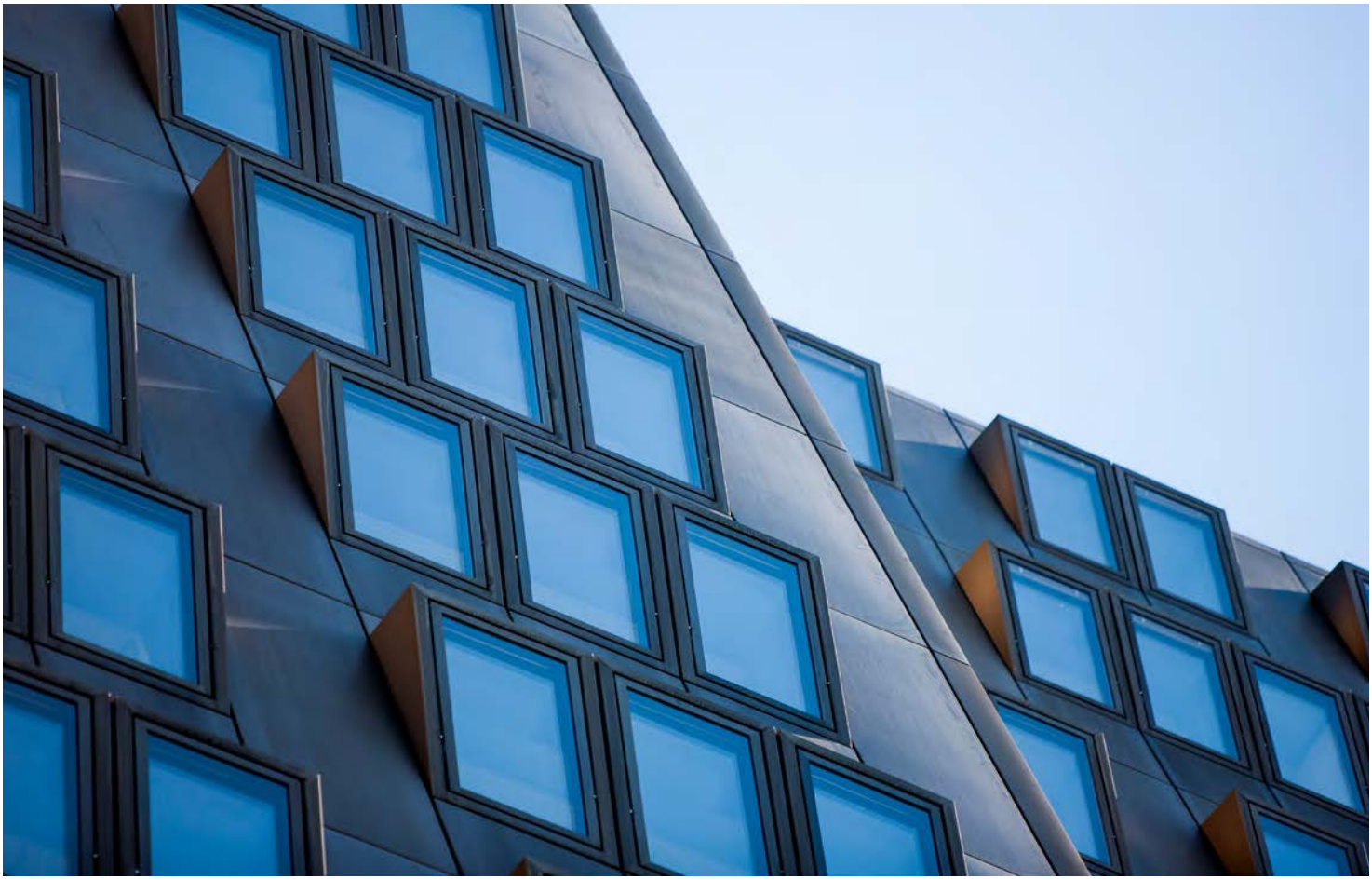
Rechnungshof Österreich

Unabhängig und objektiv für Sie.

Management der IT–Sicherheit im Land Kärnten

Reihe KÄRNTEN 2024/2

Bericht des Rechnungshofes



Rechnungshof GZ 2024–0.691.310 (005.142)

Vorbemerkungen

Vorlage

Der Rechnungshof erstattet dem Kärntner Landtag gemäß Art. 127 Abs. 6 Bundes–Verfassungsgesetz nachstehenden Bericht über Wahrnehmungen, die er bei einer Gebarungsüberprüfung getroffen hat.

Berichtsaufbau

In der Regel werden bei der Berichterstattung punkteweise zusammenfassend die Sachverhaltsdarstellung (Kennzeichnung mit 1 an der zweiten Stelle der Textzahl), deren Beurteilung durch den Rechnungshof (Kennzeichnung mit 2), die Stellungnahme der überprüften Stelle (Kennzeichnung mit 3) sowie die allfällige Gegenäußerung des Rechnungshofes (Kennzeichnung mit 4) aneinandergereiht.

Das in diesem Bericht enthaltene Zahlenwerk beinhaltet allenfalls kaufmännische Auf– und Abrundungen.

Der vorliegende Bericht des Rechnungshofes ist nach der Vorlage über die Website des Rechnungshofes www.rechnungshof.gv.at verfügbar.

IMPRESSUM

Herausgeber:
Rechnungshof Österreich
1030 Wien, Dampfschiffstraße 2
www.rechnungshof.gv.at
Redaktion und Grafik: Rechnungshof Österreich
Herausgegeben: Wien, im Oktober 2024

AUSKÜNFTE

Rechnungshof
Telefon (+43 1) 711 71 – 8946
E–Mail info@rechnungshof.gv.at
facebook/RechnungshofAT
Twitter: @RHSprecher

FOTOS

Cover, S. 7: Rechnungshof/Achim Bieniek

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

ABl.	Amtsblatt
Abs.	Absatz
AG	Arbeitsgruppe
Art.	Artikel
BGBl.	Bundesgesetzblatt
BLSG	Gremium Bund–Länder–Städte–Gemeinden
bzw.	beziehungsweise
ca.	circa
CERT	Computer Emergency Response Team (Computer–Notfallteam)
DDoS	Distributed Denial of Service (Blockierung eines Dienstes durch eine Vielzahl von Anfragen aus einer Vielzahl von Rechnern)
d.h.	das heißt
DSGVO	Datenschutz–Grundverordnung
ELAK	elektronischer Akt, elektronisches Aktenverwaltungssystem
etc.	et cetera
EU	Europäische Union
EUR	Euro
(f)f.	folgend(e)
GB	Gigabyte
i.d.(g.)F.	in der (geltenden) Fassung
IEC	International Electrotechnical Commission (Internationale Elektrotechnische Kommission – Normungsorganisation)
IKDOK	Innerer Kreis der Operativen Koordinierungsstruktur
IKT	Informations– und Kommunikationstechnologie
ISO	International Organization for Standardization (Internationale Organisation für Normung)
IT	Informationstechnologie
LGBl.	Landesgesetzblatt
lit.	litera (Buchstabe)
LVT	Landesamt für Verfassungsschutz und Terrorismusbekämpfung

Mio.	Million
NIS	Netz– und Informationssystemsicherheit
NISG	Netz– und Informationssystemsicherheitsgesetz
OpKoord	Operative Koordinierungsstruktur
rd.	rund
RH	Rechnungshof
S.	Seite
SIEM	Security Information and Event Management
SOC	Security Operations Center
TZ	Textzahl
u.a.	unter anderem
USB	Universal Serial Board
vgl.	vergleiche
VPN	Virtual Private Network (virtuelles privates Netzwerk)
Z	Ziffer
z.B.	zum Beispiel

Ein hohes Maß an IT–Sicherheit ist ein zentrales Ziel für die öffentliche Verwaltung, da die Sicherheit der IT–Systeme für die öffentliche Leistungserbringung wesentlich ist.

Das Land Kärnten war im Jahr 2022 einem Cyber–Angriff mit Datendiebstahl und Erpressung ausgesetzt. Das Land hatte bereits vor diesem Cyber–Angriff technische Maßnahmen im Bereich der IT–Sicherheit umgesetzt, das IT–Sicherheitsmanagement insgesamt war jedoch lückenhaft: So war etwa ein Cyber–Angriff – auch nach jenem im Jahr 2022 – in den Risikoanalysen nicht als potenzielles Risiko definiert, eine Zwei–Faktor–Authentifizierung war nur in wenigen Bereichen implementiert und es waren keine spezifischen Systeme zur strukturierten Angriffserkennung, Auswertung sowie Behandlung (SIEM/SOC) eingerichtet.

Die gesetzten Maßnahmen konnten den Cyber–Angriff weder erkennen noch verhindern. Die flächendeckende Nicht–Verfügbarkeit der IT–Infrastruktur hatte erhebliche Auswirkungen auf die Landesverwaltung, so kamen die Angreifer auch in den Besitz personenbezogener Daten.

Das Land Kärnten beauftragte externe private Dienstleister, um gemeinsam mit diesen die IT–Systeme wiederherzustellen. Die fachliche Expertise nationaler Cyber–Sicherheitsgremien (z.B. IKDOK, OpKoord, CERT–Verbund) bezog es nur in einem sehr geringen Ausmaß ein.

Nach dem Cyber–Angriff setzte das Land Kärnten weitere IT–Sicherheitsmaßnahmen für die zentrale Infrastruktur und für IT–Arbeitsplätze um. Damit konnten potenzielle Risiken zukünftiger Cyber–Angriffe deutlich reduziert werden. Mit Ende 2023 fehlten jedoch insbesondere noch die Zwei–Faktor–Authentifizierung für alle IT–Arbeitsplätze, vollständige Dokumentationen der umgesetzten IT–Sicherheitsmaßnahmen, ein umfassendes IT–Notfallhandbuch, verstärkte IT–Sicherheitsüberprüfungen sowie auf organisatorischer Ebene ein Informationssicherheitsmanagement–Team. Die Umsetzung dieser geplanten Maßnahmen wäre auch im Hinblick auf die NIS–2–Richtlinie der EU über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau zweckmäßig. Die Richtlinie ist bis Oktober 2024 umzusetzen; sie erfordert auch in den öffentlichen Einrichtungen der Länder eine Erhöhung der IT–Sicherheitsmaßnahmen, insbesondere im Risiko– und Notfallmanagement.

WIRKUNGSBEREICH

- Land Kärnten

Management der IT–Sicherheit im Land Kärnten

Prüfungsziel

Der RH überprüfte von August bis Dezember 2023 die Konzeption und Umsetzung ausgewählter Aspekte des Managements der IT–Sicherheit im Land Kärnten. Prüfungsziele waren die Darstellung und Beurteilung insbesondere der IT–Sicherheitsstrategie, der IT–Sicherheitsorganisation, der IT–Sicherheit bei Personal und Telearbeit, der technischen Maßnahmen zur Erhöhung der IT–Sicherheit sowie der Ereignisse und Maßnahmen bezüglich des Cyber–Angriffs im Jahr 2022. Der überprüfte Zeitraum umfasste im Wesentlichen die Jahre 2020 bis 2023.

Kurzfassung

Grundlagen der IT–Sicherheit

Das Netz– und Informationssystemsicherheitsgesetz (**NISG**) verpflichtete auf Bundesebene zu Maßnahmen für ein hohes Sicherheitsniveau von Netz– und Informationssystemen. Um ein vergleichbares Schutzniveau auch auf Landesebene herbeizuführen, konnten die Länder entsprechende Landesgesetze erlassen. Das Land Kärnten hatte – so wie die anderen Länder – von dieser Möglichkeit nicht Gebrauch gemacht. Mit dem NISG setzte Österreich die europäische NIS–Richtlinie aus 2016 um. Die weiterentwickelte NIS–2–Richtlinie ist bis Oktober 2024 in nationales Recht umzusetzen und erfordert eine Erhöhung der IT–Sicherheitsmaßnahmen in öffentlichen Einrichtungen auf Bundes– und Landesebene, insbesondere im Bereich Risiko– und Notfallmanagement. (TZ 4)

Die IT–Sicherheitsstrategie des Landes Kärnten stammte aus 2018 und war nicht aktuell. Dies betraf insbesondere die Abstimmung mit der IT–Strategie 2023 des Landes und die Verantwortung der oberen Leitungsebene. (TZ 5)

Zur Verarbeitung von Informationen, die einer Geheimhaltung bedürfen (sogenannte klassifizierte Informationen), verwies das Land Kärnten auf den verfassungsrechtlichen Grundsatz der Amtsverschwiegenheit. Neben einzelnen Regelungen wie der Kanzleiordnung gab es keine organisationsweiten, umfassenden und einheitlichen Vorgaben zum Umgang mit klassifizierten Informationen. (TZ 3)

Das Land Kärnten hatte ein IT–Risikomanagementsystem eingerichtet. Allerdings waren auch nach dem Cyber–Angriff im Jahr 2022 Bedrohungen aus Cyber–Angriffen nicht in der Risikoanalyse bei den allgemeinen IT–Risiken angeführt. Die Risikoanalysen für die einzelnen IT–Systeme aktualisierte die IT–Abteilung des Landes gemeinsam mit den Fachabteilungen alle fünf Jahre. Die obere Leitungsebene (die Landesamtsdirektion und das zuständige Mitglied der Landesregierung) erhielt keine standardisierten und regelmäßigen Berichte mit IT–Sicherheitskennzahlen. (TZ 6)

IT–Sicherheitsorganisation

Im Land Kärnten lag die Verantwortung für die IT–Sicherheit auf Ebene der Landesregierung beim Landeshauptmann. Die unmittelbare Leitung der IT und der IT–Sicherheit des Landes war der IT–Abteilung, einer Unterabteilung der Abteilung 1 – Landesamtsdirektion, zugeordnet. Die Leitung der IT–Abteilung war von 1. April 2022 bis 31. Mai 2022 – und damit auch zu Beginn des Cyber–Angriffs – nicht besetzt. (TZ 7)

Ein für die Informations– und IT–Sicherheit gesamtverantwortlicher Chief Information Security Officer (CISO) wurde mit Jänner 2024 eingerichtet. Das Land Kärnten verfügte über kein Informationssicherheitsmanagement–Team, das die IT–Sicherheit koordinieren sowie Pläne, Vorgaben und Richtlinien entwickeln sollte. (TZ 8, TZ 9)

IT–Sicherheit bei Personal und Telearbeit

Das Land Kärnten beauftragte zur Entwicklung, zum Betrieb und zur Wartung von IT–Systemen externe Dienstleister. Der IT–Abteilung war nicht in jedem Fall das Informationssicherheitsniveau der externen Dienstleister bekannt. Eine Regelung zur Risikominimierung bei (Fern–)Zugriffen durch externe Dienstleister auf die IT–Systeme des Landes gab es nicht. (TZ 11)

Die Datenschutzinformation an neu eintretende Bedienstete enthielt veraltete Informationen zu den Kontaktdaten des bzw. der Datenschutzbeauftragten. (TZ 11)

Eine dienstliche, mobile IT–Ausstattung für Bedienstete, die Telearbeit verrichteten, war nicht standardmäßig vorgesehen. Bedienstete ohne dienstliche mobile IT–Ausstattung konnten für die Telearbeit eine private IT–Ausstattung nutzen. Diese wurde zwar als Thin–Client betrieben, d.h., sie war über eine Benutzerschnittstelle mit der IT–Infrastruktur des Landes verbunden. Die Anwendungen liefen aber nicht lokal am Endgerät, sondern am zentralen Applikationsserver. Bei der Verwendung einer privaten IT–Ausstattung für dienstliche Zwecke gab es IT–Sicherheitsrisiken, etwa eine geringere Sicherheit gegenüber Schadsoftware. Das Land Kärnten hatte Regelungen zur Gewährleistung der IT–Sicherheit bei Telearbeit erlassen, die es den Bediensteten zur Kenntnis brachte. Diese enthielten aber keine Vorgaben zur Nutzung einer privaten IT–Ausstattung als Thin–Client. (TZ 12, TZ 13)

Technische Maßnahmen zur Erhöhung der IT–Sicherheit

Ziel von technischen und organisatorischen Maßnahmen im Bereich IT–Sicherheit ist es, die Sicherheit der zentralen IT–Komponenten und der IT–Anwendungen zu erhöhen. Das Land Kärnten hatte bereits vor dem Cyber–Angriff 2022 technische Maßnahmen umgesetzt: eine Firewall, Spamfilter oder Intrusion–Detection– und Intrusion–Prevention–Systeme. Nach dem Cyber–Angriff setzte es weitere Maßnahmen. Eine flächendeckende Zwei–Faktor–Authentifizierung und eine USB–Port–Deaktivierung bzw. –Kontrolle waren jedoch noch nicht eingerichtet. (TZ 14, TZ 15)

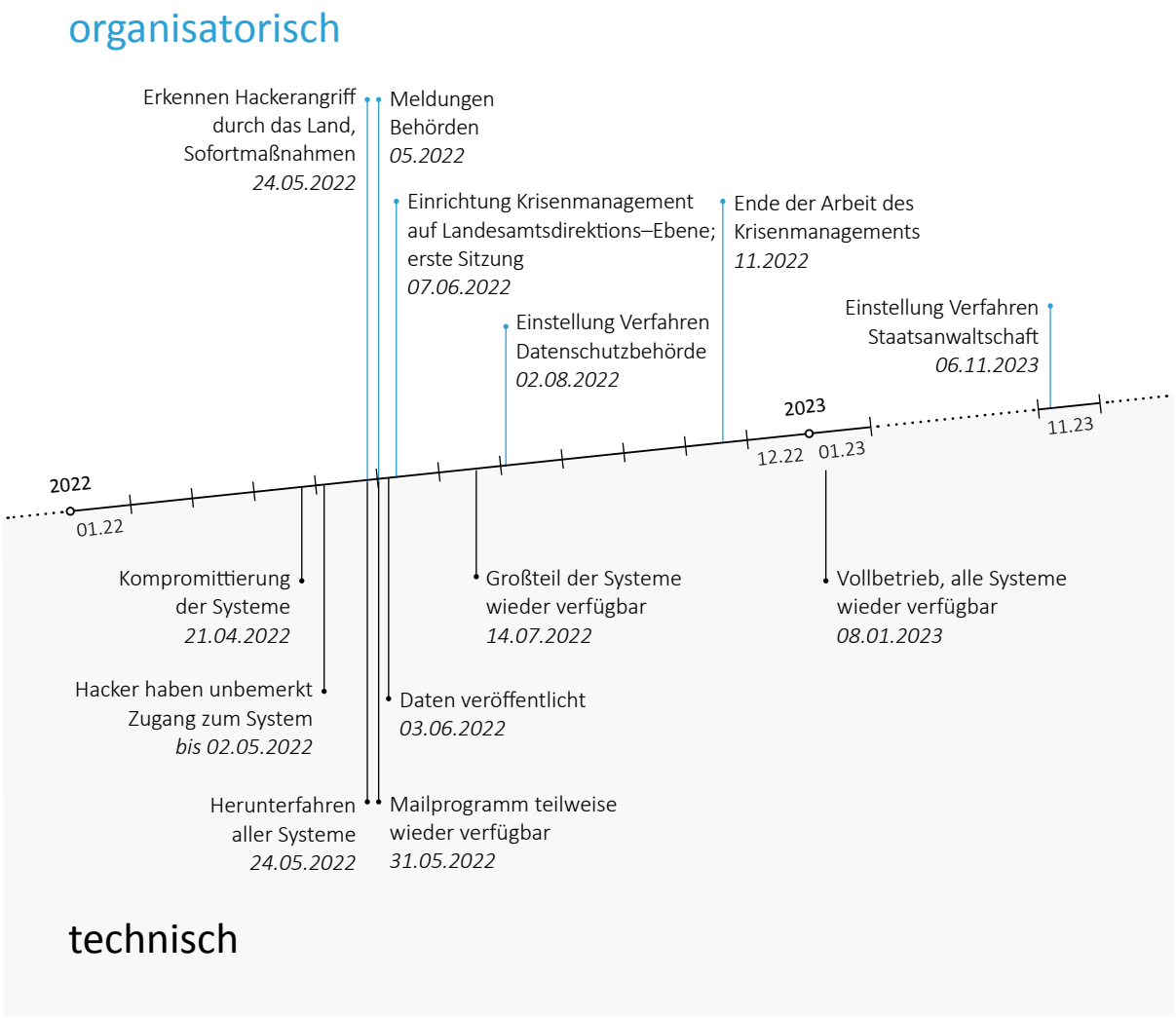
Im Zeitraum 2020 bis 2023 führte das Land Kärnten fünf externe sowie acht interne IT–Sicherheitsüberprüfungen durch. Diese Überprüfungen deckten jedoch nicht alle wesentlichen Bereiche ab und erfassten nicht alle Risiken. (TZ 16)

Das Land Kärnten verfügte auch nach dem schwerwiegenden Cyber–Angriff 2022 über kein umfassendes IT–Notfallhandbuch. Zudem waren maßgebende Dokumente, wie der Sicherheits– und Notfallplan für das Hauptrechenzentrum (aus 2019) und das Sicherungs– und Wiederherstellungskonzept (aus 2014), sowie die IT–Notfallnummern und Zutrittsregelungen nicht aktuell. (TZ 17)

