der Leitlinie) 60 zusätzliche Stellen und finanzielle Mittel in Höhe von rd. 8,3 Millionen € jährlich bereitgestellt. 15

---

21 Das BSI stellt mit dem sogenannten IT-Grundschutz eine Methodik zur Verfügung, mit der eine Organisation ein dem eigenen Schutzbedarf angemessenes IT-Sicherheitsniveau etablieren kann. Die Methodik ermöglicht, durch ein systematisches Vorgehen notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen.

22 Vgl. Runderlass zur Anwendung des IT-Grundschutzhandbuches des Ministeriums für Inneres und Justiz zugleich im Namen des Ministerpräsidenten und aller Landesministerien vom 22.08.1998, MBl. NRW. 1998 S. 1014.

23 Nicht öffentlich abrufbar.

24 Vgl. Ziffer 4 Informationssicherheitsleitlinie NRW.

25 Vgl. Ziffer 5 Informationssicherheitsleitlinie NRW.

Mit Inkrafttreten der Informationssicherheitsleitlinie NRW hat die Landesregierung in 2015 die Koordinierung der Umsetzung der Leitlinie und der Sicherheitsstrategie der/dem CIO übertragen.[26] Die/Der CIO ist der Landesregierung gegenüber berichtspflichtig. Sie/er soll in Abstimmung mit den Ressorts Entscheidungen über ressortübergreifende Richtlinien und Regelungen zur Informationssicherheit in der Landesverwaltung herbeiführen.[27] 16

Seit 2016 ist die/der CIO nach § 22 Abs. 1 Satz 1 EGovG NRW zuständig für die Steuerung und Koordinierung der Informationstechnik in der Landesverwaltung und legt insbesondere die technischen und organisatorischen Rahmenbedingungen für deren Einsatz in Abstimmung mit der Ministerpräsidentin oder dem Ministerpräsidenten und den Ministerien fest. 17

Hierzu stimmen die Ministerpräsidentin oder der Ministerpräsident und die Ministerien die informationstechnischen Vorhaben ihrer Geschäftsbereiche mit der/dem CIO ab (§ 22 Abs. 2 EGovG NRW). 18

Gesetzlich ist in § 22 Abs. 3 Nr. 5 EGovG NRW konkret festgelegt, dass die/der CIO die Informationssicherheit in der Landesverwaltung koordiniert und zentrale informationstechnische Sicherheitskomponenten bereitstellt. 19

Die/Der CIO hat gemäß der in der Informationssicherheitsleitlinie NRW beschriebenen Organisationsstruktur die/den Informationssicherheitsbeauftragte/n der Landesverwaltung (Landes-CISO) benannt.[28] Diese/r plant und koordiniert in Abstimmung mit den Informationssicherheitsbeauftragten der Ressorts (Ressort-CISO) das ressortübergreifende ISMS. Dazu initiiert und koordiniert sie/er die Erstellung und Fortschreibung ressortübergreifender Richtlinien und Regelungen zur Informationssicherheit. Sie/er überprüft diese regelmäßig mit dem Ziel, Defizite zu erkennen und zu beheben. Zudem leitet sie/er die ressortübergreifend besetzte Koordinierungsgruppe Informationssicherheit 20

---

[26] Vgl. Ziffer 7.1 und Ziffer 7.2 Informationssicherheitsleitlinie NRW.

[27] Vgl. Ziffer 7.2 Informationssicherheitsleitlinie NRW.

[28] Vgl. Ziffer 7.2 Informationssicherheitsleitlinie NRW. CISO ist die Abkürzung für „Chief Information Security Officer“.