Cyber–Angriff im Jahr 2022

Das Land Kärnten war im Jahr 2022 einem Cyber–Angriff mit Datendiebstahl und Erpressung ausgesetzt. Der Cyber–Angriff beeinflusste die Tätigkeit der Landesverwaltung im Zeitraum April 2022 bis Jänner 2023. (TZ 18, TZ 19)

Abbildung: Organisatorische und technische Ereignisse im Rahmen des Cyber–Angriffs



Quelle: Land Kärnten; Darstellung: RH

Durch den Datenabfluss infolge des missbräuchlichen Zugriffs auf Datenspeicher im IT–Netzwerk kamen die Angreifer auch in den Besitz personenbezogener Daten. Für den Umgang mit Daten sowie deren Ablage und Speicherung verwies das Land Kärnten auf den Erlass zur Datenschutz–Grundverordnung, auf eine Anleitung im

Intranet zum Schutz sensibler Daten sowie auf das Amtsgeheimnis. Allgemein gültige Vorgaben zur Datenklassifizierung (z.B. eine Datenklassifizierungs–Policy) waren nicht in Kraft. (TZ 20)

Die Bewältigung des Cyber–Angriffs übernahm in der ersten Phase die IT–Abteilung in Abstimmung mit der Landesamtsdirektion im Rahmen der Linienorganisation. Nach der Veröffentlichung von Daten des Landes auf einer File–Sharing–Plattform richtete das Land einen IT–Krisenstab im IT–Bereich und eine Cyber–Einsatz–Gruppe auf Ebene der Landesamtsdirektion ein. (TZ 22)

Das Land Kärnten verfügte zur Bewältigung von Krisen über einen im Jahr 2017 erstellten „Leitfaden Krisenmanagement". Eine Aktualisierung durch den Landesamtsdirektor, u.a. mit den Erkenntnissen aus dem Cyber–Angriff, unterblieb. (TZ 22)

Nach Bekanntwerden des Cyber–Angriffs am 24. Mai 2022 setzte das Land Kärnten umgehend technische Sofortmaßnahmen: Es richtete ein Rapid Response Team ein, baute eine neue Firewall auf und errichtete einen DDoS–Schutz. Zur Zeit der Gebarungsüberprüfung waren auch weitere technische Maßnahmen abgeschlossen, etwa die Absicherung des Netzwerks oder die Sicherung der notwendigen IT–Dienste. Es waren jedoch noch nicht alle geplanten technischen und organisatorischen Maßnahmen zur Erhöhung der IT–Sicherheit umgesetzt. (TZ 23)

Für Sofort– und Wiederherstellungsmaßnahmen nach dem Cyber–Angriff stellte das Land 5,75 Mio. EUR zur Verfügung. Ein Teil davon – 15.000 EUR – betraf die Beschaffung eines Security Management Systems; dieses wurde jedoch nicht operativ eingesetzt. Für einen Beratervertrag wendete das Land 33.000 EUR auf; die Zahlungen daraus erfolgten teilweise vor Leistungserbringung. (TZ 24)

Das Land Kärnten leistete keine Lösegeldzahlungen im Zusammenhang mit dem Cyber–Angriff. (TZ 24)

Zusammenarbeit mit anderen Akteuren

Die Zusammenarbeit mit Bundesbehörden und Cyber–Gremien ist wesentlich, um die Auswirkungen von Cyber–Angriffen zu verhindern oder möglichst gering zu halten. Das Land Kärnten gab an, regelmäßig an den Sitzungen des Gremiums Bund–Länder–Städte–Gemeinden (**BLSG**) und der Länderarbeitsgruppe teilgenommen zu haben. Es konnte jedoch nicht in allen Fällen die Teilnahme dokumentieren. Zur Zeit der Gebarungsüberprüfung war das Land in keiner BLSG–Arbeitsgruppe vertreten. (TZ 25)

Bis Dezember 2023 waren auch keine Bediensteten des Landes Mitglied in der Cyber Sicherheit Plattform – diese diente der Vernetzung und dem Informationsaustausch zu Cyber–Sicherheit. An den vom Innenministerium abgehaltenen Videokonferenzen zur Information der Länder über Themen der Cyber–Sicherheit nahm das Land Kärnten von April bis November 2023 in fünf von acht Fällen teil. (TZ 26)

Seit September 2022 war das Land Kärnten darüber hinaus Mitglied der Vernetzungsplattform Austrian Trust Circle, die durch das nationale Computer–Notfallteam (CERT.at) betrieben wurde. Es nahm seither an drei von sechs Treffen teil. Schließlich war das Land Kärnten auch in die Informationsdrehscheibe des Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) eingebunden. (TZ 27)

Bei Cyber–Angriffen in Landesverwaltungen waren Meldungen an verschiedene Bundesbehörden vorgesehen. Weiters waren auf Bundesebene Gremien eingerichtet, die Unterstützung für die Bewältigung von Cyber–Angriffen leisten können. Für eine effiziente staatliche Cyber–Sicherheitsvorsorge wären noch weitere Umsetzungsschritte erforderlich, z.B. die Fertigstellung eines NIS–Meldesystems, die Weiterentwicklung des Cybercrime Competence Centers oder die Einrichtung eines ständig verfügbaren Cyber–Einsatzteams. (TZ 28)

Auf Basis seiner Feststellungen hob der RH folgende Empfehlungen an das Land Kärnten hervor:

ZENTRALE EMPFEHLUNGEN

- Das Land Kärnten sollte sich auf die Anforderungen durch die Umsetzung der NIS–2–Richtlinie vorbereiten und den nationalen Umsetzungsprozess begleiten, um die wesentlichen Themen – wie Risikomanagement, Notfallvorsorge, Krisenmanagement, Verantwortung der Leitungsebene, Informationsklassifizierung – zeitgerecht zu berücksichtigen. Dabei wäre eine Zusammenarbeit mit den in gleicher Weise betroffenen anderen Bundesländern anzustreben. (TZ 4)

- Die IT–Sicherheitsstrategie des Landes Kärnten wäre unter Berücksichtigung der IT–Strategie des Landes aus 2023 zu aktualisieren und ihre Aktualität zukünftig regelmäßig zu überprüfen. Insbesondere wären in der IT–Sicherheitsstrategie

  – die Verantwortung der oberen Leitungsebene für die IT–Sicherheit ausdrücklich festzulegen,
  – die Grundzüge des Risikomanagementprozesses zu dokumentieren,
  – die Hinweise für alle Bediensteten zum Vorgehen bei Cyber–Angriffen zu konkretisieren und
  – Regelungen zur Zusammenarbeit mit bestehenden Gremien zur Cyber–Sicherheit aufzunehmen.

  Dies wäre auch im Hinblick auf die Umsetzung der NIS–2–Richtlinie zweckmäßig. (TZ 5)

- Gemäß den Vorgaben des Österreichischen Informationssicherheitshandbuchs wäre ein Informationssicherheitsmanagement–Team einzurichten; dabei wäre auf eine zweckentsprechende Einbindung der Anwenderinnen und Anwender sowie der nachgeordneten Dienststellen zu achten. (TZ 9)

- Ein umfassendes IT–Notfallhandbuch (inklusive überarbeiteter Anforderungen an das Notfallrechenzentrum) wäre zu erstellen; dieses sollte alle jene Prozesse abbilden, die den Betrieb auch in Ausnahmesituationen aufrecht halten können. Dabei sollten insbesondere die Notfallvorsorge und –bewältigung sowie Tests und Übungen berücksichtigt werden. (TZ 17)

Zahlen und Fakten zur Prüfung

Management der IT–Sicherheit im Land Kärnten				
Rechtsgrundlagen	• Datenschutz–Grundverordnung (DSGVO), Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, ABl. L 2016/119, 1 • NIS–Richtlinie, Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz– und Informationssystemen in der Union, ABl. L 2016/194, 1 • NIS–2–Richtlinie, Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, ABl. L 2022/333, 80 • Netz– und Informationssystemsicherheitsgesetz (NISG), BGBl. I 111/2018 • Landesverfassungsgesetz vom 11. Juli 1996, mit dem die Verfassung für das Land Kärnten erlassen wird, LGBl. 85/1996 i.d.g.F.			
Standards	Österreichisches Informationssicherheitshandbuch, www.sicherheitshandbuch.gv.at ISO/IEC–Norm 27001 (Informationssicherheitsmanagement)			
	Bedienstete der IT–Abteilung			
	2020	2021	2022	2023
	in Vollzeitäquivalenten zum 31. Dezember			
intern	41,28	41,80	41,38	43,10
extern[1]	1	1	1	1
	in Köpfen zum 31. Dezember			
intern	43	44	43	45
extern[1]	1	1	1	1
	durchgeführte IT–Sicherheitsüberprüfungen			
	2020	2021	2022	2023
	Anzahl			
intern	2	2	2	2
extern	1	1	1	2
	Auszahlungen für IT bzw. IT–Sicherheit			
	Veranschlagung		Auszahlung (davon IT–Sicherheit)	
Jahr	in Mio. EUR			
2020	7,22		7,59 (0,27)	
2021	6,70		8,46 (0,20)	
2022	6,81		10,59 (1,97)	

[1] Fremdmitarbeiterinnen und –mitarbeiter im Rahmen eines Outsourcing–Vertrags

Quelle: Land Kärnten

Prüfungsablauf und –gegenstand

1 (1) Der RH überprüfte von August bis Dezember 2023 ausgewählte Aspekte des Managements der IT–Sicherheit im Land Kärnten. Der überprüfte Zeitraum umfasste insbesondere die Jahre 2020 bis 2023. Soweit erforderlich nahm der RH auch auf Sachverhalte außerhalb dieses Zeitraums Bezug.

Die Gebarungsüberprüfung orientierte sich an Aspekten, die der RH etwa bereits im Zuge der Prüfungen „Dienstrechtliche und technische Umsetzung von Telearbeit in ausgewählten Bundesministerien“ (Reihe Bund 2022/27) und „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31) überprüft hatte.

(2) Ziel der Gebarungsüberprüfung war es, die Konzeption und Umsetzung ausgewählter Aspekte des Managements der IT–Sicherheit des Landes Kärnten darzustellen und zu beurteilen. Dies betraf insbesondere

- die IT–Sicherheitsstrategie,
- die IT–Sicherheitsorganisation,
- IT–Sicherheit für Personal und Telearbeit,
- technische und organisatorische Maßnahmen zur Erhöhung der IT–Sicherheit sowie
- die Ereignisse und Maßnahmen bezüglich des Cyber–Angriffs im Jahr 2022.

Darüber hinaus überprüfte der RH die Zusammenarbeit des Landes mit anderen Akteuren, insbesondere mit Einrichtungen des Bundes.

Das Management der IT–Sicherheit bei den externen IT–Dienstleistern und bei den nachgeordneten Dienststellen des Landes war nicht Gegenstand der Gebarungsüberprüfung.

(3) Das vom Bundeskanzleramt herausgegebene, laufend aktualisierte Österreichische Informationssicherheitshandbuch[1] legte Standards für die IT–Sicherheit in der öffentlichen Verwaltung fest. Es enthielt u.a. Vorgaben zu

- strategischen Ansätzen,
- Risikoanalysen,
- Organisation,
- Telearbeit,
- Verhalten von Mitarbeiterinnen und Mitarbeitern,
- Klassifikation von Informationen und
- Sicherheit von Datenträgern.

[1] ein Projekt des Bundeskanzleramts in Zusammenarbeit mit dem Zentrum für sichere Informationstechnologie – Austria (A–SIT); https://www.sicherheitshandbuch.gv.at (abgerufen am 19. August 2024)

Das Informationssicherheitshandbuch setzte primär Standards für technische und organisatorische Sicherheitsmaßnahmen innerhalb eines spezifischen Rechtsträgers. Es orientierte sich an anerkannten Standards der internationalen Organisation für Normung, wie der ISO/IEC–Norm 27001 (Informationssicherheitsmanagement), und erleichterte so die Umsetzung von Vorgaben aus der ISO–Normenreihe. Weiters waren neue Entwicklungen der umfangreichen und detaillierten Grundschutz–Standards des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI–Grundschutz) berücksichtigt (TZ 2, Abbildung 1: Elemente 7 und 9).

Der RH zog daher insbesondere ausgewählte Aspekte des Österreichischen Informationssicherheitshandbuchs als Maßstab für die Beurteilung der im Land Kärnten eingesetzten Maßnahmen im Management der IT–Sicherheit heran. Darüber hinaus orientierte er sich an der ISO/IEC–Norm 27001 sowie an dem vom deutschen Bundesamt für Sicherheit in der Informationstechnik entwickelten IT–Grundschutzkatalog.

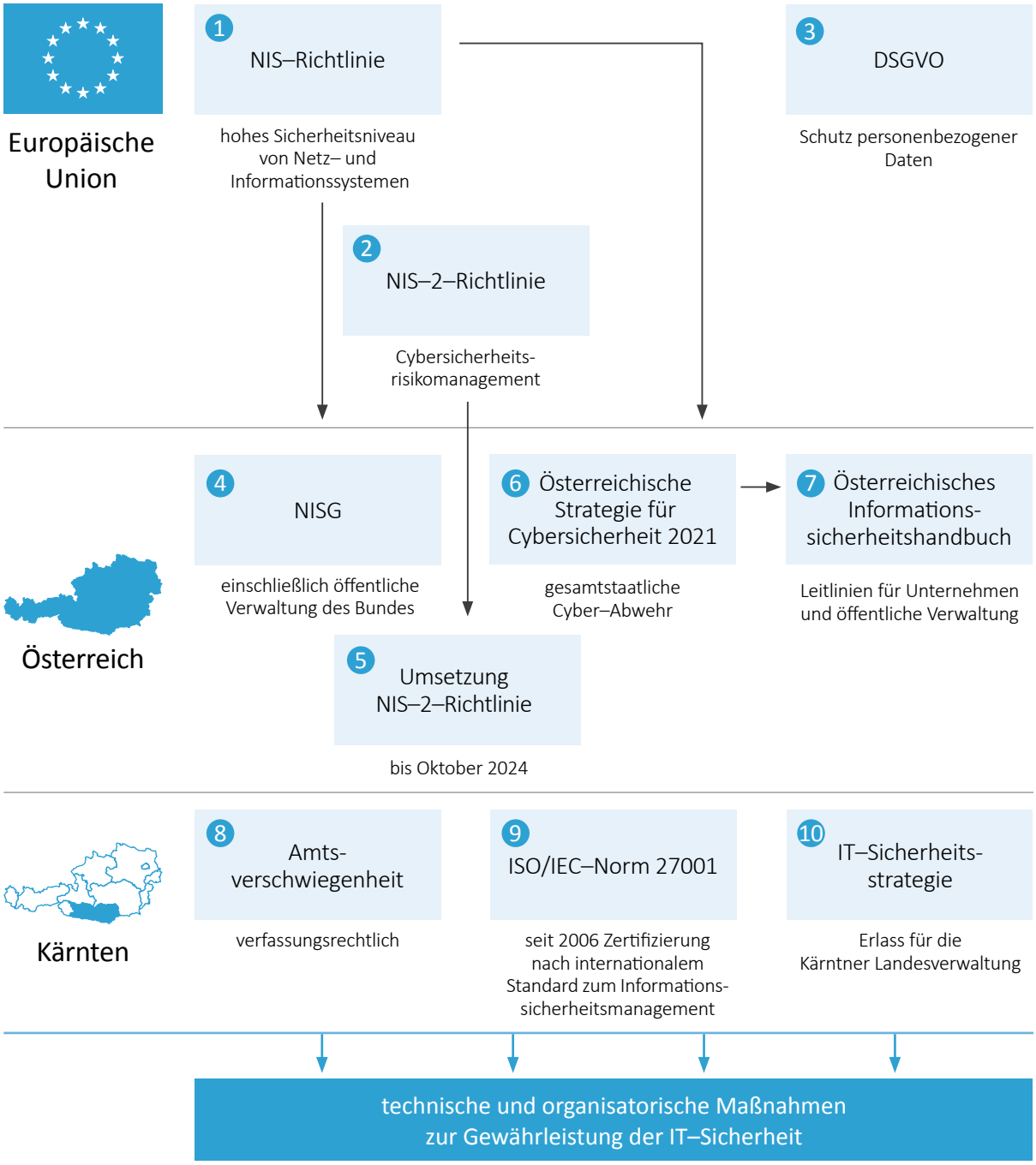
(4) Zu dem Ende April 2024 übermittelten Prüfungsergebnis nahm das Land Kärnten im Juli 2024 Stellung. Der RH erstattete seine Gegenäußerung im Oktober 2024.

Grundlagen der IT–Sicherheit

Überblick über die Vorgaben für die IT–Sicherheit

2 (1) Ein hohes Maß an IT–Sicherheit sicherzustellen, ist eine zentrale Aufgabe der öffentlichen Verwaltung, um die öffentliche Leistungserbringung aufrechterhalten zu können. Zur Gewährleistung der IT–Sicherheit können unterschiedliche organisatorische und technische Maßnahmen getroffen werden. Sowohl das Land Kärnten als auch der Bund und die EU setzten aufeinander aufbauende und einander ergänzende Initiativen, um die notwendigen Maßnahmen festzulegen. Die folgende Abbildung stellt diese Rechtsgrundlagen, Strategien und Leitlinien im Überblick dar:

Abbildung 1: Vorgaben für die IT–Sicherheit



DSGVO: Datenschutzgrundverordnung (EU) 2016/679, ABl. L 2016/119, 1
NIS–Richtlinie: Richtlinie (EU) 2016/1148, ABl. L 2016/194, 1
NIS–2–Richtlinie: Richtlinie (EU) 2022/2555, ABl. L 2022/333, 80
NISG: Netz– und Informationssystemsicherheitsgesetz, BGBl. I 111/2018 i.d.g.F.

Quelle: Land Kärnten; Darstellung: RH

Der RH beschreibt in den nachfolgenden TZ insbesondere die vom Land Kärnten gesetzten und die unmittelbar geltenden europäischen Vorgaben (TZ 3, TZ 5) sowie die auch die regionale Ebene (Länderebene) erfassende Weiterentwicklung der NIS–Richtlinie (TZ 4).

(2) Gemäß der Referatseinteilung der Kärntner Landesregierung (LGBl. 31/2023 bzw. 30/2018) fiel die Informations– und Kommunikationstechnologie einschließlich der IT–Sicherheit in den Zuständigkeitsbereich des Landeshauptmanns; gemäß der Geschäftseinteilung für das Amt der Kärntner Landesregierung (LGBl. 32/2023, 56/2019 bzw. 39/2018) in jenen der Landesamtsdirektion.

Rechtliche und technische Vorgaben

3.1 Für die IT–Sicherheit des Landes Kärnten waren verschiedene rechtliche und technische Vorgaben von Bedeutung.

(1) Die Datenschutz–Grundverordnung der EU (**DSGVO**[2]) war für das Land Kärnten unmittelbar anwendbar. Das Land sowie seine Auftragsverarbeiter hatten zum Schutz personenbezogener Daten geeignete technische und organisatorische Maßnahmen zu treffen (TZ 2, Abbildung 1: Element 3).

Die IT–Sicherheit umfasste darüber hinaus auch die Verfügbarkeit, Integrität und Vertraulichkeit nicht personenbezogener Daten.

(2) Die Amtsverschwiegenheit nach Art. 58 Kärntner Landesverfassung[3] verpflichtete alle Landesbediensteten zur Verschwiegenheit über amtlich bekannt gewordene Tatsachen im Interesse bestimmter Schutzgüter (z.B. öffentliche Sicherheit, Vorbereitung von Entscheidungen). Sie war Grundlage für den Schutz von Informationen, die aus öffentlichen Interessen eine Geheimhaltung erfordern[4] (TZ 2, Abbildung 1: Element 8).

Die Kanzleiordnung 2022, ein Erlass der Landesamtsdirektion, überließ den Dienststellenleiterinnen und –leitern weitere Anordnungen über die Einstufung vertraulicher Dokumente sowie Verschlussdokumente. Die IT–Abteilung legte für ihren Bereich besondere organisatorische Maßnahmen für Dokumente bzw. Informationen über Ausschreibungen und Personalangelegenheiten fest (Zugänglichkeit nur für einen eingeschränkten Personenkreis). Für die IT–Anwendungen waren ent-

[2] Verordnung (EU) 2016/679, ABl. L 2016/119, 1

[3] LGBl. 85/1996 i.d.g.F.

[4] gleichlautend in § 46 Kärntner Dienstrechtsgesetz 1994 (LGBl. 71/1994 i.d.g.F.) bzw. § 16 Kärntner Landesvertragsbedienstetengesetz 1994 (LGBl. 73/1994 i.d.g.F.)

sprechend einer Risikoabwägung jeweils unterschiedliche technische Maßnahmen zur Informationssicherheit eingerichtet (TZ 14, TZ 15).

Das Österreichische Informationssicherheitshandbuch empfahl, die Klassifizierung von Informationen in einer für alle Bediensteten erlassenen Rechtsgrundlage zu regeln (TZ 2, Abbildung 1: Element 7).[5] Auch die ISO/IEC–Norm 27001 setzte ein Informationsklassifizierungsschema voraus. Im Land Kärnten lag eine solche übergeordnete, organisationsweite, von zentraler Stelle verantwortete Richtlinie nicht vor. Einheitliche Vorgaben

- zur Einteilung von Informationen in Klassifikationsstufen (z.B. nach dem Vertraulichkeitsgrad),
- zu – diesen Klassifikationsstufen entsprechenden – technischen und organisatorischen Maßnahmen und
- zur Kennzeichnung sämtlicher Informationen

fehlten daher. Das im Jänner 2024 beschlossene, die gesamte Verwaltung umfassende, Informationsfreiheitsgesetz[6] sah zwar den Entfall der Amtsverschwiegenheit vor, enthielt jedoch Regelungen zur Geheimhaltung von amtlichen Informationen.

(3) Das Land Kärnten verfügte seit 2006 über eine – jeweils drei Jahre gültige – Zertifizierung nach der ISO/IEC–Norm 27001 (TZ 2, Abbildung 1: Element 9). Dieser international anerkannte Standard enthielt Vorgaben für ein dokumentiertes Informationssicherheits–Managementsystem. Ziel war es, Sicherheitsrisiken zu erkennen und zu reduzieren. Der Standard berücksichtigte die drei IT–Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit von Informationen. Somit konnte die Einhaltung des Standards zur Gewährleistung der IT–Sicherheit beitragen.

Bei den alle drei Jahre stattfindenden Re–Zertifizierungsaudits zur Überprüfung der Wirksamkeit des Informationssicherheits–Managementsystems war die Ist–Situation zu analysieren und erforderlichenfalls an die Soll–Situation nach dem Standard anzupassen. Die Zertifizierung umfasste im Land Kärnten die Bereiche Konzeption, Einkauf, Errichtung, Betriebsführung und Wartung der IT–Infrastruktur sowie Management, Beratung und Realisierung von IT–Projekten (TZ 16).

[5] Auf Bundesebene existierten dazu das Informationssicherheitsgesetz (BGBl. I 23/2002 i.d.g.F.) und die zugehörige Informationssicherheitsverordnung (BGBl. II 548/2003 i.d.g.F.). Diese befanden sich zur Zeit der Gebarungsüberprüfung in Überarbeitung.

[6] BGBl. I 5/2024

3.2 Der RH anerkannte, dass das Land Kärnten seit 2006 die (Re–)Zertifizierungen nach der ISO/IEC–Norm 27001 für wesentliche Teile seiner IT durchführen ließ.

Er hielt fest, dass das Land Kärnten zur Verarbeitung von Informationen, die einer Geheimhaltung bedürfen (klassifizierte Informationen), auf den allgemeinen verfassungsrechtlichen Grundsatz der Amtsverschwiegenheit verwies. Er kritisierte, dass es keine organisationsweiten, umfassenden und einheitlichen Vorgaben zur Behandlung klassifizierter Informationen (inklusive vertraulicher und Verschlussdokumente) gab.

Der RH empfahl dem Land Kärnten, den Grundsatz der Amtsverschwiegenheit bzw. der erforderlichen Geheimhaltung nach dem Informationsfreiheitsgesetz durch für alle Bediensteten geltende, konkretisierende Regelungen näher auszuführen. Einheitliche Vorgaben

- zur Klassifizierung von Informationen (Einteilung z.B. nach dem Vertraulichkeitsgrad),
- zur Kennzeichnung der Klassifikationsstufe,
- zu den anzuwendenden organisatorischen und technischen Sicherheitsmaßnahmen (beispielsweise Verschlüsselung, Einschränkung der elektronischen Verarbeitung, Schulungen) und
- zur Verantwortung für die Durchführung

sollten in einem organisationsweiten, von zentraler Stelle verantworteten Grundlagendokument erlassen bzw. ergänzt werden. Dies wäre auch im Hinblick auf die Anforderungen der NIS–2–Richtlinie zweckmäßig.

3.3 Laut Stellungnahme des Landes Kärnten verkenne die Empfehlung des RH, dass mit dem Erlass der IT–Sicherheitsstrategie des Landes Kärnten (TZ 5) Sicherheitsstandards und Sicherheitsklassen festgelegt worden seien, die sich als generelle Weisung allgemein an die Bediensteten richten würden. Überdies sei zu beachten, dass im österreichischen Portalverbundsystem aufgrund einer Vereinbarung zwischen allen Beteiligten Standards für das Sicherheitsmanagement festgelegt seien (z.B. Sicherheitsklassen für Anwendungen, Auflagen für Authentifizierung, räumliche Sicherheit). Die in der IT–Sicherheitsstrategie vorgesehene Verpflichtungserklärung für Endanwender sei auch im Portalverbund verpflichtend.

Ein Bedürfnis, zusätzlich zu bestehenden gesetzlichen Geheimhaltungsverpflichtungen das jeweilige Geheimhaltungsinteresse des Landes aufgrund einer generellen Norm in verschiedenen Klassifikationsstufen zum Ausdruck zu bringen und daran Zugangsbeschränkungen zu knüpfen, werde daher nicht erkannt.

3.4 Der RH entgegnete dem Land Kärnten, nicht zu verkennen, dass im Land Kärnten bereits technische Sicherheitsvorgaben und technische Sicherheitsvorkehrungen getroffen wurden; siehe dazu die Ausführungen des RH in TZ 5, TZ 14, TZ 15, TZ 20. Die IT–Sicherheitsstrategie des Landes Kärnten regelte dazu jedoch nur Teilaspekte, und zwar die Klassifizierung von Daten in personenbezogene und nicht personenbezogene sowie die Klassifizierung von IT–Anwendungen nach ihrem Verfügbarkeitsbedarf. Nach Ansicht des RH fehlte aber eine grundlegende, die einzelnen Organisationseinheiten umspannende und die einheitliche Anwendung fördernde Regelung zur Klassifizierung von Informationen, Daten und Dokumenten. Aus dieser Regelung sollten sich die weiteren Richtlinien mit organisatorischen und technischen Maßnahmen sowie Handlungsanweisungen zum Umgang mit den Informationen, Daten und Dokumenten ableiten. Der Erlass einer solchen Regelung in einer Organisation entspräche einem allgemein gültigen Standard (vergleiche dazu das Österreichische Informationssicherheitshandbuch ebenso wie den Standard des deutschen Bundesamts für Sicherheit in der Informationstechnik 200–2). Dies wird auch als Bestandteil der Risikomanagementmaßnahmen nach der NIS–2–Richtlinie und damit von der Leitungsebene sicherzustellen sein.

Der RH hielt daher seine Empfehlung aufrecht.

NIS–Richtlinien

4.1 (1) Die NIS–Richtlinie[7] aus 2016 beinhaltete Maßnahmen für ein gemeinsames hohes Sicherheitsniveau von Netz– und Informationssystemen in der EU. Österreich setzte sie mit dem Netz– und Informationssystemsicherheitsgesetz (**NISG**)[8] in nationales Recht um. Das NISG verpflichtete

- Betreiber wesentlicher Dienste (z.B. Energieversorger, Trinkwasserversorger, Kreditinstitute, Krankenanstaltenträger),
- Anbieter digitaler Dienste (z.B. Online–Marktplatz)
- und – über den Anwendungsbereich der Richtlinie hinausgehend – auch Einrichtungen des Bundes (z.B. Bundesministerien)

zu geeigneten und verhältnismäßigen technischen und organisatorischen Sicherheitsvorkehrungen. Die Länder konnten diese Vorschriften für ihren Wirkungsbereich auf freiwilliger Basis mittels Landesgesetz für anwendbar erklären. Bis Dezember 2023 hatte das Land Kärnten – so wie auch die anderen Länder – kein solches Landesgesetz erlassen (TZ 2, Abbildung 1: Elemente 1 und 4).

[7] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz– und Informationssystemen in der Union, ABl. L 2016/194, 1

[8] BGBl. I 111/2018

Die in der NIS–Richtlinie vorgesehene nationale Strategie für Cybersicherheit (in der Folge: **Cybersicherheitsstrategie 2021**)[9] diente der gesamtstaatlichen Vorbeugung und Abwehr von Cyberbedrohungen, um die Handlungsfähigkeit des Staates zu schützen.[10] Zur Zusammenarbeit mit den Ländern und Gemeinden verwies die Cybersicherheitsstrategie 2021 auf einen regelmäßigen Austausch. Die relevanten Strukturen dafür waren in der Strategie nicht enthalten (TZ 2, Abbildung 1: Element 6).

(2) Zur Erhöhung des Niveaus der Cybersicherheit in der EU erließen das Europäische Parlament und der Rat im Dezember 2022 die NIS–2–Richtlinie mit einem erweiterten Anwendungsbereich.[11] Die neue Richtlinie erfasste auch wesentliche bzw. wichtige Einrichtungen der öffentlichen Verwaltung auf Ebene der Zentralregierungen (Bundesebene) bzw. auf regionaler Ebene (Länderebene). Weitere Voraussetzung für die Anwendbarkeit der Richtlinie war, dass die nach nationalem Recht definierten regionalen Einrichtungen der öffentlichen Verwaltung nach einer risikobasierten Bewertung Dienste erbringen, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte (TZ 2, Abbildung 1: Element 2).

Die NIS–2–Richtlinie verpflichtete die Mitgliedstaaten, sicherzustellen[12], dass die erfassten Einrichtungen Sicherheitsmaßnahmen (Risikomanagementmaßnahmen) ergreifen. Dabei sind in einem gefahrenübergreifenden Ansatz sämtliche möglichen externen und internen Risiken sowie sämtliche genutzten Netz– und Informationssysteme zu berücksichtigen. Ausdrücklich sollen die Leitungsorgane der Einrichtungen zur Überwachung und Teilnahme an Schulungen verpflichtet werden. Auch für die wichtigen Einrichtungen im öffentlichen Bereich – z.B. die Einrichtungen der Länder – sind abgeschwächte Aufsichtsmaßnahmen (ex post) grundsätzlich vorzusehen.

Die NIS–2–Richtlinie ist bis Oktober 2024 in nationales Recht umzusetzen. Für die legistischen Vorbereitungsarbeiten ist federführend das Bundeskanzleramt in Abstimmung mit dem Bundesministerium für Inneres (in der Folge: **Innenministerium**) zuständig. Die konkrete Ausgestaltung der gesetzlichen Regelungen zur Einbeziehung der Länder war zur Zeit der Gebarungsüberprüfung noch offen. Im November 2023 ersuchte die Landeshauptleutekonferenz die beiden Ministerien dringend um eine umfassende Einbindung der Länder in die innerstaatliche Umset-

9 Beschluss der Bundesregierung von Dezember 2021

10 https://www.bundeskanzleramt.gv.at/dam/jcr:79eff5f6-20ed-4cf7-8d71-a6a02e4c49b3/Cyberstrategie2021.pdf (abgerufen am 19. August 2024)

11 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS–2–Richtlinie), ABl. L 2022/333, 80

12 Art. 20, 21, 31 ff.

zung und um die Einrichtung einer Bund–Länder–Arbeitsgruppe. Weitergehende vorbereitende Maßnahmen traf das Land Kärnten unter Hinweis auf den fehlenden konkreten Gesetzestext nicht (TZ 2, Abbildung 1: Element 5).

4.2 (1) Der RH stellte fest, dass die NIS–2–Richtlinie durch die ausdrückliche Einbeziehung von Einrichtungen der öffentlichen Verwaltung auf Landesebene und den gefahrenübergreifenden Ansatz dazu führt, dass sich die Sicherheitsanforderungen an die Länder erhöhen und mögliche Aufsichtsmaßnahmen vorzusehen sind. Dies erfordert ein umfassendes Risiko– und Notfallmanagementsystem für die IT der Landesverwaltungen.

Der RH empfahl dem Land Kärnten, sich auf die Anforderungen durch die Umsetzung der NIS–2–Richtlinie vorzubereiten und den nationalen Umsetzungsprozess zu begleiten, um die wesentlichen Themen – wie Risikomanagement, Notfallvorsorge, Krisenmanagement, Verantwortung der Leitungsebene, Informationsklassifizierung – zeitgerecht zu berücksichtigen. Dabei wäre eine Zusammenarbeit mit den in gleicher Weise betroffenen anderen Bundesländern anzustreben.

(2) Bereits in seinem Bericht „Koordination der Cyber–Sicherheit“ (Reihe Bund 2022/13, TZ 4 und TZ 29) hatte der RH die (Nicht–)Einbeziehung der Länder in die Verpflichtungen nach dem NISG festgehalten. Weil die Einrichtungen der Länder nicht dem gleichen verpflichtenden Schutzniveau wie die vergleichbaren Einrichtungen des Bundes unterstellt waren, hatte er empfohlen, auf eine Einbeziehung der Länder hinzuwirken.

Der RH kritisierte, dass das Land Kärnten – unabhängig von bzw. trotz der vorliegenden ISO/IEC–Zertifizierung – keine Initiative für ein Landesgesetz zur Herstellung eines gleichen verpflichtenden Schutzniveaus auf Bundes– und Landesebene durch die Übernahme der Pflichten aus dem NISG gesetzt hatte.

Er empfahl dem Land Kärnten, darauf hinzuwirken, dass auch auf Landesebene den Verpflichtungen gemäß NISG zu Sicherheitsvorkehrungen für die Netz– und Informationssysteme bestmöglich entsprochen wird. Dies mit dem Ziel, zu einem einheitlichen Schutzniveau im Cyber–Bereich auf Ebene aller Gebietskörperschaften beizutragen.

4.3 Das Land Kärnten teilte in seiner Stellungnahme mit, sich intensiv mit der Umsetzung der NIS–2–Richtlinie einschließlich der legistischen und organisatorischen Aspekte zu beschäftigen. Auf IT–Ebene erfolge bereits eine Zusammenarbeit und Abstimmung mit anderen Ländern. Ab Herbst 2024 sei auf Länderebene eine entsprechende Arbeitsgruppe im IT–Bereich geplant.

Zur Empfehlung, auch auf Landesebene den Verpflichtungen gemäß NISG bestmöglich zu entsprechen, führte das Land Kärnten aus, dass eine landesgesetzliche Anwendbarerklärung von Pflichten aus dem NISG auf eine verfassungsrechtlich fragwürdige Vorgangsweise hinauslaufen würde. Dem Bund fehle die Kompetenz, ein solches landesgesetzliches Opting–in vorzusehen. Zudem sei kein praktischer Mehrwert für ein solches Landesgesetz ersichtlich, weil schon die DSGVO geeignete technische und organisatorische Maßnahmen vorschreibe, das Land ohnehin in die gesamtstaatlichen Strukturen eingebunden und im Beirat zum Schutz kritischer Infrastruktur vertreten sei.

4.4 Der RH erwiderte dem Land Kärnten, dass seine Empfehlung – abgesehen von allfälligen verfassungsrechtlichen Grundsatzüberlegungen – darauf abzielte, die nach dem NISG vorgesehenen und von öffentlichen Einrichtungen des Bundes anzuwendenden Sicherheitsvorkehrungen auch auf Landesebene für die Einrichtungen der Verwaltung des Landes Kärnten bestmöglich umzusetzen. Zum Argument des Landes Kärnten, dass schon die DSGVO geeignete technische und organisatorische Maßnahmen vorschreibe, hielt der RH fest, dass sich der Anwendungsbereich der DSGVO auf den Schutz personenbezogener Daten, jener des NISG dagegen allgemein auf die Verfügbarkeit von Netz– und Informationssystemen bezog. Die Einbindung in die organisatorischen Strukturen zum Schutz der staatlichen Funktionsfähigkeit bzw. der kritischen Infrastrukturen war nach Ansicht des RH als eine weitere Maßnahme neben der erforderlichen Eigenvorsorge zu sehen.

Der RH hielt daher seine Empfehlung aufrecht. Ergänzend wies er darauf hin, dass ein Bundesgesetz zur Umsetzung der NIS–2–Richtlinie (NISG 2024) bis August 2024 noch nicht beschlossen war. Aufgrund des Begutachtungsverfahrens war jedoch zu erwarten, dass die Einrichtungen der Verwaltung der Länder (Ämter der Landesregierungen und Bezirkshauptmannschaften) denselben Risikomanagementmaßnahmen und Berichtspflichten unterliegen werden wie die Einrichtungen der Verwaltung des Bundes.

IT–Sicherheitsstrategie

5.1 (1) Das Österreichische Informationssicherheitshandbuch[13] empfahl, eine schriftliche IT–Sicherheitsstrategie für die Gesamtorganisation als Grundlage des IT–Sicherheitsmanagements zu erstellen und durch die Leitungsebene („Management Commitment“) für alle Bediensteten transparent in Kraft zu setzen. Dieses strategische Dokument sollte klare Ziele, Verantwortlichkeiten (einschließlich der Unterstützung durch die Leitungsebene) und nachvollziehbare Methoden des IT–Sicherheitsmanagements festlegen.

(2) Die folgende Tabelle stellt dar, inwiefern das Land Kärnten diese Kriterien erfüllte:

Tabelle 1: IT–Sicherheitsstrategie

Kriterien	Umsetzung durch das Land Kärnten
IT–Sicherheitsstrategie vorhanden	ja, aus 2018
Bezeichnung	„Sicherheitspolitik für das IT–System des Landes Kärnten (Generalpolicy)“
weitere Umsetzungsdokumente	Detailpolicies (z.B. Zwei–Faktor–Authentifizierung aus 2022)
Erfassung des nachgeordneten Bereichs	ja, Dienststellen des Amtes der Landesregierung und Bezirkshauptmannschaften
unterzeichnet von	Landesamtsdirektor
Kundmachung mit Rundschreiben	ja (Erlasssammlung im Intranet)
wesentliche Ziele der IT–Sicherheitsstrategie	• Informationssicherheits–Managementsystem (ISMS) für eine funktionierende und geschützte IT–Infrastruktur • Verfügbarkeit von Daten • Risikobewertung
Verantwortung der oberen Leitungsebene	nicht festgelegt
Organisation und Personal	Regelungen enthalten

Quelle: Land Kärnten

Die IT–Sicherheitsstrategie des Landes Kärnten stammte aus dem Jahr 2005 und wurde im Jahr 2018 – und damit zuletzt vor dem Cyber–Angriff – mit Erlass des Landesamtsdirektors aktualisiert. Die Verantwortung der oberen Leitungsebene für die IT–Sicherheit war darin nicht festgelegt. Der in der IT–Abteilung etablierte Risikomanagementprozess war in eigenen Dokumenten beschrieben; die IT–Sicherheitsstrategie führte die Risikobewertung als ein generelles Ziel an, stellte diese aber nicht näher dar. Wie die Bediensteten bei möglichen Cyber–Angriffen vorzugehen hatten, war in im Intranet zugänglichen Informationen sowie in Schulungsunterlagen vorgegeben; in der IT–Sicherheitsstrategie fehlte ein konkreter Hinweis auf die

[13] Version 4.4.0 Kapitel 4

zu verständigenden Anlaufstellen[14]. Weiters enthielt die IT–Sicherheitsstrategie keine Regelungen für die Zusammenarbeit mit bestehenden Gremien zur Cyber–Sicherheit.

Nach dem Cyber–Angriff von Mai 2022 (TZ 18) setzte die Cyber–Einsatz–Gruppe auf Ebene der Landesamtsdirektion (TZ 22) das Ziel, die IT–Sicherheitsstrategie zu evaluieren. Eine Aktualisierung der IT–Sicherheitsstrategie war bis Ende 2023 noch nicht abgeschlossen. Die übergeordnete IT–Strategie des Landes wurde im September 2023 aktualisiert. Sie maß einer umfassenden, aktuellen IT–Sicherheitsstrategie entscheidende Bedeutung zu. Weiters sah sie als Maßnahmen für die IT–Sicherheitsstrategie Mitarbeiterschulungen und technische Sicherheitsmaßnahmen in der zentralen IT–Infrastruktur und am IT–Arbeitsplatz vor. Nicht alle dieser, auf den aktuellen Stand der Technik bezogenen Sicherheitsmaßnahmen waren in der IT–Sicherheitsstrategie aus 2018 enthalten. Insbesondere war auch die Zwei–Faktor–Authentifizierung (Erlass 2022) nicht berücksichtigt.

5.2 Der RH hielt fest, dass die IT–Strategie und die IT–Sicherheitsstrategie des Landes Kärnten wesentliche Ziele und nachvollziehbare Maßnahmen für alle – auch nachgeordnete – Dienststellen definierten und organisatorische sowie personelle Aspekte berücksichtigten.

Der RH hielt jedoch kritisch fest, dass das Land Kärnten die IT–Sicherheitsstrategie seit 2018 nicht aktualisiert hatte. Dies betraf vor allem die folgenden fehlenden Punkte:

- Verantwortung der oberen Leitungsebene,
- zusammenfassende Darstellung des Risikomanagementprozesses,
- konkrete Hinweise auf Anlaufstellen bei Cyber–Angriffen für alle Bediensteten,
- Abstimmung mit der IT–Strategie 2023 sowie mit dem Erlass zur Zwei–Faktor–Authentifizierung aus 2022,
- Regelungen zur Zusammenarbeit mit bestehenden Gremien zur Cyber–Sicherheit.

Der RH empfahl dem Land Kärnten, seine IT–Sicherheitsstrategie unter Berücksichtigung der IT–Strategie des Landes aus 2023 zu aktualisieren und zukünftig ihre Aktualität regelmäßig zu überprüfen.