(KG InfoSic)[29] und hat die/den CIO über den Stand der Informationssicherheit in der Landesverwaltung zu unterrichten.[30]

Die Ressort-CISO sind für die Koordination des Informationssicherheitsprozesses im jeweiligen Geschäftsbereich verantwortlich. Sie unterstützen die/den Landes-CISO in allen Fragen der Informationssicherheit, insbesondere bei der Erstellung von Berichten. Die Aufgaben und Befugnisse der Ressort-CISO regeln die Ressorts.[31] **21**

[29] Die KG InfoSic als Informationssicherheitsmanagement-Team unterstützt und berät die/den Landes-CISO in Fragen der Informationssicherheit. Sie wirkt bei der Entwicklung der ressortübergreifenden Regelungen für die Informationssicherheit sowie IT-Sicherheitsstandards mit. Sie besteht aus der/dem Landes-CISO als Vorsitzenden und den Ressort-CISO der Landesverwaltung NRW. Vgl. Ziffer 7.4 Informationssicherheitsleitlinie NRW.

[30] Vgl. Ziffer 7.3 Informationssicherheitsleitlinie NRW.

[31] Vgl. Ziffer 7.5 Informationssicherheitsleitlinie NRW.

5 CIO: Moderation statt Steuerung

Mit der Informationssicherheitsleitlinie aus 2015 sowie der Festschreibung der Koordinierungsfunktion der/des CIO im EGovG NRW hat die Landesregierung beim Informationssicherheitsmanagement in der Landesverwaltung grundsätzlich zentrale Strukturen unter ihrer Gesamtverantwortung eingerichtet. Für die operative Umsetzung konkreter Maßnahmen der Informationssicherheit sind aber nach wie vor die Ressorts selbst (bzw. die jeweiligen Behörden und Einrichtungen) verantwortlich.[32] Daher ist das operative Informationssicherheitsmanagement in der Landesverwaltung im Kern weiterhin dezentral organisiert. Die CIO-Rolle moderiert somit mehr, als dass sie steuert. **22**

Ressortübergreifende Vorgaben oder Priorisierungen zur Informationssicherheit nach dem EGovG NRW unterliegen einem aufwendigen Abstimmungsprozess (siehe Rn. 17). Zur Abstimmung und Koordinierung der Umsetzung der zahlreichen Maßnahmen des EGovG NRW zwischen den Ressorts ist der EGov-Rat[33] als zentrales, ressortübergreifendes Gremium eingerichtet. In diesem sind unter Vorsitz des/der CIO alle Ressorts auf Ebene der für E-Government verantwortlichen Abteilungsleitungen vertreten. Beschlüsse des EGov-Rates werden nach seiner Geschäftsordnung[34] mit einfacher Mehrheit der Stimmberechtigten getroffen. Die Beschlüsse sind verbindlich, wenn im Nachgang kein Mitglied die Befassung der Staatssekretärskonferenz mit den getroffenen Entscheidungen fordert. Ferner können auch die Ressorts nach Beschlussfassung fordern, dass sich die Staatssekretärskonferenz und ggf. das Kabinett mit den Mehrheitsentscheidungen befasst. Im Ergebnis sind Abreden im EGov-Rat grundsätzlich nur dann verbindlich, wenn kein Ressort Widerspruch dagegen erhebt. Umgekehrt bedeutet dies, dass Beschlüsse im EGov-Rat, welche alle Ressorts gleichermaßen zur Umsetzung von Maßnahmen des EGovG NRW verpflichten, somit nur dann getroffen werden dürften, wenn alle Ressorts mit diesen einverstanden sind. **23**

---

[32] Im Rahmen des in Art. 55 Abs. 2 der Landesverfassung verankerten Ressortprinzips, vgl. auch entsprechend Ziffer 4 Informationssicherheitsleitlinie NRW.

[33] Vgl. § 13a Abs. 1 Gemeinsame Geschäftsordnung für die Ministerien des Landes Nordrhein-Westfalen (GGO) mit Stand vom 24.01.2023, MBl. NRW. 2014, S. 826.

[34] Nicht öffentlich abrufbar.

Bezogen auf die Rolle des CIO ist sie/er auch im EGov-Rat nur Moderator und besitzt keine formalen Durchsetzungsmöglichkeiten. In dem Fall, in dem Beschlussgegenstände in die Staatssekretärs- oder Kabinettsebene eskaliert werden, nimmt die Möglichkeiten des/der CIO zur Einflussnahme weiter ab, da die/der CIO in diesen Formaten kein Stimmrecht besitzt. **24**

Auch ressortübergreifende Vorgaben oder Priorisierungen zur Informationssicherheit im Weg von Verwaltungsvorschriften unterliegen einem aufwendigen Abstimmungsprozess. Für den Erlass von entsprechenden Verwaltungsvorschriften zur Informationssicherheit durch das für Digitalisierung zuständige Ministerium ist das Einvernehmen mit der Ministerpräsidentin oder dem Ministerpräsidenten und den Ministerien vorgeschrieben (§ 23 Abs. 2 Nr. 10 EGovG NRW). Dieses setzt wiederum Einstimmigkeit zwischen den Ressorts voraus. **25**

Auch in der Informationssicherheitsleitlinie NRW wird die (lediglich) koordinierende Funktion der/des CIO festgeschrieben.[35] Selbstständige Kontrollen zur Umsetzung der Informationssicherheit in den Ressorts kann sie/er nicht durchführen. Zwar hat die Landesregierung in der Informationssicherheitsleitlinie NRW Berichtspflichten der Ressorts (über die/den Landes-CISO) an die/den CIO festgelegt. Darüber hinaus hat aber z. B. die/der CIO keine Möglichkeit, in den Ressorts den Umsetzungsstand konkreter Maßnahmen zur Informationssicherheit selbst zu überprüfen.[36] **26**

---

35 Vgl. Ziffern 7.2 und 7.3 Informationssicherheitsleitlinie NRW.

36 Vgl. Ziffern 7.2 bis 7.5 Informationssicherheitsleitlinie NRW.

6 CIO stärken und IT zentralisieren

Die unzureichende Umsetzung der Informationssicherheit in der Landesverwaltung ist unstreitig (vgl. Rn. 12). Die Pflicht zur Umsetzung des BSI-Grundschutzes besteht mit Erlass von 1998. Der Beschluss der Informationssicherheitsleitlinie (2015) und die Verabschiedung des EGovG NRW (2016), mit denen u. a. die ressortübergreifenden Koordinierungsfunktion der/des CIO etabliert wurde, waren Schritte in die richtige Richtung (siehe Kapitel 4). Diese Vorgaben und die darauf beruhenden strukturellen Verbesserungen haben jedoch noch nicht zu einem angemessenen Informationssicherheitsniveau in der Landesverwaltung geführt. **27**

Die Landesregierung sollte daher untersuchen, inwieweit die bestehenden Strukturen für Informationssicherheit weiterentwickelt werden müssen. Dies umso mehr, da die IT der Landesverwaltung im hohen Grade ressortübergreifend vernetzt ist. Mit Blick auf diesen Befund fordern die Rechnungshöfe des Bundes und der Länder ein zentrales ISMS mit Befugnissen zum Durchgriff in die Ressortverantwortlichkeiten.[37] Die Kompetenzen der/des CIO in NRW sind in den Regelungen des EGovG NRW und der Informationssicherheitsleitlinie NRW diesbezüglich zu schwach ausgeprägt. Daher sollte für die/den CIO eine Ausweitung der Befugnisse für eine stringentere Steuerung des ISMS geprüft werden (siehe 6 a.). Zudem sollten der/dem CIO umfassende Kontrollbefugnisse in Bezug auf die Informationssicherheit eingeräumt werden (siehe 6 b.). Für eine stringentere Steuerung der Informationssicherheit ist ferner auch eine weitgehende Zentralisierung der IT zu prüfen (siehe 6 c.). **28**

---

[37] Vgl. Grundsatzpapier zum Informationssicherheitsmanagement der Rechnungshöfe des Bundes und der Länder, S. 9 (abrufbar unter: https://lrh.nrw.de/index.php/veroeffentlichungen/gemeinsame-veroeffentlichungen-der-rechnungshoefe-des-bundes-und-der-laender).