Insbesondere wären in der IT–Sicherheitsstrategie

- die Verantwortung der oberen Leitungsebene für die IT–Sicherheit ausdrücklich festzulegen,
- die Grundzüge des Risikomanagementprozesses zu dokumentieren,

[14] außer bei einer Verletzung des Schutzes personenbezogener Daten nach der DSGVO

- die Hinweise für alle Bediensteten zum Vorgehen bei Cyber–Angriffen zu konkretisieren und
- Regelungen zur Zusammenarbeit mit bestehenden Gremien zur Cyber–Sicherheit aufzunehmen.

Dies wäre auch im Hinblick auf die Umsetzung der NIS–2–Richtlinie zweckmäßig.

5.3 Laut Stellungnahme des Landes Kärnten werde die IT–Sicherheitsstrategie aktualisiert und nach den Vorgaben der NIS–2–Richtlinie angepasst, sobald das NISG 2024 verabschiedet worden sei. Vorarbeiten dazu seien schon geleistet worden.

5.4 Der RH merkte an, dass ein Bundesgesetz zur Umsetzung der NIS–2–Richtlinie (NISG 2024) bis August 2024 noch nicht beschlossen war.

Management von IT–Sicherheitsrisiken und Berichtswesen

6.1 (1) Das Österreichische Informationssicherheitshandbuch[15] empfahl zur Reduktion möglicher IT–Sicherheitsrisiken eine Risikoanalyse und –bewertung der IT–Verfahren und IT–Systeme sowie die Festlegung entsprechender Maßnahmen. Diese Maßnahmen konnten je nach festgestelltem Schutzbedarf für die einzelnen IT–Verfahren und IT–Systeme als pauschale Grundschutzmaßnahmen bei niedrigem Risiko oder als individuelle, detaillierte Maßnahmen bei höherem Risiko ausgestaltet sein (kombinierter Ansatz). Die Durchführung der Risikoanalysen lag im Aufgabenbereich der IT–Abteilung unter Beiziehung der Fachabteilungen, die ein IT–Verfahren nutzten.

Wie im Österreichischen Informationssicherheitshandbuch und in der NIS–2–Richtlinie festgehalten, war die obere Leitungsebene für die Steuerung und Optimierung der IT–Sicherheit verantwortlich. Zur Wahrnehmung dieser Verantwortung benötigte sie regelmäßig bzw. im Anlassfall Informationen zu den Eckdaten der IT–Sicherheit, z.B. zum Stand der Umsetzung der Sicherheitsanforderungen, zu Sicherheitskennzahlen, zu aktuellen Sicherheitsrisiken und Sicherheitsschwachstellen oder

[15] Version 4.4.0 Kapitel 5 und 18.1.2; siehe auch den RH–Bericht „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31, TZ 8)

zu Cyber–Angriffen. Das Österreichische Informationssicherheitshandbuch empfahl, das interne Berichtswesen so zu strukturieren,

- dass konkrete Anlassfälle – z.B. Cyber–Angriffe – jedenfalls an die Leitungsebene zu berichten sind und
- dass regelmäßige Berichte mit aktuellen Sicherheitskennzahlen zu erstatten sind.

(2) Die Systematik des Managements von IT–Sicherheitsrisiken sowie das Berichtswesen stellten sich im Land Kärnten wie folgt dar:

Tabelle 2: Systematik des Managements von IT–Sicherheitsrisiken und Berichtswesen

Kriterium	Umsetzung im Land Kärnten
Risikomanagement	
Dokumentation	ja, in Prozessbeschreibungen
Ansatz	kombiniert (Grundschutzmaßnahmen und individuelle Sicherheitsmaßnahmen je nach Schutzbedarf)
Schutzbedarfs– und Risikoanalysen	ja, regelmäßig
Berichtswesen	
Dokumentation	ja, für anlassbezogene Berichte
Festlegung von Berichtsweg und Berichtsempfängerin bzw. –empfänger	ja
Erstellung von regelmäßigen Berichten	ja
Empfängerin bzw. Empfänger regelmäßiger Berichte	Leitung IT–Abteilung; Leitung Landesamtsdirektion

Quelle: Land Kärnten

Die IT–Abteilung des Landes Kärnten richtete bereits vor dem Cyber–Angriff ein IT–Risikomanagementsystem ein. Sie erstellte bzw. aktualisierte die Risikoanalysen für die allgemeinen IT–Risiken (z.B. Projektrisiken, Ressourcenmangel) jährlich, die Risikoanalysen für die einzelnen IT–Systeme gemeinsam mit den Fachabteilungen – unabhängig von der Höhe des Risikos – alle fünf Jahre. Auch nach dem Cyber–Angriff im Jahr 2022 waren Bedrohungen aus Cyber–Angriffen nicht angeführt.

Die Risiken wurden nach Eintrittswahrscheinlichkeit und Auswirkungen bewertet und daraus Sicherheitsmaßnahmen abgeleitet. Die Ergebnisse aus der Aktualisierung der Risikoanalysen, aus den internen und externen Sicherheitsüberprüfungen, den laufenden Verbesserungsmaßnahmen und der Bewältigung von (Sicherheits–) Vorfällen flossen in die jährliche Managementbewertung der IT–Abteilung ein.

(3) Ein regelmäßiges Berichtswesen war in der IT–Sicherheitsstrategie des Landes Kärnten nicht vorgesehen. Monatlich erstellte die IT–Abteilung für sich interne technische Prüfprotokolle sowie jährlich einen internen zusammenfassenden Themenbericht.

Bei den mehrmals pro Jahr stattfindenden Koordinationssitzungen der Landesamtsdirektion berichtete die IT–Abteilungsleitung mündlich über aktuelle Entwicklungen. Die obere Leitungsebene (Landesamtsdirektion und Büro des zuständigen Mitglieds der Landesregierung) erhielt jährlich einen Managementbericht der IT–Abteilung, der auch IT–Sicherheit umfasste. Diesen Managementbericht erläuterte die IT–Abteilungsleitung in unregelmäßig stattfindenden Lenkungsausschüssen zur IT–Sicherheit (2016, 2019, 2021; siehe dazu TZ 9). Einen standardisierten, jährlichen, zusammenfassenden Bericht zur IT–Sicherheit an die obere Leitungsebene gab es nicht.

Anlassbezogene Meldungen bzw. Berichte waren bei Cyber–Angriffen vorgesehen, Berichtsweg und Berichtsempfängerin bzw. Berichtsempfänger waren festgelegt.

6.2 Der RH anerkannte, dass das Land Kärnten ein IT–Risikomanagementsystem eingerichtet und dokumentiert hatte.

Er hielt kritisch fest, dass die IT–Abteilung in den Risikoanalysen für die allgemeinen IT–Risiken aktuelle Bedrohungen aus Cyber–Angriffen nicht anführte.

Weiters hielt der RH kritisch fest, dass die IT–Abteilung die Risikoanalysen für die einzelnen IT–Systeme gemeinsam mit den zuständigen Fachabteilungen unabhängig von der Höhe des Risikos alle fünf Jahre aktualisierte.

Der RH empfahl dem Land Kärnten, die Risikoanalysen für die allgemeinen IT–Risiken jedenfalls um Bedrohungen aus Cyber–Angriffen zu erweitern.

Weiters empfahl er dem Land Kärnten, die IT–Systeme nach der Höhe des Risikos und den möglichen Auswirkungen einer Störung auf die Verwaltungstätigkeit festzulegen. Die Risikoanalysen einzelner IT–Systeme mit hohem Risiko wären in kürzeren Abständen (z.B. jährlich oder alle drei Jahre) zu überprüfen und gegebenenfalls zu aktualisieren.

Der RH wies kritisch darauf hin, dass die IT–Sicherheitsstrategie des Landes Kärnten kein regelmäßiges Berichtswesen vorsah und die obere Leitungsebene des Landes (Leitung Landesamtsdirektion, zuständiges Mitglied der Landesregierung) keine regelmäßigen und schriftlichen standardisierten Berichte mit Kennzahlen zur IT–Sicherheit für die Überwachung und Steuerung des IT–Sicherheitsmanagements erhielt.

Der RH empfahl dem Land Kärnten, in der IT–Sicherheitsstrategie ein regelmäßiges, standardisiertes Berichtswesen zur IT–Sicherheit – unter Einbeziehung der oberen Leitungsebene (Leitung Landesamtsdirektion, zuständiges Mitglied der Landesregierung) als Berichtsempfänger – festzulegen. Dies wäre auch im Hinblick auf die Überwachungspflichten der Leitungsorgane nach der NIS–2–Richtlinie (Art. 20 Abs. 1) zweckmäßig.

6.3 Laut Stellungnahme des Landes Kärnten werde der Empfehlung zur Erweiterung der Risikoanalysen zu den allgemeinen IT–Risiken um Bedrohungen aus Cyber–Angriffen Folge geleistet. Weiters werde die bestehende Risikoanalyse zu einzelnen IT–Systemen adaptiert und würden die Prüfzyklen entsprechend der Empfehlung angepasst. Dazu werde ein Information Security Management System (ISMS) evaluiert. Das bestehende Berichtswesen werde zudem um den vom RH empfohlenen Teilnehmerkreis erweitert und in der IT–Sicherheitsstrategie niedergeschrieben.

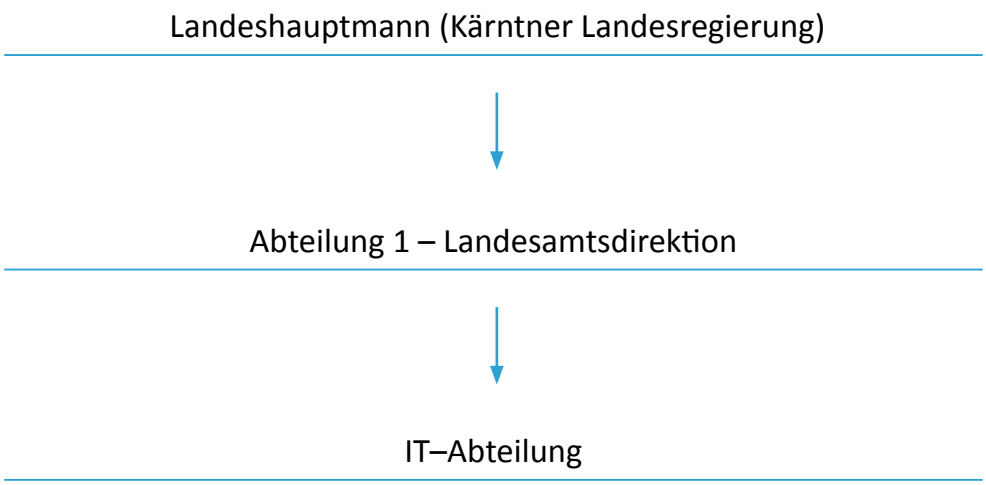
IT–Sicherheitsorganisation

Aufbau der IT–Sicherheitsorganisation

7.1 (1) Gemäß dem Österreichischen Informationssicherheitshandbuch hatte jede Institution die Organisation ihres Informationssicherheits–Managements spezifisch – nach Größe, Struktur und Aufgaben – festzulegen.[16]

Im Land Kärnten lag die Verantwortung für die IT–Sicherheit auf Ebene der Landesregierung beim Landeshauptmann[17]. Die unmittelbare Leitung der IT und der IT–Sicherheit des Landes[18] war – sowohl vor als auch nach dem Cyber–Angriff 2022 – der Abteilung „Informationstechnologie“ (in der Folge: **IT–Abteilung**), einer Unterabteilung der Abteilung 1 – Landesamtsdirektion, zugeordnet:

Abbildung 2: Organisation der IT–Sicherheit im Land Kärnten



Quelle: Land Kärnten; Darstellung: RH

Die IT–Abteilung war u.a. für Softwareentwicklung und Datenbankservices, Fachanwendungen und Projektmanagement sowie für die Systemtechnik (Serverbetrieb, Betrieb des Rechenzentrums, Datennetz) zuständig.

16 Version 4.4.0 Kapitel 6.1.3

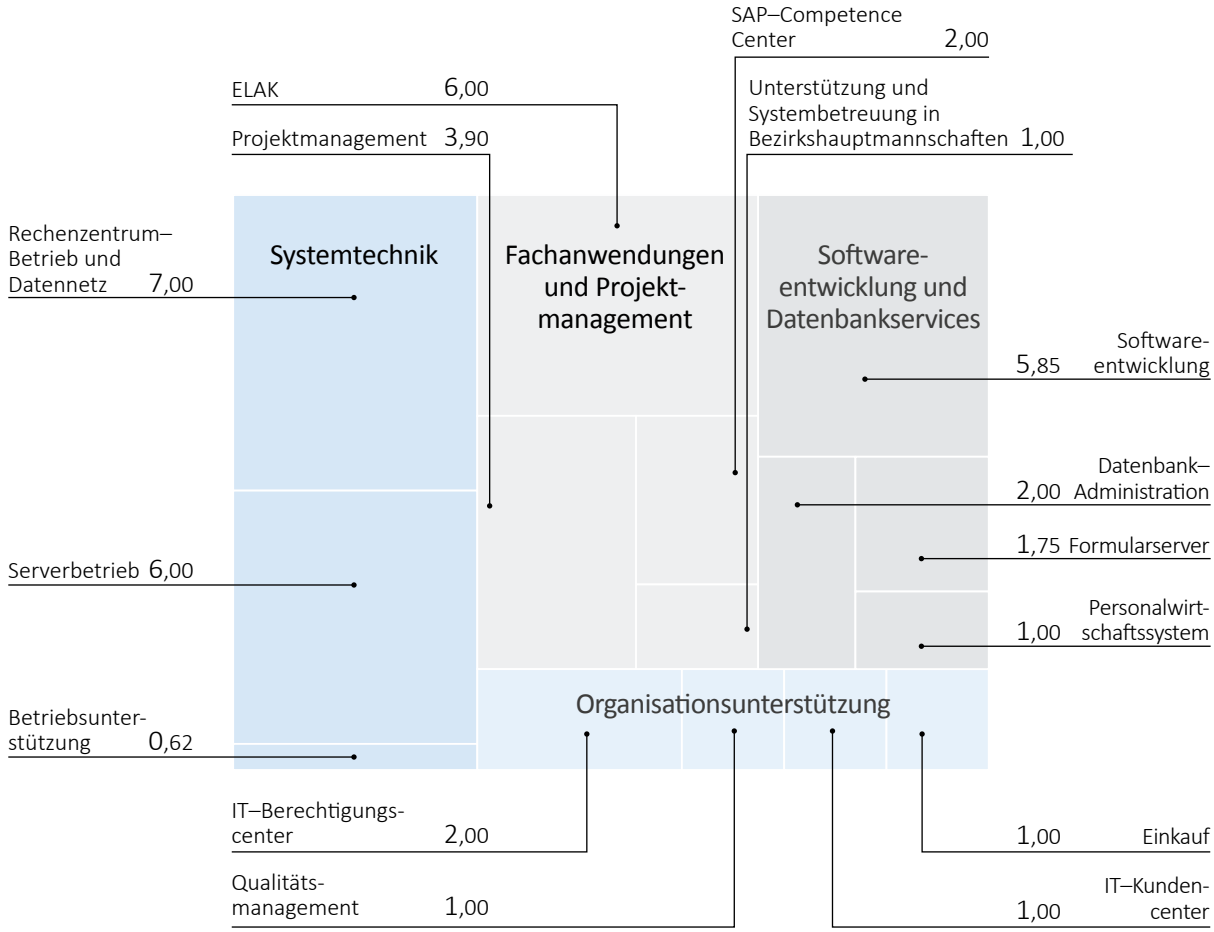
17 Dr. Peter Kaiser

18 Amt der Kärntner Landesregierung, Landesbehörden, Bezirkshauptmannschaften sowie nachgeordnete Anstalten, Betriebe und Dienststellen

In den weiteren Fachabteilungen gab es vor Ort insgesamt 48 Systemverantwortliche (zuzüglich 48 Stellvertretungen), die als erste Anlaufstellen für IT–Angelegenheiten das organisatorische Bindeglied zur IT–Abteilung bildeten, dieser aber nicht unterstellt waren.[19]

Abbildung 3 zeigt die Organisation der IT–Abteilung (ohne Sekretariat), ihre Aufgaben und das zugeordnete Personal in Vollzeitäquivalenten (in Summe 42,12) mit Stand August 2023:

Abbildung 3: IT–Abteilung: Gruppen, Aufgaben und Personalstand in Vollzeitäquivalenten



Angaben in Vollzeitäquivalenten;
Stand August 2023; die Größe der Fläche der Rechtecke entspricht der Anzahl der Vollzeitäquivalente.

Quelle: Land Kärnten; Darstellung: RH

[19] Aufgabengebiete waren u.a. Begleitung von Hardware Rollouts, Anfragen zu Hardware– und Softwareanforderungen, Druckerangelegenheiten, Datensicherung, Installation und Konfiguration von Softwareprodukten, Unterstützung des Notbetriebs im Stör– oder Katastrophenfall.

Dem Leiter der IT–Abteilung waren ausschließlich Leitungsaufgaben zugewiesen, der Stellvertretung und den Gruppenleitungen auch operative Aufgaben innerhalb ihrer Gruppen.

Die IT–Sicherheit war als Querschnittsmaterie kein eigens ausgewiesener Aufgabenbereich. Der Informationssicherheitsmanager (Gruppe Softwareentwicklung und Datenbankservices) und der Leiter der Gruppe Systemtechnik nahmen im überprüften Zeitraum die Angelegenheiten der IT–Sicherheit wahr.

(2) Im überprüften Zeitraum gab es zwei Wechsel der IT–Abteilungsleitung, die Stellvertretung wechselte nicht; die drei IT–Abteilungsleiter des überprüften Zeitraums waren in folgenden Zeiträumen tätig:

- bis 31. März 2022,
- von 1. Juni 2022 bis 31. Mai 2023,
- seit 12. Juni 2023.

Von 1. April bis 31. Mai 2022 und damit auch zu Beginn des Cyber–Angriffs (TZ 18) war die IT–Abteilungsleitung nicht besetzt.

Im Juli 2021 erklärte der damalige IT–Abteilungsleiter, mit Ende März 2022 aus dem Dienststand ausscheiden und in den Ruhestand übertreten zu wollen. Die öffentliche Ausschreibung für seine Nachbesetzung erfolgte am 16. Dezember 2021.[20]

Das Land Kärnten begründete die Vorgangsweise, erst im Dezember auszuschreiben, damit, dass der ausscheidende IT–Abteilungsleiter seine Erklärung bis spätestens drei Monate vor ihrer Wirksamkeit (und damit bis Jahresende 2021) hätte widerrufen können. Der im Auswahlverfahren Erstgereihte zog seine Bewerbung mit 31. März 2022 zurück, Anfang April 2022 vereinbarte die Personalabteilung mit dem Zweitgereihten dessen Dienstantritt am 1. Juni 2022.

7.2 Der RH hielt fest, dass die Leitung der IT–Abteilung von 1. April 2022 bis 31. Mai 2022 und damit auch zu Beginn des Cyber–Angriffs unbesetzt war. Er kritisierte, dass das Land Kärnten – unter Berufung auf einen möglichen Widerruf der Ausscheidenserklärung – die Neuausschreibung der Funktion der IT–(Unter–)Abteilungsleiterin bzw. des –leiters erst im Dezember 2021 (dreieinhalb Monate vor Freiwerden der Funktion) durchführte und es dadurch zu einer zweimonatigen Vakanz in der Leitung der IT–Abteilung kam. Damit waren ein nahtloser Übergang und eine geordnete Übergabe der Agenden durch den bisherigen Funktionsinhaber nicht möglich; die

[20] § 14 Abs. 1 Kärntner Objektivierungsgesetz (LGBl. 98/1992 i.d.g.F.): Das Kärntner Objektivierungsgesetz sah die Ausschreibung von bestimmten Leitungsfunktionen möglichst Monate vor Freiwerden der Funktion vor. Die Funktion der IT–(Unter–)Abteilungsleiterin bzw. des –leiters fiel jedoch nicht unter diese Regelung.

Wissensübertragung sowie strategische, nachhaltige Entscheidungen waren im Übergangszeitraum in der Abteilung erschwert.

Der RH empfahl dem Land Kärnten, frei werdende Stellen in leitenden Positionen so bald als möglich und – in Anlehnung an die Bestimmungen zur Ausschreibung von bestimmten Leitungsfunktionen gemäß dem Kärntner Objektivierungsgesetz – im Idealfall bereits sechs Monate vor dem bekannten Ausscheiden auszuschreiben, um eine nahtlose Nachbesetzung der Stelle zu ermöglichen.

7.3 Laut Stellungnahme des Landes Kärnten sei mit der Dienstrechtsnovelle LGBl. 90/2023 die Widerrufsfrist einer Erklärung auf Versetzung in den Ruhestand für alle Beamtinnen und Beamten von bisher drei Monaten auf sechs Monate verlängert worden. Dadurch verbessere sich die Personalplanung im Sinne einer möglichen frühzeitigen Nachbesetzung deutlich.