Hierzu im Einzelnen:

a. Mehr Steuerungskompetenzen für die CIO-Rolle

Der LRH regt an, eine Änderung der §§ 22 und 23 EGovG NRW zu prüfen. Es sollte in Erwägung gezogen werden, die dort festgelegten Abstimmungs- und Einvernehmensregelungen zwischen der/dem CIO bzw. dem für Digitalisierung zuständigen Ministerium einerseits und der Ministerpräsidentin oder dem Ministerpräsidenten und den Ressorts andererseits (siehe Kapitel 5) zu Gunsten der/des CIO bzw. des für Digitalisierung zuständigen Ministeriums durch eine Benehmensregelung zu ersetzen. Hierdurch könnten effektiv zentrale Verwaltungsvorschriften mit Vorgaben zentraler Standards für die Informationssicherheit erlassen werden. Die Benehmensregelung hätte dabei zur Folge, dass die/der CIO sowie ggf. das für Digitalisierung zuständige Ministerium die Ressorts anhören und sich mit ihren Erwägungen auseinander setzen müssten.[38] Anders als beim Einvernehmen würde aber keine Zustimmung der beteiligten Ressorts – ebenso wenig wie eine Willensübereinstimmung – verlangt.[39] **29**

Auch die Verortung der CIO-Rolle auf Staatssekretärsebene mit eigenem Vortragsrecht im Kabinett sollte die Landesregierung prüfen.[40] Der unmittelbare Kabinettzugang kann Entscheidungen betreffend die Informationssicherheit beschleunigen. **30**

Der LRH fordert schon seit Jahren und zuletzt mit Entscheidung vom 31.03.2022, die Rechte und die Stellung der/des CIO entsprechend zu stärken.[41] In der Prüfung, die dieser Entscheidung zugrunde lag[42], hat der LRH das Programm der Landesregierung zur Umsetzung der digitalen Transformation der Verwaltungsarbeit untersucht. Er stellte **31**

---

38 Vgl. z. B. BVerwG, Urteil vom 29.04.1993 - 7 A 2_92, NVwZ 1993, 890 (892); vgl. VGH München, Urteil vom 09.12.2003 - 7 N 02.1381, BayVGHE 57, 70; VG Gelsenkirchen Beschluss vom 31.07.2008 – 4 L 764_08, BeckRS 2008, 39443.

39 Ebenda.

40 Zehn von 16 Bundesländern sowie der Bund haben eine(n) CIO (bzw. eine vergleichbare Funktion) mindestens auf der Staatssekretärsebene eingerichtet.

41 Vgl. Vorlage 17/6715: „Beratung des Landtags nach § 88 Absatz 2 Landeshaushaltsordnung zur Prüfung „Programm ‚Digitale Verwaltung Nordrhein-Westfalen' – Initiierung, Management und Finanzierung" – Schriftliche Stellungnahme des LRH zu dem Bericht des MWIDE vom 07.03.2022“.

42 Vgl. Vorlage 17/5319: „Beratung des Landtags nach § 88 Absatz 2 Landeshaushaltsordnung zur Prüfung „Programm ‚Digitale Verwaltung Nordrhein-Westfalen' – Initiierung, Management und Finanzierung".

fest, dass die damaligen erzielten Ergebnisse deutlich hinter den Planungen zurücklagen – trotz eines hohen Ressourceneinsatzes. Aus Sicht des LRH waren dafür die schwergängige Struktur und Organisation des Programms verantwortlich. Als Programmverantwortliche/r hatte die/der CIO insbesondere im Zusammenspiel mit den Ressorts nur eingeschränkte Steuerungsmöglichkeiten. Zur Umsetzung des Programms war die/der CIO nach den Regelungen des EGovG NRW auf das Einvernehmen mit den Ressorts angewiesen. Unterschiedliche Interessenlagen führten hier zu zeitaufwendigen Diskussions- und Eskalationsprozessen, die in der Folge die Digitalisierung bremsten. Dies kann sich NRW als eine der bedeutendsten Wirtschaftsregionen Europas nicht leisten. Für eine moderne und leistungsfähige Verwaltung stellt die Digitalisierung ein maßgebliches Element dar. Vor diesem Hintergrund hat der LRH eine gesetzliche Stärkung der ressortübergreifenden Kompetenzen der/des CIO sowie eine Verortung der CIO-Rolle auf Staatssekretärsebene angeregt. Die Anregungen des LRH hat die Landesregierung bisher nicht aufgegriffen.

Eine vergleichbare Sachlage besteht hinsichtlich der Informationssicherheit. Auch hier **32**
kann die/der CIO bzw. das für Digitalisierung zuständige Ministerium landesweite Vorgaben und Regelungen zur ähnlich komplexen Umsetzung der Informationssicherheit nur im Einvernehmen mit den Ressorts treffen. Aus Sicht des LRH ist es aufgrund der vergleichbaren Strukturen und Probleme bei lebensnaher Würdigung zu erwarten, dass die bislang nicht hinreichende Umsetzung der Informationssicherheit in der Landesverwaltung durch die empfohlenen Maßnahmen (siehe Rn. 27 und 28) beschleunigt werden kann.

Wie auch schon in der Entscheidung des LRH vom 31.03.2022 ausgeführt, steht einer **33**
Erweiterung ressortübergreifender Kompetenzen die in Art. 55 Abs. 2 der Verfassung für das Land Nordrhein-Westfalen im Rahmen des Ressortprinzips garantierte Organisationshoheit der Ministerien nicht entgegen.[43] Denn die Informationssicherheit gewährleistet, dass die Ressorts die ihnen obliegenden Aufgaben wahrnehmen können. Sie hat

---

[43] Vgl. *Schönenbroicher* in: Heusch/Schönenbroicher, Die Landesverfassung Nordrhein-Westfalen, 2. Aufl., 2020, Art. 55 Rn. 37: „Die Ressortkompetenz vermittelt keinen Freibrief für den eigensinnigen Aufbau und Betrieb nicht abgestimmter (Doppel-) Strukturen auf Kosten des Steuerzahlers […] insbesondere hinsichtlich umfassender eigener Servicestrukturen […]. […] All dies ist verfehlt und widerspricht nicht nur dem Prinzip der ‚Kabinettsolidarität', sondern auch den Prinzipien der effizienten und sparsamen Mittelbewirtschaftung."

also eine rein „dienende“ Funktion (im Gegensatz zu einer „lenkenden“ Funktion).[44] Die Sachkompetenz der Ressorts wird durch aufgabenneutrale Vorgaben (Kommunikations- und Sicherheitsstandards, gemeinsame Anwendungen, gemeinsames Behördennetz) in der Regel nicht berührt.[45]

b. Mehr ressortübergreifende Kontrollbefugnisse für die CIO-Rolle

Der LRH regt an zu prüfen, der/dem CIO umfassendere Kontrollbefugnisse im Hinblick auf die Informationssicherheit einzuräumen. Der Stand der Informationssicherheit und der jeweils bestehende Handlungsbedarf in den Ressorts sollte jederzeit „unabhängig“ festgestellt werden können. Z. B. könnte durch regelmäßige Audits[46] auch die Dringlichkeit der dort erforderlichen Maßnahmen zentral identifiziert und bewertet werden.[47] Damit wird regelmäßig der aktuelle Stand der Informationssicherheit in den Ressorts für den CIO und die Landesregierung transparent. Dies erzeugt aus Sicht des LRH bei den Ressorts einen erhöhten Umsetzungsdruck. **34**

c. Weitgehende Zentralisierung der IT bei den Rechenzentren des Landes

Der LRH hat auf der Grundlage eigener Prüfungen bereits Empfehlungen zu einer weitgehenden IT-Zentralisierung ausgesprochen.[48] Es ist nicht wirtschaftlich, dass IT-Dienste, die mehrere Behörden und Einrichtungen des Landes in vergleichbarer Weise nutzen, von jeder dieser Stellen separat vorgehalten und betrieben werden. Diese IT-Dienste erfordern jeweils auch vergleichbare Maßnahmen zur Informationssicherheit, die durch das „dezentral“ vorgehaltene IT-Personal umgesetzt werden müssen. **35**

---

44 Vgl. auch z. B. das Positionspapier der Arbeitsgruppe „Zukunft“ der BLK für Datenverarbeitung, „Rechtliche Rahmenbedingungen des Einsatzes standardisierter Informationstechnik der Bundes- und der Landesverwaltung in der Justiz“, Stand: 29.04.2009, abrufbar unter: https://jurpc.de/jurpc/show?id=20090202&q=*%3A*, unter II. 5. Lit. c), zuletzt abgerufen am 18.07.2022.