Funktionen in der IT–Sicherheitsorganisation

8.1 (1) Für die effiziente Wahrnehmung der operativen Aufgaben der IT–Sicherheit war es gemäß Österreichischem Informationssicherheitshandbuch[21] notwendig, Funktionen und klare Verantwortlichkeiten festzulegen. Dafür hatten sich national und international Standardfunktionen (Rollen, Tätigkeiten) mit entsprechenden Aufgaben etabliert:

- Die im internationalen Kontext geläufige Funktion für alle Fragen der Informations– und IT–Sicherheit ist der Chief Information Security Officer (**CISO**), der zentral für Informations– und IT–Sicherheit verantwortlich ist.
- Der Leiter der für die gesamte Infrastruktur und für den Betrieb verantwortlichen IT–Abteilung wird auch als Chief Information Officer (**CIO**) bezeichnet.
- Der Chief Digital Officer (**CDO**) ist für die Digitalisierungsstrategie und Digitalisierungsmaßnahmen gesamtverantwortlich.

[21] Version 4.4.0 Kapitel 6.1.3

(2) Im Land Kärnten gab es aus Anlass des Cyber–Angriffs keine Änderungen bei den festgelegten Funktionen. Tabelle 3 zeigt die Funktionen der IT–Sicherheitsorganisation im überprüften Zeitraum:

Tabelle 3: Funktionen der IT–Sicherheitsorganisation

Funktion	verantwortlich für	zuständige Person im Land Kärnten
Chief Information Security Officer (CISO)	Informationssicherheit; somit auch für die IT–Sicherheit	seit 15. Jänner 2024 eingerichtet
Leiter der IT–Abteilung / Chief Information Officer (CIO)	IT–Infrastruktur	IT–Abteilungsleitung
Chief Digital Officer (CDO)	Entwicklung und Umsetzung einer grundlegenden Digitalisierungsstrategie	IT–Abteilungsleitung
Informationssicherheitsmanager	technische Leitung; Umsetzung der ISO/IEC–Norm 27001	Referent IT–Abteilung

Quelle: Land Kärnten

Der RH stellte dazu fest:

- Ein für die Informations– und IT–Sicherheit gesamtverantwortlicher Chief Information Security Officer (CISO) war im Land Kärnten bis zum 15. Jänner 2024 nicht eingerichtet. Dessen Aufgaben waren bis dahin auf Mitarbeiter der IT–Abteilung (den Abteilungsleiter und den Informationssicherheitsmanager) aufgeteilt.
- Im Land Kärnten war ein Informationssicherheitsmanager eingerichtet, dem die Umsetzung der Vorgaben nach der ISO/IEC–Norm 27001 oblag.
- Die Funktion des Chief Digital Officers (CDO) wurde mit 12. Juni 2023 erstmals besetzt.

8.2 Der RH hielt fest, dass das Land Kärnten mit 15. Jänner 2024 einen Chief Information Security Officer (CISO) einsetzte; ein Informationssicherheitsmanager für die Umsetzung der ISO/IEC–Norm 27001 war auch schon vorher eingerichtet.

Informationssicherheitsmanagement–Team

9.1 (1) Für die Umsetzung der IT–Sicherheitsziele ist die organisationsweite Koordinierung der IT–Sicherheit wesentlich. Die Koordinierung sollte jedenfalls die Führungskräfte, die für die IT–Sicherheit verantwortlichen Funktionsträger und ausgewählte Vertretungen der Anwenderinnen und Anwender umfassen. Bei Bedarf können auch weitere Expertinnen und Experten, beispielsweise zum Risikomanagement, sowie die nachgeordneten Dienststellen eingebunden werden.

In größeren Organisationen war es daher zweckmäßig – wie im Österreichischen Informationssicherheitshandbuch dargestellt – ein Informationssicherheitsmanagement–Team (ISMT)[22] aufzubauen, das die Verantwortlichen unterstützt, die übergreifenden Belange der IT–Sicherheit koordiniert sowie Pläne, Vorgaben und Richtlinien (z.B. Schutzmaßnahmen, Klassifizierung und Kennzeichnung von Informationen) erarbeitet. Laut Österreichischem Informationssicherheitshandbuch sollte neben dem Chief Information Security Officer (CISO) und seiner Stellvertretung auch eine Vertreterin bzw. ein Vertreter der Anwenderinnen und Anwender Mitglied des Informationssicherheitsmanagement–Teams sein.

(2) Das Land Kärnten verfügte im überprüften Zeitraum – sowohl vor als auch nach dem Cyber–Angriff – über kein Informationssicherheitsmanagement–Team. Die IT–Abteilung initiierte nach 2016 und 2019 zuletzt im September 2021 eine Sitzung des Lenkungsausschusses zur IT–Sicherheit, um künftige Entwicklungen zum Thema IT–Sicherheit und Maßnahmen zur Erhöhung der IT–Sicherheit abzustimmen. Teilnehmerinnen und Teilnehmer dieses Ausschusses waren neben der IT–Abteilungsleitung und einem Mitarbeiter der IT–Abteilung Vertreterinnen und Vertreter weiterer Abteilungen des Landes Kärnten (Landesamtsdirektor, Präsidium, Verfassungsdienst, Personalabteilung). Der in unregelmäßigen Abständen einberufene Lenkungsausschuss erfüllte nicht die Anforderungen eines Informationssicherheitsmanagement–Teams. Aus Sicht des Landes Kärnten war der Lenkungsausschuss seitdem nicht mehr notwendig.

9.2 Der RH kritisierte, dass das Land Kärnten kein Informationssicherheitsmanagement–Team eingerichtet hatte. Dieses ist wesentlich für die organisationsweite Koordinierung der IT–Sicherheit.

Er empfahl dem Land Kärnten, ein Informationssicherheitsmanagement–Team gemäß den Vorgaben des Österreichischen Informationssicherheitshandbuchs einzurichten und dabei auf eine zweckentsprechende Einbindung der Anwenderinnen und Anwender sowie der nachgeordneten Dienststellen zu achten.

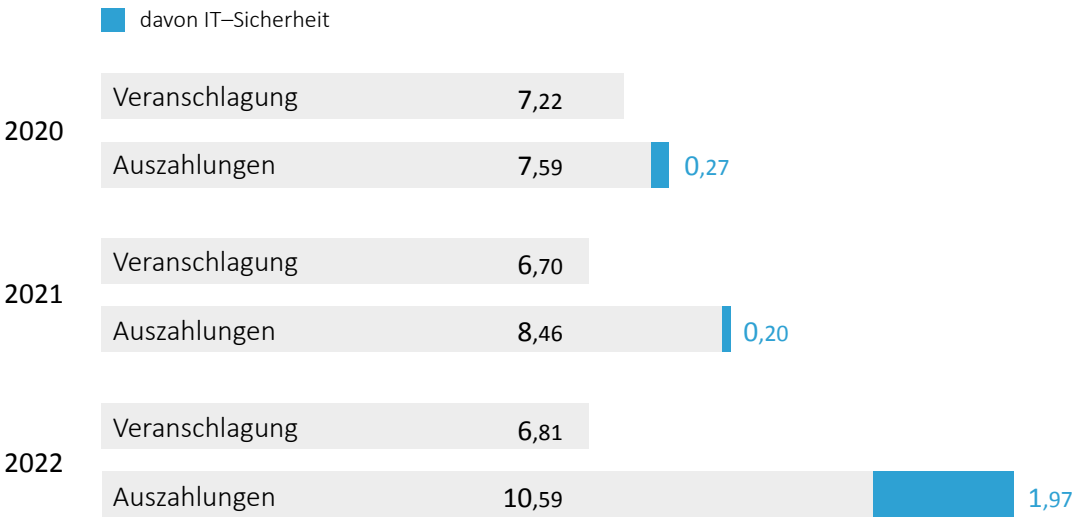
[22] Version 4.4.0 Kapitel 6.1.3.2

9.3 Laut Stellungnahme des Landes Kärnten werde ein entsprechendes Informationssicherheitsmanagement–Team unter der Leitung des Chief Information Security Officers (CISO) eingerichtet.

Auszahlungen für IT und IT–Sicherheit

10 Abbildung 4 zeigt die Auszahlungen des Landes Kärnten gemäß Finanzierungshaushalt für die IT–Sachkosten der IT–Abteilung einschließlich Dienstleistungen und den direkt zuordenbaren Anteil der Auszahlungen für IT–Sicherheit:

Abbildung 4: Auszahlungen für IT bzw. IT–Sicherheit in Mio. EUR



Quelle: Land Kärnten; Darstellung: RH

Die Auszahlungen für IT–Sachkosten betrugen im Jahr 2022 10,59 Mio. EUR, davon entfielen 1,97 Mio. EUR auf IT–Sicherheit. Das ergab gegenüber dem Jahr 2020 eine Steigerung der IT–Auszahlungen um 40 % und eine Steigerung der Auszahlungen für IT–Sicherheit um über 600 %. Die Auszahlungen überstiegen die Veranschlagungen in allen drei überprüften Jahren. Im Jahr 2022 war die Abweichung aufgrund des Cyber–Angriffs und der damit verbundenen, zusätzlich erforderlichen Mittel mit +3,78 Mio. EUR besonders ausgeprägt.

IT–Sicherheit bei Personal und Telearbeit

Regelungen und Maßnahmen zu IT–Sicherheit Personal

11.1 (1) Der RH orientierte sich bei der Überprüfung der Regelungen und Maßnahmen des Landes Kärnten für die IT–Sicherheit beim internen sowie externen Personal an den Vorgaben des Österreichischen Informationssicherheitshandbuchs, das insbesondere die Verpflichtung der Bediensteten zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen sowie die Aus– und Weiterbildung des Personals vorsah.

(2) Grundlegende Regelungen zur Amtsverschwiegenheit und Telearbeit enthielten die Kärntner Landesverfassung, das Kärntner Landesvertragsbedienstetengesetz 1994 und das Kärntner Dienstrechtsgesetz 1994. Weitere Vorgaben zum Umgang mit vertraulichen Informationen fanden sich in der Kanzleiordnung (TZ 3). In Vorgaben, Erlässen und Richtlinien zur IT–Sicherheit, zum Datenschutz und zur Telearbeit[23] gab es detailliertere Anweisungen zu IT–Sicherheitsaspekten für die Bereiche Organisation und Personal.

Die Datenschutzinformation des Dienstgebers aus 2018 enthielt veraltete Kontaktdaten der bzw. des Datenschutzbeauftragten. Nach dem Cyber–Angriff veröffentlichte das Land Kärnten im Intranet den „Erlass zur Meldepflicht bei Datenschutzverletzungen“ – mit den aktuellen Kontaktdaten des bzw. der Datenschutzbeauftragten – sowie den „Notfallplan für den IT–Sicherheitsvorfall Verschlüsselungsvirus und Derivate“.

(3) (a) Bereits vor Beschäftigungsbeginn setzte das Land Kärnten Maßnahmen, um die Qualifikation der zukünftigen Bediensteten und ihre Vertrauenswürdigkeit sicherzustellen: Die Bediensteten erhielten Informationen über die Verschwiegenheitspflicht und die Pflicht zum Schutz der zu verarbeitenden Daten.

(b) Während des Beschäftigungsverhältnisses boten freiwillig zu absolvierende Awareness–Schulungen (E–Learning–Kurse mit abschließender Wissensabfrage) eine laufende Sensibilisierung zur IT–Sicherheit. Die Fortbildungs– und Ausbildungsmaßnahmen, insbesondere für IT–Personal, nahmen die zuständigen Organisationseinheiten je nach Erfordernis in Anspruch. Zur Verbesserung der personellen IT–Sicherheit nach dem Cyber–Angriff sensibilisierte das Land Kärnten die Bediensteten im Umgang mit Phishing–Mails.

[23] z.B. Sicherheitspolitik für das IT–System des Landes Kärnten, Sicherheitspolitik für mobile Endgeräte, Erlass für die private Nutzung der IKT–Infrastruktur des Landes Kärnten durch seine Bediensteten, Datenschutzinformation des Dienstgebers für neu eintretende Mitarbeiterinnen und Mitarbeiter, Telearbeit Allgemein – Dienstverrichtung mittels Telearbeit

Informationen über mögliche Cyber–Angriffe, Meldewege, IT–Support und IT–Anforderungen waren dokumentiert und für die Bediensteten verfügbar bzw. abrufbar. Ebenso hatte das Land Kärnten Regelungen zur privaten Nutzung der dienstlichen IT–Ausstattung, zur elektronischen Kommunikation (aus dem Jahr 2014) und zu Passwörtern (aus dem Jahr 2018) in Kraft gesetzt.

(c) Die Beendigung des Dienstverhältnisses war in einem Prozess festgelegt, in dem Zugangs– und Zutrittsberechtigungen entzogen wurden sowie Unterlagen und Betriebsmittel zu retournieren waren.

(4) Das Land Kärnten beauftragte zur Entwicklung, zum Betrieb und zur Wartung von IT–Systemen externe Dienstleister. Die Vereinbarungen mit diesen beinhalteten neben der Leistungsbeschreibung auch Regelungen zur Einhaltung von einschlägigen Datenschutz– und IT–Sicherheitsvorschriften. Informationen über das Informationssicherheitsniveau der externen Dienstleister lagen der IT–Abteilung nicht in jedem Fall vor, z.B. Informationen zu Zertifizierungen nach der ISO/IEC–Norm 27001.

Das Land Kärnten behielt sich in den Vereinbarungen das Recht vor, Aspekte der Informationssicherheit bei seinen externen Dienstleistern zu überprüfen. Hierzu erstellte die IT–Abteilung ein Verzeichnis der externen Dienstleister samt Bewertung nach bestimmten Kriterien[24]. In den Jahren 2020 und 2021 führte die IT–Abteilung jeweils ein Lieferanten–Audit bei einem externen Dienstleister durch. Im Februar 2023 genehmigte die IT–Abteilung eine Richtlinie zur Überwachung, ob die externen Dienstleister die Service– und Betriebsführungsqualität einhielten.

Zur Entwicklung, Administration und Wartung von IT–Systemen benötigten die externen Dienstleister auch (Fern–)Zugriffe auf die IT–Systeme des Landes. Eine Regelung zur Beaufsichtigung und Überwachung von externen Dienstleistern zur Einhaltung der geltenden Anforderungen zur Informationssicherheit (Zertifikate, Know–how, Erfahrung) gab es im überprüften Zeitraum nicht. Laut Land Kärnten befinde sich diese in Ausarbeitung.

11.2 Der RH hielt anerkennend fest, dass das Land Kärnten in den Jahren 2020 und 2021 Lieferanten–Audits bei externen Dienstleistern durchführte.

Der RH kritisierte, dass der IT–Abteilung des Landes Kärnten das Informationssicherheitsniveau von externen Dienstleistern nicht in jedem Fall bekannt war. Aufgrund der Abhängigkeit von externen Dienstleistern in den Bereichen Entwicklung, Betrieb und Wartung konnten Sicherheitsrisiken bei den externen Dienstleistern auch zu Risiken für die IT–Sicherheit des Landes Kärnten führen. Zudem verwies der RH auf die in der NIS–2–Richtlinie festgelegte Verpflichtung zu umfassenden Risikomanage-

[24] Termintreue, Lieferservice, Reklamation und Fehlerbehandlung, Kompetenz der Ansprechpartner, Produktqualität, Einhaltung von vereinbarten Serviceleistungen

mentmaßnahmen, die auch das Sicherheitsniveau der externen Dienstleister in der Lieferkette umfassten (TZ 4). Der RH kritisierte auch, dass eine Regelung zur Risikominimierung bei (Fern–)Zugriffen von externen Dienstleistern auf die IT–Systeme des Landes Kärnten noch nicht erlassen war.

Er empfahl dem Land Kärnten, auch im Hinblick auf die bevorstehende Umsetzung der NIS–2–Richtlinie das Informationssicherheitsniveau der externen Dienstleister in eine Risikobeurteilung einfließen zu lassen, adäquate Maßnahmen zu treffen und die Regelung zur Beaufsichtigung und Überwachung von externen Dienstleistern so bald als möglich in Kraft zu setzen.

Der RH kritisierte, dass die Datenschutzinformation aus 2018 an neu eintretende Bedienstete veraltete Informationen zu den Kontaktdaten der bzw. des Datenschutzbeauftragten beinhaltete.

Er empfahl dem Land Kärnten, die Datenschutzinformation aus dem Jahr 2018 an neu eintretende Bedienstete zu aktualisieren.

11.3 Das Land Kärnten teilte in seiner Stellungnahme mit, dass der Empfehlung des RH zum Informationssicherheitsniveau der externen Dienstleister Folge geleistet werde. Der Detaillierungsgrad der Prüfung und Evaluierung der Dienstleister sei noch zu definieren.

Die Datenschutzinformation für neu eintretende Landesbedienstete werde aufgrund der Anregung des RH aktualisiert.

Ausstattung der IT–Arbeitsplätze für Telearbeit

12.1 (1) Die Möglichkeit für Bedienstete des Landes Kärnten, Telearbeit zu verrichten, war im Kärntner Dienstrechtsgesetz 1994 bzw. im Kärntner Landesvertragsbedienstetengesetz 1994 gesetzlich verankert. Die gesetzlichen Bestimmungen legten die Voraussetzungen zur Eignung des Bediensteten, des Arbeitsplatzes und der zu erfüllenden Aufgaben fest. Bei Vorliegen dieser Voraussetzungen konnte Beamtinnen und Beamten Telearbeit genehmigt bzw. konnte Telearbeit mit Vertragsbediensteten vereinbart werden (Telearbeitsanordnung bzw. Telearbeitsvereinbarung).

Bedienstete ohne Telearbeitsanordnung bzw. –vereinbarung konnten anlassbezogene Telearbeit in Anspruch nehmen. Diese war als stunden– oder tageweise Abwesenheit zu beantragen.

(2) Das Land Kärnten sah eine dienstliche mobile IT–Ausstattung für Bedienstete mit Telearbeitsanordnung bzw. –vereinbarung nicht standardmäßig vor. Sofern eine

dienstliche Notwendigkeit gegeben war, erhielten Bedienstete auf Antrag eine dienstliche mobile IT–Ausstattung bzw. ein Mobiltelefon. Die Entscheidung darüber hatte die Abteilungs– bzw. Behördenleitung zu treffen.

Bedienstete ohne dienstliche mobile IT–Ausstattung konnten für die Telearbeit eine private IT–Ausstattung nutzen. Die privaten Endgeräte waren über eine Benutzerschnittstelle mit der IT–Infrastruktur des Landes Kärnten verbunden (Thin–Client), dadurch liefen die Anwendungen nicht lokal am Endgerät, sondern am zentralen Applikationsserver. Bei der Verwendung einer privaten IT–Ausstattung für dienstliche Zwecke ergaben sich bestimmte IT–Sicherheitsrisiken, beispielsweise geringere IT–Sicherheitsvorkehrungen gegenüber Schadsoftware; dazu verwies der RH auf seine Berichte „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31, TZ 17) und „Dienstrechtliche und technische Umsetzung von Telearbeit in ausgewählten Bundesministerien“ (Reihe Bund 2022/27, TZ 10 und 21). Der RH hatte in diesen Berichten festgestellt, dass der Einsatz privater IT–Ausstattung für Telearbeit nicht standardmäßig vorgesehen sein sollte.

(3) Die folgende Tabelle zeigt für die Monate April 2022 (vor dem Cyber–Angriff) und September 2023 (nach dem Cyber–Angriff) die Inanspruchnahme von Telearbeit sowie die Ausstattung mit dienstlichen, für Telearbeit geeigneten IT–Arbeitsplätzen bzw. Thin–Client–Berechtigungen im Land Kärnten:

Tabelle 4: Telearbeit beim Land Kärnten – Ausstattung und Inanspruchnahme

	22. April 2022 (vor dem Cyber–Angriff)	30. September 2023 (nach dem Cyber–Angriff)
	Anzahl	
Summe der Bediensteten	3.732	3.776
davon		
mit Telearbeitsanordnung bzw. –vereinbarung	*138*	*70*
mit dienstlicher, auch für Telearbeit geeigneter IT–Ausstattung[1]	*863[2]*	*913[3]*
mit Thin–Client–Berechtigung	*k.A.*	*1.478[4]*
Bedienstete mit Telearbeitsanordnung bzw. –vereinbarung, die in diesem Monat Telearbeit in Anspruch nahmen	138	70
in diesem Monat tatsächlich geleistete Telearbeitstage mit Telearbeitsanordnung bzw. –vereinbarung	2.628	1.911
Bedienstete, die in diesem Monat anlassbezogene Telearbeit in Anspruch nahmen	649	575
in diesem Monat tatsächlich geleistete anlassbezogene Telearbeitstage	1.959	1.788

k.A. = keine Angabe Quelle: Land Kärnten

[1] verstanden als generell für die Dienstleistung außerhalb der Dienststelle geeignete IT–Ausstattung, z.B. auch für Dienstverrichtung im Außendienst
[2] 22. März 2022
[3] 4. September 2022
[4] 17. Oktober 2023

70 Bedienstete des Landes Kärnten verfügten mit Stichtag 30. September 2023 über eine Telearbeitsanordnung bzw. –vereinbarung; der Anteil der aufrechten Telearbeitsanordnungen bzw. –vereinbarungen war damit seit 30. April 2022 um knapp 50 % gesunken. Das Land Kärnten begründete diesen Rückgang mit der zunächst auf ein Jahr befristeten und seit 1. Juli 2022 dauerhaft verlängerten Möglichkeit, die flexiblere anlassbezogene Telearbeit in Anspruch zu nehmen. Im Vergleich zu April 2022 verrichtete im September 2023 auch ein geringerer Anteil an Bediensteten anlassbezogene Telearbeit.