45 Vgl. entsprechend, mit Bezug auf das Grundgesetz: *Steinmetz*, IT – Standardisierung und Grundgesetz – Rechtsprobleme bei der technischen Vernetzung der Verwaltung, 2010, S. 104; vgl. auch *Liesegang*, in: von Münch, Grundgesetz, 2. Aufl., 1983, Art. 65 Rn. 30, der die grds. Möglichkeit der organisatorischen Zusammenfassung von Querschnittsfunktionen anerkennt; vgl. i. Ü. Grundsätze für die Verwaltungsorganisation der Rechnungshöfe des Bundes und der Länder, 05.12.2016, S. 10, abrufbar unter www.lrh.nrw.de.

46 Als Audit (audire = hören, zuhören) wird eine systematische, unabhängige Prüfung von Aktivitäten und deren Ergebnissen bezeichnet (IT-Grundschutz-Kompendium des BSI, DER.3.1 Audits und Revisionen).

47 Zur Bedeutung von Audits für das Informationssicherheitsmanagement vgl. ebenda.

48 Vgl. Prüfung IT-Strukturen in der Landesverwaltung (Jahresbericht 2015, S. 80 ff.), abrufbar unter https://lrh.nrw.de.

Die Vorlage an den EGov-Rat (vgl. Rn. 12) zeigt auf, dass bei den dezentral betriebenen IT-Verfahren offenbar kein ausreichendes Sicherheitsniveau gewährleistet werden kann. IT-Zentralisierungen werden auch im kommunalen Bereich diskutiert, um gemeinsam ein höheres Sicherheitsniveau erreichen zu können.[49] Insbesondere vor dem Hintergrund des IT-Fachkräftemangels[50] ist es nach Auffassung des LRH fraglich, ob die Informationssicherheit bei Beibehaltung der dezentralen IT-Strukturen zukünftig verbessert werden kann. Hier kann eine Zentralisierung Synergien schaffen und so auch dem Fachkräftemangel entgegensteuern. **36**

Zudem erzeugt eine zentralisierte IT stringentere Steuerungsmöglichkeiten der Informationssicherheit. Die Koalitionsvereinbarung von CDU und GRÜNEN 2022-2027 sieht vor, die öffentlichen Rechenzentren des Landes zu einem starken, resilienten Rechenzentrumsverbund zusammenzuführen.[51] Würde zudem die Fachaufsicht über die zusammengeführten Rechenzentren der/dem CIO zugewiesen, erhielte diese/dieser einfacher Kenntnis über den Stand der Informationssicherheit. Vorgaben und Priorisierungen könnte sie/er unmittelbar anordnen. **37**

gez.
Prof. Dr. Mandt
Präsidentin

gez.
Kisseler
Vizepräsident

gez.
Dr. Hähnlein
Direktor beim LRH

gez.
Dr. Lascho
Direktor beim LRH

gez.
Zelljahn
Direktor beim LRH

gez.
Dr. Rohde
Leitender Ministerialrat

gez.
Krüger
Leitende Ministerialrätin

---

49 Vgl. Bericht der Süddeutschen Zeitung „Wenn Hacker alles lahmlegen“, Ausgabe Donnerstag/Freitag, 05./06.01.2023, Nr. 4.

50 Vgl. z. B. Presseinformation des Branchenverbands bitkom vom 16.11.2022, abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Deutschland-fehlen-137000-IT-Fachkraefte.

51 Abrufbar unter: https://www.cdu-nrw.de/sites/www.neu.cdu-nrw.de/files/zukunftsvertrag_cdu-grune.pdf, vgl. Rn. 3744.