Mit Stichtag 22. März 2022 bzw. 4. September 2023 stand 863 bzw. 913 Bediensteten eine mobile IT–Ausstattung für dienstliche Zwecke (neben Telearbeit z.B. auch für die Dienstverrichtung im Außendienst) zur Verfügung. Dazu, wie vielen davon eine mobile IT–Ausstattung für die Verrichtung von Telearbeit zugeteilt war, konnte die IT–Abteilung des Landes Kärnten für die jeweiligen Stichtage keine Angaben machen.

(4) Das Land Kärnten setzte eine einheitliche Softwarelösung für Videokonferenzsysteme ein, deren Nutzung die Bediensteten zu beantragen hatten. Das Österreichische Informationssicherheitshandbuch nannte als Sicherheitsanforderungen für Videokonferenzsysteme neben technischen und datenschutzrechtlichen Aspekten auch das Erstellen und Bereitstellen von Informationen zur sicheren Verwendung der Videokonferenzsysteme.[25] Im Land Kärnten gab es keine spezifischen Sicherheitsrichtlinien für die eingesetzte Videokonferenzlösung. Eine Anleitung zur Nutzung der Videokonferenzlösung stand den Bediensteten im Intranet des Landes zur Verfügung; diese war zur Zeit der Gebarungsüberprüfung nicht aktuell.

12.2 Wie schon in seinen Berichten „Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien“ und „Dienstrechtliche und technische Umsetzung von Telearbeit in ausgewählten Bundesministerien“ stellte der RH kritisch fest, dass Bedienstete, die über keine dienstliche mobile IT–Ausstattung verfügten, bei der Telearbeit eine private IT–Ausstattung für dienstliche Zwecke nutzen konnten. Mit der Verwendung privater IT–Ausstattung waren bestimmte IT–Sicherheitsrisiken verbunden. Der Einsatz privater IT–Ausstattung sollte daher für Telearbeit nicht standardmäßig vorgesehen sein.

Der RH empfahl dem Land Kärnten, bei einer zukünftig erforderlichen Neuausstattung der IT–Arbeitsplätze Bedienstete mit regelmäßiger Telearbeit mit mobilen Endgeräten auszustatten.

[25] Version 4.4.0 Kapitel 6.3.5

Der RH hielt fest, dass das Land Kärnten über eine einheitliche Videokonferenzlösung verfügte; er kritisierte jedoch, dass es keine spezifischen Sicherheitsrichtlinien dazu gab. Weiters stellte er kritisch fest, dass die Anleitung zur Nutzung der Videokonferenzlösung zur Zeit der Gebarungsüberprüfung nicht aktuell war.

Der RH empfahl dem Land Kärnten, Sicherheitsrichtlinien zur Nutzung der Videokonferenzlösung zu erstellen und in Kraft zu setzen. Die Anleitung zur Nutzung der Videokonferenzlösung wäre zu aktualisieren und den Bediensteten zur Kenntnis zu bringen.

12.3 Das Land Kärnten nahm in seiner Stellungnahme die Empfehlung zur Ausstattung mit mobilen Endgeräten zur Kenntnis. Es wies darauf hin, dass sich zur Zeit der Stellungnahme eine Arbeitsgruppe mit der Ausstattung im Sinne einer Mobile–Device–Strategie des Landes Kärnten beschäftige.

Die Anleitung zur Nutzung der Videokonferenzlösungen werde aktualisiert. Die Kritik an fehlenden Sicherheitsrichtlinien könne nicht nachvollzogen werden, da das Land Kärnten auf eine Standardlösung zugreife, wie auch viele andere Länderorganisationen oder Bundesministerien.

12.4 Der RH verwies gegenüber dem Land Kärnten erneut auf das Österreichische Informationssicherheitshandbuch, das als Sicherheitsanforderungen für Videokonferenzsysteme neben technischen und datenschutzrechtlichen Aspekten auch das Erstellen und Bereitstellen von Informationen zur sicheren Verwendung von Videokonferenzsystemen nannte. Er blieb daher bei seiner Empfehlung.

Regelungen für Bedienstete zur Gewährleistung der IT–Sicherheit bei Telearbeit

13.1 (1) Das Österreichische Informationssicherheitshandbuch empfahl, zur Gewährleistung der IT–Sicherheit Regelungen für Telearbeit schriftlich festzuhalten, den Bediensteten zur Kenntnis zu bringen und regelmäßig zu aktualisieren.[26]

Die von der IT–Abteilung des Landes Kärnten erstellte „Sicherheitspolitik für mobile Endgeräte" enthielt Vorgaben für die Verwendung mobiler Endgeräte für den Dienstbetrieb. Sie umfasste u.a. konkrete Regelungen für den Transport und die Aufbewahrung der Arbeitsgeräte sowie den Umgang mit personenbezogenen Daten. Darüber hinaus legte sie fest, dass private mobile Endgeräte nicht direkt in das Landesnetz integriert werden konnten. Weitere Regelungen zur Nutzung einer privaten IT–Ausstattung waren veraltet; Regelungen zur Nutzung einer privaten IT–Ausstattung als Thin–Client gab es nicht.[27]

(2) Die „Sicherheitspolitik für mobile Endgeräte", die IT–Sicherheitsstrategie sowie die dienstlichen Vorgaben zur Verrichtung anlassbezogener Telearbeit übermittelte die Landesamtsdirektion per Erlass an die Abteilungen bzw. Dienststellen. Diese waren dafür verantwortlich, den Bediensteten die Regelungen auf geeignete Weise zur Kenntnis zu bringen. Zusätzlich wurden die Regelungen im Intranet des Landes Kärnten veröffentlicht.

13.2 Der RH hielt fest, dass das Land Kärnten Regelungen zur Gewährleistung der IT–Sicherheit bei Telearbeit erlassen hatte, die es den Bediensteten zur Kenntnis brachte und im Intranet veröffentlichte.

Ebenso wies er darauf hin, dass gemäß der „Sicherheitspolitik für mobile Endgeräte" private Endgeräte nicht in das Landesnetz integriert werden konnten. Er kritisierte jedoch, dass die „Sicherheitspolitik für mobile Endgeräte" keine Regelungen zur Nutzung einer privaten IT–Ausstattung für eine Verbindung als Thin–Client zur IT–Infrastruktur des Landes Kärnten enthielt. Der RH verwies dazu auf seine grundsätzliche Feststellung in TZ 12, dass der Einsatz privater IT–Ausstattung für Telearbeit nicht standardmäßig vorgesehen sein sollte.

Der RH empfahl daher dem Land Kärnten, konkrete Regelungen für die dienstliche Nutzung einer privaten IT–Ausstattung (z.B. Nutzung als Thin–Client) zu erlassen und den Bediensteten zur Kenntnis zu bringen.

[26] Version 4.4.0 Kapitel 6.3.4

[27] Auch die IT–Sicherheitsstrategie (TZ 5), die dienstlichen Vorgaben zur Verrichtung anlassbezogener Telearbeit sowie die bei regelmäßiger Telearbeit abzuschließenden Telearbeitsvereinbarungen enthielten einzelne Regelungen, um die IT–Sicherheit bei Telearbeit gewährleisten zu können.

13.3 Das Land Kärnten teilte in seiner Stellungnahme mit, dass sich die IT–Policy in Überarbeitung befinde und auch noch einmal die Nutzung der privaten IT–Ausstattung in Bezug auf Thin–Client–Zugriffe geprüft werde.

Technische Maßnahmen zur Erhöhung der IT–Sicherheit

Erhöhung der IT–Sicherheit der zentralen IT–Infrastruktur

14.1 (1) Ziel von technischen und organisatorischen Maßnahmen war es, die IT–Sicherheit der zentralen IT–Komponenten bzw. IT–Anwendungen zu erhöhen. Dabei sollten solche Maßnahmen gesetzt werden, die unter Berücksichtigung von Kosten–Nutzen–Erwägungen die Erreichung eines möglichst hohen Sicherheitsniveaus erwarten ließen.

Tabelle 5 zeigt ausgewählte Maßnahmen, um die IT–Sicherheitsrisiken in der zentralen IT–Infrastruktur zu reduzieren, und welche davon im Land Kärnten vor und nach dem Cyber–Angriff 2022 eingerichtet waren:

Tabelle 5: Maßnahmen zur Erhöhung der IT–Sicherheit der zentralen IT–Infrastruktur

Maßnahme	Stand April 2022 (vor dem Cyber–Angriff)	Stand Oktober 2023 (nach dem Cyber–Angriff)
Intrusion Detection Systeme (IDS) / Intrusion Prevention Systeme (IPS) zur Erkennung bzw. Verhinderung von Cyber–Angriffen	eingerichtet	neu eingerichtet
Firewall unterbindet unerwünschte Netzwerkverbindungen vom Internet in das lokale Netz des Landes und umgekehrt	eingerichtet	neu eingerichtet
Spamfilter zur Unterdrückung unerwünschter E–Mails	eingerichtet	neu eingerichtet
Schutz vor Schadsoftware (Viren, Trojaner, Ransomware, Spyware etc.) für die zentralen Systeme – z.B. Serversysteme	eingerichtet	eingerichtet
DDoS–Schutz gegen gebündelte Überlastungsangriffe auf zentrale Systeme	nicht eingerichtet	eingerichtet
Security Information and Event Management System (SIEM) zur strukturierten Analyse, Klassifikation und Protokollierung ungewöhnlichen Verhaltens im Netz	nicht eingerichtet	eingerichtet
Security Operations Center (SOC) zur laufenden Überwachung und Analyse aller sicherheitsrelevanten Systeme (Netzwerke, Server, Clients, Webservices etc.) auf Grundlage des SIEM	nicht eingerichtet	eingerichtet
Cyber Threat Intelligence zur Analyse der Motive, Ziele und des Verhaltens von Cyber–Angriffen	nicht eingerichtet	eingerichtet
Schwachstellenmanagementsystem/Patchmanagementsystem zur permanenten Erkennung, Bewertung, Priorisierung und Behebung von Sicherheitslücken von Software	eingerichtet	eingerichtet
Richtlinien zur sicheren Softwareentwicklung	lagen vor	lagen vor
Netzwerksegmentierung zur Einschränkung von Angriffen auf Teilbereiche des Netzwerks	eingerichtet	eingerichtet
Computer–Notfall–Team (CERT, CSIRT) zur Bewältigung konkreter IT–Sicherheitsprobleme (z.B. Bekanntwerden neuer Sicherheitslücken)	nicht eingerichtet	nicht eingerichtet (TZ 27)

Quelle: Land Kärnten; Zusammenstellung: RH

Das Land Kärnten setzte nach dem Cyber–Angriff mehrere Maßnahmen zur Erhöhung der zentralen IT–Sicherheit. Unter anderem verbesserte es die Firewall und den Spamfilter und richtete einen DDoS–Schutz, ein Cyber Threat Intelligence System, ein Security Information and Event Management System (**SIEM**) sowie ein Security Operations Center (**SOC**) ein.

(2) Das Österreichische Informationssicherheitshandbuch[28] beinhaltete zur Dokumentation von IT–Sicherheitsmaßnahmen weitreichende Vorgaben. Diese Dokumentation sollte beitragen

- zur Nachvollziehbarkeit der Systemkonfigurationen insbesondere bei Änderungen,
- zu einem geordneten Wiederanlauf des IT–Systems im Notfall und
- zur Weiterführung des IT–Betriebs in Vertretungsfällen.

Schriftliche Dokumentationen über Umsetzung und Ausgestaltung der Maßnahmen zur Erhöhung der IT–Sicherheit der zentralen IT–Infrastruktur lagen im Land Kärnten nur teilweise vor.

14.2 Der RH hielt fest, dass das Land Kärnten nach dem Cyber–Angriff im Jahr 2022 mehrere IT–Sicherheitsmaßnahmen (z.B. neue Firewall, DDoS–Schutz, Cyber Threat Intelligence System, SIEM, SOC) für zentrale IT–Komponenten einrichtete bzw. aktualisierte.

Er kritisierte, dass schriftliche Dokumentationen über Umsetzung und Ausgestaltung der Maßnahmen lediglich teilweise vorlagen; diese Dokumentation wäre wesentlich für die Nachvollziehbarkeit der Funktionsweise der IT–Systeme.

Der RH empfahl dem Land Kärnten, die schriftliche Dokumentation über Umsetzung und Ausgestaltung der IT–Sicherheitsmaßnahmen für die zentralen IT–Komponenten zu vervollständigen – auch im Hinblick auf die Anforderungen durch die NIS–2–Richtlinie. Eine umfassende Dokumentation sollte die Nachvollziehbarkeit der Funktionsweise der IT–Systeme gewährleisten.

14.3 Laut Stellungnahme des Landes Kärnten werde der Empfehlung des RH Folge geleistet, eine entsprechende Adaptierung und Ergänzung der IT–Sicherheitsmaßnahmen befänden sich in Ausarbeitung.

[28] Version 4.4.0 Kapitel 12.2

Erhöhung der IT–Sicherheit am IT–Arbeitsplatz

15.1 (1) IT–Sicherheitsrisiken bei IT–Arbeitsplätzen betrafen z.B. den Ausfall der zentralen IT–Infrastruktur, Schäden durch Elementarereignisse, Schadsoftware–Befall, Hackerangriffe oder Social–Engineering–Angriffe.

Bei der Telearbeit ergaben sich weitere spezifische Risiken, etwa der Verlust der mobilen IT–Ausstattung, der unbemerkte Zugang nicht berechtigter Personen zu den mobilen Arbeitsplatzrechnern, das Ausspähen von Zugangsdaten oder eine allfällige, infrastruktur–bedingt geringere IT–Sicherheit.

Ein Teil dieser Risiken konnte durch geeignete, dem Stand der Technik entsprechende, technische sowie organisatorische Maßnahmen reduziert werden.

Die Maßnahmen für IT–Sicherheit am IT–Arbeitsplatz und welche davon im Land Kärnten vor und nach dem Cyber–Angriff 2022 eingerichtet waren, sind der Tabelle 6 zu entnehmen:

Tabelle 6: Maßnahmen zur Erhöhung der IT–Sicherheit am IT–Arbeitsplatz

Maßnahme am IT–Arbeitsplatz	Stand April 2022 (vor dem Cyber–Angriff)	Stand Oktober 2023 (nach dem Cyber–Angriff)
Zwei–Faktor–Authentifizierung zum Identitätsnachweis einer bzw. eines Bediensteten mittels einer Kombination aus zwei unterschiedlichen, voneinander unabhängigen Komponenten[1]	nur in einem sehr geringen Ausmaß (Testbetrieb) eingerichtet	teilweise eingerichtet[2]
Verschlüsselung der Daten auf den Festplatten zur Reduktion des Risikos, die gespeicherten Daten missbräuchlich zu verwenden oder zu manipulieren	eingerichtet	eingerichtet
Unterbinden des Startvorgangs eines Arbeitsplatzrechners von einem externen Datenträger aus (z.B. Booten von USB–Stick) zur Reduktion des Risikos eines missbräuchlichen Zugangs auf diesem IT–Arbeitsplatz	eingerichtet	eingerichtet
USB–Port–Deaktivierung bzw. **–Kontrolle** zur Reduktion des Risikos, Schadsoftware zu laden	nicht eingerichtet	nicht eingerichtet
Applikations–Whitelisting zur Beschränkung auf erlaubte Anwendungen **Applikations–Blacklisting** zum Unterbinden verbotener Anwendungen	nicht eingerichtet	Applikations–Blacklisting eingerichtet
verschlüsselter Datenaustausch zwischen mobilem Arbeitsplatz und zentraler IT–Infrastruktur	eingerichtet	neu eingerichtet
Schutz vor Schadsoftware zum Schutz der IT–Arbeitsplätze vor Viren, Trojanern, Ransomware, Spyware	eingerichtet	neu eingerichtet
Endpoint–Protection–System zur Identifikation von Cyber–Bedrohungen direkt am Endgerät, zu ihrer Eindämmung und Eliminierung	eingerichtet	neu eingerichtet
Auto–VPN–Funktionalität automatisch generierte, verschlüsselte Verbindung vom Arbeitsplatzrechner zu den zentralen IT–Systemen des Landes inklusive Nutzung ihrer Sicherheitsmechanismen	im Testbetrieb	neu eingerichtet
(automatisierte) **Software–Updates** der Arbeitsplatzrechner	eingerichtet	eingerichtet

[1] z.B. Wissen (Passwort), Besitz, biometrische Eigenschaften
[2] ausgenommen Standrechner in den Dienststellen

Quelle: Land Kärnten

Das Land Kärnten setzte nach dem Cyber–Angriff mehrere Maßnahmen zur Erhöhung der IT–Sicherheit am IT–Arbeitsplatz. So verbesserte es u.a. die Endpoint–Protection und richtete ein Applikations–Blacklisting ein. Eine flächendeckende Zwei–Faktor–Authentifizierung sowie eine USB–Port–Deaktivierung bzw. –Kontrolle waren nicht eingerichtet.

(2) Wie für die IT–Sicherheit der zentralen IT–Infrastruktur (TZ 14) galten die Dokumentationsvorgaben des Österreichischen Informationssicherheitshandbuchs auch für die IT–Sicherheit des IT–Arbeitsplatzes. Deren Einhaltung soll auch hier zur Nach-

vollziehbarkeit der Systemkonfigurationen, zum geordneten Wiederanlauf des IT–Systems im Notfall und zur Weiterführung des IT–Betriebs in Vertretungsfällen beitragen.

Schriftliche Dokumentationen über Umsetzung und Ausgestaltung der Maßnahmen zur Erhöhung der IT–Sicherheit am IT–Arbeitsplatz lagen im Land Kärnten nur teilweise vor.

15.2 Der RH hielt fest, dass das Land Kärnten nach dem Cyber–Angriff im Jahr 2022 mehrere IT–Sicherheitsmaßnahmen für IT–Arbeitsplätze einrichtete, z.B. eine verbesserte Endpoint–Protection oder ein Applikations–Blacklisting.

Er kritisierte, dass schriftliche Dokumentationen über Umsetzung und Ausgestaltung der IT–Sicherheitsmaßnahmen lediglich teilweise vorlagen; diese Dokumentation wäre wesentlich für die Nachvollziehbarkeit der Funktionsweise der IT–Systeme.

Der RH empfahl dem Land Kärnten, die schriftliche Dokumentation über Umsetzung und Ausgestaltung der IT–Sicherheitsmaßnahmen für die Arbeitsplatzrechner zu vervollständigen – auch im Hinblick auf die Anforderungen durch die NIS–2–Richtlinie. Eine umfassende Dokumentation sollte die Nachvollziehbarkeit der Funktionsweise der IT–Systeme gewährleisten.

Der RH kritisierte, dass das Land Kärnten eine dem Stand der Technik entsprechende Zwei–Faktor–Authentifizierung nicht für alle IT–Arbeitsplätze einsetzte.

Er empfahl dem Land Kärnten, eine Zwei–Faktor–Authentifizierung für alle IT–Arbeitsplätze einzuführen.

Der RH kritisierte weiters, dass weder eine USB–Port–Deaktivierung noch eine USB–Port–Kontrolle eingerichtet war. Aus Sicht des RH bestand trotz Überwachung der USB–Port–Aktivitäten durch das System der Endpoint–Protection ein Restrisiko.

Er empfahl dem Land Kärnten, zu evaluieren, ob eine USB–Port–Deaktivierung oder USB–Port–Kontrolle zu einer Erhöhung der IT–Sicherheit führt, und diese gegebenenfalls einzurichten.

15.3 Laut Stellungnahme des Landes Kärnten werde der Empfehlung zur schriftlichen Dokumentation über Umsetzung und Ausgestaltung der IT–Sicherheitsmaßnahmen Folge geleistet; eine entsprechende Adaptierung und Ergänzung der IT–Sicherheitsmaßnahmen befänden sich in Ausarbeitung.

Die flächendeckende Zwei–Faktor–Authentifizierung sei in Vorbereitung, der Abschluss des Rollouts sei mit Sommer 2024 in Aussicht genommen.

Das Thema USB–Port–Deaktivierung oder USB–Port–Kontrolle sei bereits im Dezember 2022 einer Bewertung unterzogen worden. Bei dieser habe sich gezeigt, dass eine Deaktivierung der USB–Ports zu einer erheblichen Betriebseinschränkung in vielen Fachbereichen führen würde. Zudem würde als Sicherheitsmaßnahme jede Aktivität über das USB–Port auf Bedrohungen gescannt und das Thema USB–Port–Nutzung in die Awareness–Schulung der Mitarbeiter aufgenommen.

15.4 Der RH bewertete positiv, dass das Land Kärnten zur USB–Port–Sicherheit bereits Maßnahmen gesetzt hatte. Er hielt allerdings fest, dass aktivierte USB–Ports trotzdem noch Angriffsflächen bieten können. Er erachtete es daher für zweckmäßig, USB–Ports nur im unbedingt erforderlichen Ausmaß freizuschalten, um so die Risiken weiter zu reduzieren.

IT–Sicherheitsüberprüfungen

16.1 (1) Der RH orientierte sich beim Thema IT–Sicherheitsüberprüfungen am Österreichischen Informationssicherheitshandbuch, an der ISO/IEC–Norm 27001 sowie am vom deutschen Bundesamt für Sicherheit in der Informationstechnik entwickelten IT–Grundschutzkatalog.

Ziel von IT–Sicherheitsüberprüfungen (IT–Sicherheits–Audits) war es demnach, die Wirksamkeit der technischen und organisatorischen IT–Sicherheitsmaßnahmen zu überprüfen. Diese Überprüfungen sollten auf einer umfangreichen Risikoanalyse beruhen und konnten – bei vorhandener Expertise – durch die jeweilige Organisation selbst oder von externen Spezialistinnen bzw. Spezialisten, zum Teil automatisiert[29], durchgeführt werden.

(2) Im Zeitraum 2020 bis 2023 führte das Land Kärnten fünf externe sowie acht interne – damit in Summe 13 – IT–Sicherheitsüberprüfungen durch:

- Das Land Kärnten war seit 2006 nach der ISO/IEC–Norm 27001 (Informationssicherheitsmanagement) zertifiziert (TZ 3). Die Zertifizierung umfasste die Bereiche Konzeption, Einkauf, Errichtung, Betriebsführung und Wartung der IT–Infrastruktur sowie Management, Beratung und Realisierung von IT–Projekten. Im Zeitraum 2020 bis 2023 fanden vier externe Überprüfungen nach der ISO/IEC–Norm statt. Das Land Kärnten wechselte im überprüften Zeitraum die Auditoren nicht.
- Im Jahr 2023 wurde die externe Sicherheits–Architektur überprüft. Die Ergebnisse daraus flossen in den Maßnahmenkatalog ein (TZ 23).
- Die jährlichen internen Überprüfungen betrafen die zentrale Benutzerverwaltung sowie das Server–Betriebssystem.

[29] z.B. automatisierte Penetration–Tests, Port–Scans, Schwachstellen–Scans

Im Rahmen der IT–Betriebsführung nahm das Land Kärnten auch laufende Monitoring–Aufgaben wahr und analysierte Log–Files. Weitere Arten von IT–Sicherheitsüberprüfungen, die im Sinne eines Best–Practice–Ansatzes dem Stand der Technik entsprachen, fanden in den Jahren 2020 bis 2023 nicht statt.

16.2 Der RH betonte, dass IT–Sicherheitsüberprüfungen sämtliche IT–sicherheitsspezifischen Risiken abdecken und regelmäßig durchgeführt werden sollten, um auch aktuelle Bedrohungen im innovativen Bereich der IT–Sicherheit zeitnah berücksichtigen zu können.

Der RH kritisierte,

- dass das Land Kärnten in den Jahren 2020 bis 2023 lediglich 13 IT–Sicherheitsüberprüfungen durchführte,
- dass diese nicht alle wesentlichen Bereiche abdeckten und nicht alle wesentlichen Risiken erfassten und
- dass das Land Kärnten im überprüften Zeitraum die externen Auditoren nicht wechselte. Nach Ansicht des RH fördert ein Wechsel die Unabhängigkeit der Prüfung und bringt neue Sichtweisen ein.

Der RH empfahl dem Land Kärnten, auf Basis einer umfassenden Risikoanalyse und der verfügbaren Ressourcen sowohl interne als auch externe IT–Sicherheitsüberprüfungen verstärkt und regelmäßig durchzuführen. Bei externen IT–Sicherheitsüberprüfungen wären die Auditoren regelmäßig zu wechseln, um die Unabhängigkeit der Prüfung zu gewährleisten und neue Sichtweisen einbringen zu können.

16.3 Das Land Kärnten teilte in seiner Stellungnahme mit, dass für Juli 2024 ausführliche externe Risikoanalysen durch externe Dienstleister anberaumt seien. Es sei geplant, solche Tests zyklisch durchzuführen und dabei alternierend verschiedene Dienstleister zu beauftragen.

Notfallkonzepte, Notfallszenarien, Notfallorganisation

17.1 (1) Der RH orientierte sich bei der Überprüfung des Notfallmanagements am Österreichischen Informationssicherheitshandbuch bzw. dem IT–Grundschutzkatalog des deutschen Bundesamts für Sicherheit in der Informationstechnik. Das Notfallmanagement soll demnach die Funktionsfähigkeit einer Behörde selbst in kritischen Situationen mit geeigneten Maßnahmen sichern.

(2) Das Land Kärnten führte eine Risikobewertung seiner Informationssysteme durch und definierte die für die Gewährleistung des Betriebs und der IT–Sicherheit wichtigen IT–Systeme.

Die nachfolgende Tabelle gibt einen Überblick über die Notfallkonzepte, –szenarien und –organisation sowie die kritischen Systeme und Notfallprozesse des Landes Kärnten:

Tabelle 7: Notfallkonzepte, Notfallszenarien und Notfallorganisation

Notfall–Element	Stand vor und nach dem Cyber–Angriff
Notfallhandbuch bzw. –konzept	nicht vorhanden
IT–Notfallszenarien bzw. IT–Notfallpläne	vorhanden
Definition der Kriterien, wann ein Ereignis als IT–Notfall gilt	teilweise vorhanden auf Ebene einzelner Szenarien
Definition einer IT–Notfallorganisation	vorhanden
Festlegung wichtiger IT–Systeme	durchgeführt
Definition der IT–Notfallprozesse	vorhanden
Sicherungs– und Wiederherstellungsverfahren	vorhanden
Testung Notfallszenarien	regelmäßig
Überprüfungen	Teil der Zertifizierung nach der ISO/IEC–Norm–27001

Quelle: Land Kärnten

Das Land Kärnten verfügte im überprüften Zeitraum über kein umfassendes IT–Notfallhandbuch bzw. –konzept. Im Zuge der Aufarbeitung der Folgen des Cyber–Angriffs analysierte ein externes Beratungsunternehmen im Jänner 2023 die IT–Sicherheit für das Land Kärnten. Das Beratungsunternehmen empfahl, ein IT–Notfallhandbuch zu erstellen mit einem Handlungsleitfaden für kritische Situationen, mit Lösungsansätzen sowie Verantwortlichkeiten.

(3) Bereits vor dem Cyber–Angriff verfügte das Land Kärnten über Dokumente, Vorgaben und Richtlinien zum IT–Notfallmanagement.

Der zur Zeit der Gebarungsüberprüfung aktuelle Sicherheits– und Notfallplan für das Hauptrechenzentrum stammte vom Juli 2019, das Sicherungs– und Wiederherstellungskonzept (Dokument zum Thema „Desaster Recovery“, d.h. zur Wiederherstellung von Systemen aus Backup–Sicherungen) vom März 2014. Die Kontaktdaten im Dokument über IT–Notfallnummern und Zutrittsregelungen der Landesamtsdirektion vom Februar 2023 waren veraltet.

(4) Für den Notfallbetrieb war ein – seit 2015 an einem eigenen Standort betriebenes – Notfallrechenzentrum eingerichtet, das bei Ausfall des Hauptrechenzentrums eine Basisinfrastruktur bereitstellen konnte. Die Überprüfung der Funktionalität aller Systeme des Notfallrechenzentrums fand laufend durch den aktiven Betrieb und durch ein Monitoring–System statt. Zu der jährlich durchzuführenden Überar-

beitung der Risikoanalyse und der Anforderungen an das Notfallrechenzentrum konnte die IT–Abteilung keine Aufzeichnungen vorlegen.

17.2 Der RH kritisierte, dass – trotz des schwerwiegenden Cyber–Angriffs im Jahr 2022 und der darauffolgenden Empfehlung eines externen Beratungsunternehmens – ein umfassendes IT–Notfallhandbuch (inklusive überarbeiteter Anforderungen an das Notfallrechenzentrum) Ende 2023 nicht vorlag. Weiters stellte er kritisch fest, dass maßgebende Dokumente, wie der Sicherheits– und Notfallplan für das Rechenzentrum (aus 2019) und das Sicherungs– und Wiederherstellungskonzept (aus 2014), sowie die IT–Notfallnummern und Zutrittsregelungen nicht aktuell waren. Dies widersprach den Vorgaben an eine regelmäßige Qualitätssicherung.

Der RH wies darauf hin, dass Notfälle und Krisen jederzeit eintreten können und daher die Dokumentationen bzw. Vorgaben zu ihrer Bewältigung vorhanden sein und auf einem aktuellen Stand gehalten werden sollten.

Er empfahl dem Land Kärnten, ein umfassendes IT–Notfallhandbuch (inklusive überarbeiteter Anforderungen an das Notfallrechenzentrum) zu erstellen; dieses sollte alle jene Prozesse abbilden, die den Betrieb auch in Ausnahmesituationen aufrecht halten können. Dabei sollten insbesondere die Notfallvorsorge und –bewältigung sowie Tests und Übungen berücksichtigt werden.

Weiters empfahl er dem Land Kärnten, den Sicherheits– und Notfallplan für das Rechenzentrum aus 2019, das Sicherungs– und Wiederherstellungskonzept aus 2014 sowie die Regelung für IT–Notfallnummern und Zutritt einer Qualitätsüberprüfung zu unterziehen und zu aktualisieren. Im Sicherheits– und Notfallplan für das Rechenzentrum wären die aktuellen Risikoanalysen und die Erfassung der Anforderungen an das Notfallrechenzentrum besonders zu beachten.

17.3 Laut Stellungnahme des Landes Kärnten werde ein IT–Notfallhandbuch erstellt.

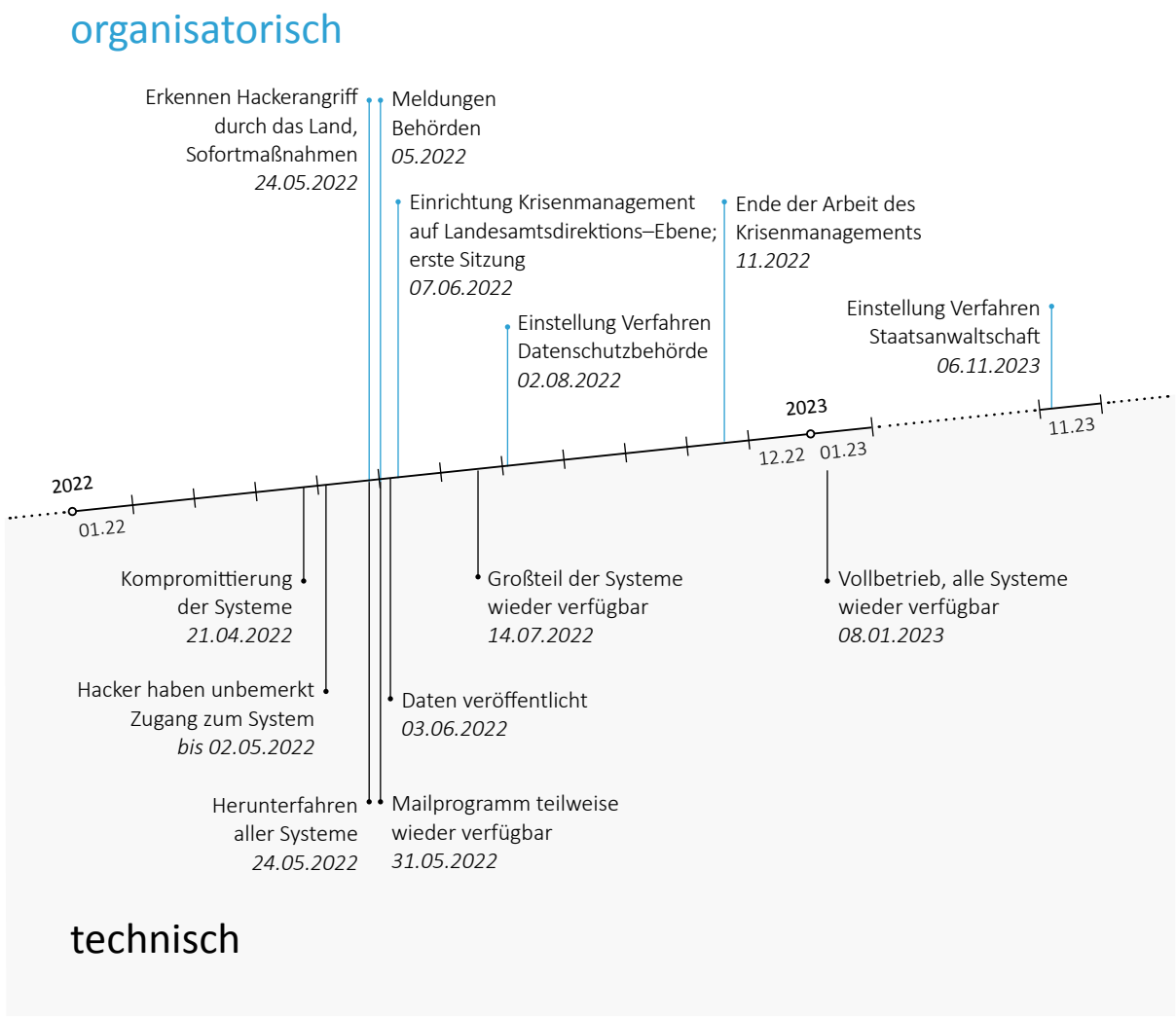
Der Sicherheits– und Notfallplan sowie das Sicherungs– und Wiederherstellungskonzept würden unter dem Gesichtspunkt des in Bau befindlichen Parallelrechenzentrums angepasst. Die Zutrittsregeln seien bereits aktualisiert und mit dem Audit nach der ISO/IEC–Norm 27001 im März 2024 überprüft worden.

Cyber–Angriff im Jahr 2022 auf das Land Kärnten

Überblick

18 Das Land Kärnten war im Jahr 2022 einem Cyber–Angriff mit Datendiebstahl und Erpressung ausgesetzt. Der Cyber–Angriff betraf den Zeitraum April 2022 bis Jänner 2023 (siehe Abbildung 5). Eine detaillierte Chronologie auf Grundlage der Dokumentation des Landes Kärnten ist im Anhang dargestellt.

Abbildung 5: Organisatorische und technische Ereignisse im Rahmen des Cyber–Angriffs



Quelle: Land Kärnten; Darstellung: RH

Ablauf des Cyber–Angriffs

19 (1) Die initiale Kompromittierung der Systeme durch den Cyber–Angriff erfolgte am 21. April 2022. Gemäß einer forensischen Analyse eines externen Dienstleisters wurde der Cyber–Angriff über einen Arbeitsplatzrechner durchgeführt. Nach Erlangen von privilegierten Benutzerberechtigungen konnten sich die Angreifer im Netzwerk weiterverbreiten und sich Zugriffe u.a. auf Datenspeicher im Netzwerk (File–Server) sowie weitere Server verschaffen. Im Zeitraum 21. April 2022 bis 2. Mai 2022 hatten die Angreifer unbemerkt teilweisen Zugang zu zahlreichen IT–Systemen.

(2) Das Land Kärnten erkannte den Ransomware–Angriff[30] am 24. Mai 2022 aufgrund von Anomalien im Netzwerk, Anmeldeproblemen von Nutzerinnen und Nutzern und auch teilweise aufgrund bereits erfolgter Verschlüsselungen von Arbeitsplatzrechnern und Server–Systemen. Die Angreifer hinterließen einen Hinweis auf eine Erpressernachricht im Darknet[31], die eine Lösegeldforderung von 5 Mio. EUR in Bitcoins beinhaltete.

(3) Am 3. Juni 2022 wurden auf einer öffentlich zugänglichen File–Sharing–Plattform Daten des Landes Kärnten im Umfang von 5,6 Gigabyte (**GB**) online gestellt, worauf das Innenministerium eine unmittelbare Löschung dieser Daten veranlasste.[32] Am 17. Juni 2022 wurden Daten des Landes Kärnten auf einer Darknet–Seite veröffentlicht. Im Juni 2022 konnten Überlastungsangriffe[33] der Angreifer abgewehrt werden. Laut der forensischen Analyse waren die Extraktion von Daten aus dem File–System des Landes Kärnten und damit ein Datendiebstahl nachvollziehbar. Am 2. Juli 2022 veröffentlichten die Angreifer eine Meldung im Darknet, dass die gestohlenen personenbezogenen Daten an einen unbekannten Dritten verkauft worden seien; dazu lagen dem RH keine weiteren Informationen vor.

(4) Der auf umfangreichen forensischen Untersuchungen basierende Abschlussbericht zum Cyber–Angriff an die Kärntner Landesregierung vom Juni 2022 hielt fest, dass es keine Anhaltspunkte für den Zugriff auf das elektronische Aktenverwaltungssystem des Landes (ELAK–System) oder auf autonome Datenbanken (insbesondere Gesundheitsdatenbanken, kaufmännisches System, Bundesapplikationen wie Zentrales Melderegister oder Zentrale Evidenz der Passbehörden) durch die Angreifer gegeben habe.

30 Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegelds (englisch „ransom“) wieder freigeben (vgl. Deutsches Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT–Sicherheit in Deutschland 2019, S. 78).

31 Das Darknet ist ein Teil des Internets, der nur über spezielle Browser zugänglich ist. Daten im Darknet werden anonym und verschlüsselt über verschiedene Server gesendet.

32 Die Sicherung des Pakets konnte aufgrund der kurzzeitigen Verfügbarkeit nicht vollständig durchgeführt werden, da die Direktion Staatsschutz und Nachrichtendienst (DSN) beim Innenministerium mittels internationalen Rechtshilfeersuchens die Löschung der Daten unmittelbar veranlasste.

33 „Distributed Reflective Denial of Service“–Angriffe; diese sollten vermutlich die Lösegeldforderung untermauern.

Datenabfluss aufgrund des Cyber–Angriffs

20.1 (1) Der Datenabfluss wurde von einem externen Dienstleister forensisch untersucht. Er betraf Daten der Landesverwaltung im Umfang von vermutlich ca. 250 GB und umfasste folgende Inhalte:

- Daten von ca. 80.000 Personen im Zusammenhang mit Niederlassungs– und Aufenthaltsbewilligungen für Fremde sowie Dokumentationen des unionsrechtlichen Aufenthaltsrechts,
- Akten von ca. 318 Personen über Verfahren zur Verleihung von Ehrenzeichen und Berufstiteln und rd. 4.000 Kontaktdaten für Einladungen zu Feierlichkeiten,
- personenbezogene Angaben im Schriftverkehr sowie Arbeitsunterlagen von Mitgliedern der Kärntner Landesregierung,
- persönliche Dateien von 37 Regierungsmitgliedern und Landesbediensteten,
- personenbezogene Daten betreffend Reisepässe von 97 Personen, Personalausweise von vier Personen und Führerscheine von zwei Personen (jeweils Regierungsmitglieder, Landesbedienstete und vereinzelt Dritte),
- personenbezogene Daten betreffend einzelne Bedienstete der Regierungssekretariate (aus Dienstgeberunterlagen).

(2) Der Datenabfluss erfolgte von Datenspeichern im Netzwerk. Für den Umgang mit Daten (Zugänglichkeit, Ablage, Speicherung und Übermittlung) galten im Land Kärnten der Erlass zur DSGVO, die Kanzleiordnung sowie eine Anleitung im Intranet zum Schutz sensibler Daten mittels Verschlüsselungstechniken. Das Land Kärnten verwies zudem auf die Amtsverschwiegenheit. Darüber hinaus waren keine allgemein gültigen Vorgaben zur Datenklassifizierung (etwa eine Datenklassifizierungs–Policy) in Kraft (TZ 3).

(3) Aufgrund des Datenabflusses von personenbezogenen Daten war der Cyber–Angriff im Sinne der DSGVO (Art. 4 Z 12) als Verletzung des Schutzes personenbezogener Daten zu werten. Die Datenschutzbehörde stellte letztlich das Verfahren ein, da das Land Kärnten seinen Verpflichtungen nach der DSGVO nachgekommen war, indem es die notwendigen Meldungen erstattete, die betroffenen Personen verständigte sowie organisatorische und technische Sicherheitsmaßnahmen zur Behebung der nachteiligen Auswirkungen bzw. auch zur zukünftigen Vorbeugung traf.

20.2 Der RH hielt fest, dass durch den Datenabfluss infolge des missbräuchlichen Zugriffs auf das IT–Netzwerk des Landes Kärnten die Angreifer in den Besitz von personenbezogenen Daten kamen. Er hielt weiters fest, dass das Land Kärnten seine daraus folgenden Verpflichtungen nach der DSGVO erfüllte.

Der RH wiederholte seine Kritik (TZ 3), dass es im Land Kärnten keine organisationsweiten, umfassenden und einheitlichen Vorgaben zur Behandlung klassifizierter Informationen gab. Diese Vorgaben sollten die Grundlage für die zu setzenden, adäquaten Maßnahmen zum Schutz der Daten sein. Der RH verwies dazu auf seine Empfehlung in TZ 3, diesbezügliche Vorgaben zu erlassen.

Der RH empfahl dem Land Kärnten, konkrete Regelungen für alle Bediensteten zum Umgang mit digitalen, sensiblen, personenbezogenen und nicht personenbezogenen Daten im Netzwerk zu treffen und begleitende technische Maßnahmen umzusetzen, z.B. Verschlüsselung, Passwortschutz von Dokumenten, Klassifizierung von elektronischen Dokumenten und Ablage in besonders geschützten Bereichen.

20.3 Das Land Kärnten verwies auf seine Stellungnahme zur Empfehlung in TZ 3.

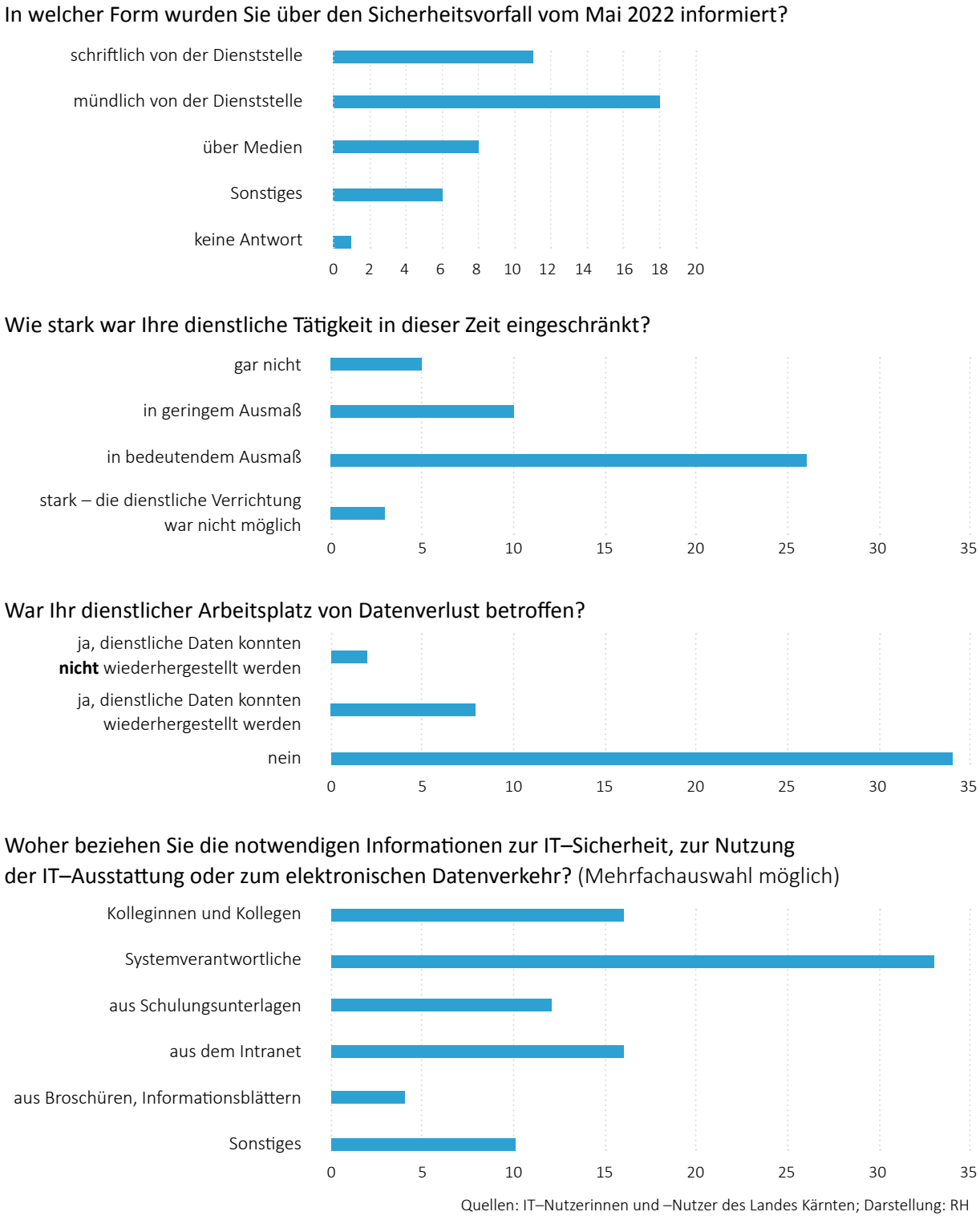
20.4 Der RH verwies auf seine Gegenäußerung in TZ 3.

Auswirkungen auf die Aufgabenerfüllung

21 (1) Der RH versendete an die IT–Nutzerinnen und –Nutzer in der Landesverwaltung Kärnten einen Fragebogen zu den Auswirkungen des Cyber–Angriffs auf ihre Aufgabenerfüllung. Der Fragebogen erging an 135 nach dem Zufallsprinzip ausgewählte Nutzerinnen und Nutzer, davon beantworteten 44 den Fragebogen vollständig.

Die nachfolgende Abbildung zeigt wesentliche Ergebnisse aus der Befragung:

Abbildung 6: Wesentliche Ergebnisse der Fragebogenerhebung zum Cyber–Angriff bei den IT–Nutzerinnen und –Nutzern



Quellen: IT–Nutzerinnen und –Nutzer des Landes Kärnten; Darstellung: RH

(2) Die dienstlichen Tätigkeiten der meisten Nutzerinnen und Nutzer waren aufgrund der Nicht–Verfügbarkeit zentraler IT–Systeme zumindest wesentlich eingeschränkt. So gaben 29 von 44 Nutzerinnen und Nutzern an, dass ihre dienstliche Tätigkeit in einem bedeutenden Maß oder stark eingeschränkt war. Im Durchschnitt (Median) lag eine zeitliche Einschränkung von rund vier Wochen vor, bei drei der 44 Nutzerinnen und Nutzer bestand die Einschränkung länger als ein halbes Jahr.

(3) Die Nutzerinnen und Nutzer wurden vorwiegend mündlich oder schriftlich von der Dienststelle über den Cyber–Angriff informiert, acht Personen erhielten die Information über die Medien. 38 Nutzerinnen und Nutzer gaben mit Stand November 2023 an, dass sie nunmehr darüber unterrichtet seien, wie sie sich bei verdächtigen Vorgängen an ihrem IT–Arbeitsplatz bzw. ihren elektronischen Daten verhalten sollen.

(4) Zehn Nutzerinnen und Nutzer waren laut ihren Angaben dienstlich vom Datenverlust betroffen – die verlorenen Daten konnten aber zum Großteil wiederhergestellt werden.

(5) Die Nutzerinnen und Nutzer teilten weiters mit, dass sie durch den Cyber–Angriff zusätzlich sensibilisiert worden seien und dass das Thema IT–Sicherheit an Stellenwert gewonnen habe. Zudem habe sich die Anzahl der Spam–Nachrichten reduziert. Negativ beurteilten sie, dass der Zugriff auf manche Internet–Seiten gesperrt wurde.

Krisenmanagement des Landes

22.1 (1) Das Land Kärnten verfügte zur Bewältigung von Krisen über einen im Jahr 2017 erstellten „Leitfaden Krisenmanagement“. Eine Aktualisierung durch den Landesamtsdirektor, u.a. mit den Erkenntnissen aus dem Cyber–Angriff, unterblieb. Der Leitfaden beinhaltete allgemein die Strukturen und Prozesse für die Bewältigung einer Krise, wobei die Krise nach bestimmten Merkmalen zu beurteilen war, etwa Gesundheitsgefährdung, umwelt– oder sicherheitsrelevantes Ereignis, potenzieller und erheblicher Imageschaden für das Land Kärnten, überregionale bzw. interne oder externe interdisziplinäre Auswirkungen. Bei ausgeprägter Realisierung eines Merkmals lag ein kritisches Ereignis vor.

(2) Die IT–Abteilung des Landes Kärnten übernahm ab Bekanntwerden des Cyber–Angriffs im Jahr 2022 das IT–Krisenmanagement. Sie handelte dabei in Abstimmung mit den beiden Unterabteilungen der Landesamtsdirektion für Präsidial– und Kommunikationsangelegenheiten, welche im Rahmen der Linienorganisation ebenfalls Aufgaben zur Bewältigung des Cyber–Angriffs wahrnahmen.

(3) Nach der Veröffentlichung von Daten des Landes Kärnten auf einer File–Sharing–Plattform (TZ 19) am 3. Juni 2022 richtete das Land Kärnten einen IT–Krisenstab im IT–Bereich und eine Cyber–Einsatz–Gruppe auf Ebene der Landesamtsdirektion ein:

Abbildung 7: Krisenorganisation des Landes Kärnten während des Cyber–Angriffs

Cyber–Einsatz–Gruppe

- Landesamtsdirektor und Stellvertreter
- IT–Abteilung
- Präsidium Zivilrecht
- Verfassungsdienst, Datenschutz
- Politik

IT–Krisenstab

- IT–Abteilungsleiter
- Informationssicherheitsmanager
- Koordinator für Aufgaben
- Krisen–Fall–Manager aus den IT–Fachbereichen

Quelle: Land Kärnten; Darstellung: RH

Die Aufgabenteilung zwischen den beiden Krisen–Einheiten sah vor, dass die Cyber–Einsatz–Gruppe die Abstimmung über Informationen an Behörden und Betroffene, die Kommunikation und die Priorisierung für den Wiederanlauf übernahm, datenschutzrelevante Themen mit den erforderlichen Meldungen ausarbeitete, Ermittlungsergebnisse der Behörden und die Bereitstellung weiterer Erkenntnisse an die Behörden besprach und festlegte. Weitere Aufgaben der Cyber–Einsatz–Gruppe betrafen die Öffentlichkeitsarbeit, die Information der Mitarbeiterinnen und Mitarbeiter und die Informationsweitergabe an den Landeshauptmann, die Regierungsmitglieder, die Amtsinspektion, die Landespolizeidirektorin, den Cyber–Spezialisten für die Medienarbeit sowie den Behördenvertreter vom Landesamt für Verfassungsschutz und Terrorismusbekämpfung (**LVT**).

Dem IT–Krisenstab oblagen die Planung und Umsetzung der technischen Maßnahmen (TZ 23).

(4) Die erste Sitzung der Cyber–Einsatz–Gruppe fand am 7. Juni 2022 – zwei Wochen nach Feststellung des Cyber–Angriffs am 24. Mai 2022 – statt. Insgesamt wurden bis Mitte November 2022 35 Sitzungen abgehalten. Die Inhalte und Ergebnisse wurden

in Sitzungsprotokollen zusammengefasst. Zum Zeitpunkt der letzten protokollierten Sitzung war die Umsetzung einiger technischen Maßnahmen noch offen, u.a. Zugänge für externe Projektpartner und VPN–Zugänge für Bedienstete.

(5) Seitens des Landes Kärnten ergingen Informationen und Meldungen an Ermittlungsbehörden (Kriminalpolizei, Staatsanwaltschaft sowie Direktion Staatsschutz und Nachrichtendienst (DSN) des Innenministeriums). Mit dem LVT stand das Land Kärnten auch während der Bewältigung des Cyber–Angriffs mehrmals im Informationsaustausch. Es erstattete eine Anzeige an die Datenschutzbehörde und eine Meldung an die NIS–Behörde beim Innenministerium.

Das Land Kärnten informierte den vom Datenabfluss betroffenen Personenkreis persönlich und in einer öffentlichen Bekanntmachung gemäß Art. 34 Abs. 3 lit. c DSGVO über den Cyber–Angriff.

22.2 Der RH hielt fest, dass das Land Kärnten den Cyber–Angriff am 24. Mai 2022 erkannte. Ab diesem Zeitpunkt hatte die unmittelbare flächendeckende Nicht–Verfügbarkeit der IT–Infrastruktur massive Auswirkungen auf die Landesverwaltung (TZ 21). Die Bewältigung des Cyber–Angriffs erfolgte in der ersten Phase durch die IT–Abteilung des Landes Kärnten in Abstimmung mit der Landesamtsdirektion im Rahmen der Linienorganisation. Der RH kritisierte, dass das Land Kärnten in dieser Phase noch keine Krisenorganisation eingerichtet hatte.

Der RH hielt kritisch fest, dass das Land Kärnten den „Leitfaden Krisenmanagement“ aus 2017 nicht mit den Erkenntnissen aus dem Cyber–Angriff aktualisiert hatte.

Er empfahl dem Land Kärnten, den „Leitfaden Krisenmanagement“ im Sinne einer Qualitätssicherung zu aktualisieren. Die Erkenntnisse aus der Bewältigung des Cyber–Angriffs wären dabei zu berücksichtigen und einzuarbeiten. Insbesondere wären Beurteilungskriterien für das Vorliegen einer „Cyber–Krise“ aufzunehmen.

22.3 Das Land Kärnten teilte in seiner Stellungnahme mit, dass die Überarbeitung des Leitfadens hinsichtlich der neu gewonnenen Erkenntnisse aus den aufgetretenen Krisen (insbesondere Cyber–Angriff im Jahr 2022) bereits begonnen habe.

Sofort– und Wiederherstellungsmaßnahmen

23.1 (1) Nach Bekanntwerden des Cyber–Angriffs am 24. Mai 2022 setzte das Land Kärnten umgehend technische Sofortmaßnahmen. Am selben Tag wurden alle IT–Systeme geordnet heruntergefahren sowie alle Netzwerkverbindungen getrennt. Von diesen Maßnahmen waren rd. 3.100 Arbeitsplätze und 180 Server–Systeme in der gesamten Landesverwaltung und in weiteren Dienststellen (z.B. Bezirkshauptmannschaften, Bildungsdirektion, Landesarchiv, Landtagsamt, Landesrechnungshof) betroffen.

Der Cyber–Angriff wurde unter Einbeziehung externer IT–Dienstleister untersucht, um weitere Sicherheitsrisiken zu identifizieren und Sofortmaßnahmen setzen zu können. Zu den Sofortmaßnahmen zählten:

- Einrichtung eines Rapid Response Teams (schnell verfügbare Einsatzgruppe),
- Aufbau einer neuen Firewall,
- Errichtung eines DDoS–Schutzes.

Das Rapid Response Team des externen IT–Dienstleisters nahm noch am 24. Mai 2022 seine Tätigkeit auf. Es analysierte den Cyber–Angriff und übernahm Aufgaben der System–Bereinigung und –Wiederherstellung in Zusammenarbeit mit der IT–Abteilung des Landes Kärnten.

(2) Zusätzlich zu diesen Sofortmaßnahmen setzte das Land weitere dringende IT–Maßnahmen um. Diese betrafen im Wesentlichen die Absicherung des Netzwerks, das laufende Monitoring der IT–Infrastruktur und die Sicherung der notwendigen IT–Dienste (z.B. Anwendungsbereitstellung für Wartung, Telearbeit, Schulnetz und Softwareverteilung) unter Einbeziehung externer Dienstleister. Ende 2022 beauftragte das Land Kärnten zudem eine Analyse aller wichtigen Bereiche der IT–Sicherheitsarchitektur. Ergebnis der Analyse waren Vorschläge für Maßnahmen zur Erhöhung der IT–Sicherheit (etwa Firewall, Endpoint–Protection), die in den Maßnahmenkatalog des Landes Kärnten einflossen. Im Oktober 2023 waren von 32 Maßnahmen 26 umgesetzt, sechs technische und organisatorische Maßnahmen befanden sich noch in Umsetzung.

(3) Im Rahmen der Wiederherstellungsmaßnahmen mussten sieben Arbeitsplatzrechner neu installiert werden. 113 Server–Systeme waren vom Ransomware–Angriff direkt betroffen und verschlüsselt. Für die Aufrechterhaltung des Dienstbetriebs wurden zwölf Umgehungslösungen (Workarounds) für bürgerrelevante Services implementiert. Das Datensicherungssystem (Backup) konnten die Angreifer nicht kompromittieren, weil es als eigenes Netzwerksegment abgeschottet war.

Die IT–Systeme wurden entsprechend ihrer Priorität und unter Berücksichtigung von Sicherheitsaspekten wieder in Betrieb genommen:

Tabelle 8: (Wieder–)Verfügbarkeit der IT–Systeme nach dem Cyber–Angriff

Datum	
24. Mai 2022	geordnetes Herunterfahren aller Systeme
29. Mai 2022	erste Wiederherstellungen erfolgreich
31. Mai 2022	Mail–System wieder verfügbar
14. Juli 2022	Großteil der Systeme wieder verfügbar
26. Juli 2022	Freigabe Internet
22. November 2022	Systeme wieder verfügbar (Ausnahme Nutzung von Thin–Clients)
8. Jänner 2023	Vollbetrieb

Quelle: Land Kärnten

23.2 Der RH hielt fest, dass die im April 2022 vorhandenen IT–Sicherheitsmaßnahmen des Landes Kärnten den Cyber–Angriff weder erkennen noch verhindern konnten. Die seither umgesetzten Maßnahmen (TZ 14, TZ 15) waren aus Sicht des RH geeignet, um künftig das Risiko eines Cyber–Angriffs deutlich zu reduzieren. Zur Zeit der Gebarungsüberprüfung waren jedoch noch nicht alle geplanten technischen und organisatorischen Maßnahmen zur Erhöhung der IT–Sicherheit umgesetzt.

Der RH empfahl dem Land Kärnten, die geplanten technischen und organisatorischen Maßnahmen zur Erhöhung der IT–Sicherheit zeitnah umzusetzen.

23.3 Laut Stellungnahme des Landes Kärntens werde dieser Empfehlung durch die jährlichen ISO–Zertifizierungen 27001 und 9001 sowie durch die Verpflichtung zur zeitnahen Umsetzung der NIS–2–Richtlinie implizit Folge geleistet.

Kosten der Maßnahmen im Zusammenhang mit dem Cyber–Angriff

24.1 (1) Die Kärntner Landesregierung genehmigte mittels Umlaufbeschluss am 31. Mai 2022 finanzielle Mittel für Sofortmaßnahmen:

- 305.000 EUR für die Beschaffung einer Firewall und
- 195.000 EUR für ein Rapid Response Service.

Die direkt zurechenbaren Kosten für die Aufarbeitung des Cyber–Angriffs betrugen zusätzlich rd. 515.000 EUR und umfassten vor allem Beraterleistungen zu Wiederherstellungsmaßnahmen.

Am 26. Juli 2022 erteilte die Kärntner Landesregierung die grundsätzliche Genehmigung (Grundsatzakt) für weitere 5,25 Mio. EUR für Sicherheitsmaßnahmen als Konsequenz des Cyber–Angriffs.

Die Kostenschätzungen dieser beiden Beschlüsse wurden in der jährlichen Budgetplanung (Voranschlag und Mittelfristprognose) berücksichtigt.

Die folgende Tabelle fasst die zusätzlich beschlossenen Mittel für IT–Sicherheitsmaßnahmen zusammen:

Tabelle 9: Zusätzliche finanzielle Mittel für IT–Sicherheitsmaßnahmen (Kostenschätzung vom 18. Juli 2022)

	2022	2023	2024	2025	Summe 2022 bis 2025
	in 1.000 EUR				
Rapid Response Service	195,00	–	–	–	195,00
Firewall	280,00	10,00	10,00	5,00	305,00
Sofortmaßnahmen Wartungsvertrag	228,00	228,00	228,00	228,00	912,00
Stunden Unterstützungspool	275,50	–	–	–	275,50
Cyber Defense Center	191,00	340,50	340,50	340,50	1.212,50
Maßnahmen aus Forensik–Bericht und Ergebnissen der geplanten Überprüfungen – Schätzung	250,00	150,00	100,00	50,00	550,00
SIEM / SOC – Schätzung	–	400,00	200,00	200,00	800,00
Security Management System (Modell und Lizenzen)	13,00	7,00	7,00	5,50	32,50
weitere Maßnahmen	637,50	297,50	297,50	237,50	1.470,00
Summe	**2.070,00**	**1.433,00**	**1.183,00**	**1.066,50**	**5.752,50**

SIEM = Security Information and Event Management
SOC = Security Operations Center

Quelle: Land Kärnten

Für das Jahr 2022 stellte das Land Kärnten mittels Umlaufbeschluss vom 31. Mai 2022 und dem Grundsatzakt vom 26. Juli 2022 zusätzliche Mittel für Sicherheitsmaßnahmen in Höhe von 2,07 Mio. EUR zur Verfügung. Für die Folgejahre waren zwischen 1,07 Mio. EUR und 1,43 Mio. EUR geplant, sodass mit Stand 18. Juli 2022 in Summe 5,75 Mio. EUR an zusätzlichen Mitteln für IT–Sicherheitsmaßnahmen des Landes Kärnten genehmigt waren.

Im Jahr 2022 konnten aufgrund von zeitlichen Verschiebungen und des Abschlusses mehrjähriger Verträge Einsparungen gegenüber der Planung erzielt werden. Eine Aktualisierung der in Tabelle 9 angeführten Kostenschätzung war nicht vorgesehen. Das Land Kärnten aktualisierte jedoch in seiner jährlichen Budgetplanung die voraussichtlichen Kosten der Maßnahmen, welche auch aktualisiert in die Mittelfristprognose 2024 bis 2027 einflossen.

Das Land Kärnten finanzierte die zusätzlichen Mittel für das Jahr 2022 aus einem Zweckzuschuss des Bundes für die Länder, der u.a. für Förderungen von Investitionen im Bereich digitaler Wandel geschaffen wurde. Der Zweckzuschuss war bundesweit mit 500 Mio. EUR dotiert, davon entfielen auf Kärnten 32,57 Mio. EUR. Von diesen 32,57 Mio. EUR verwendete das Land Kärnten 2,07 Mio. EUR für IT–Sicherheitsmaßnahmen. Die beschlossenen Mittel berücksichtigte das Land in der Mittelfristprognose für die Jahre 2023 bis 2025.

(2) Die IT–Abteilung des Landes Kärnten beschaffte im Dezember 2022 bei einem privaten IT–Dienstleister ein Security Management System inklusive Modell Servicierung um 15.000 EUR und schloss einen Beratervertrag zur „Konformitätsbewertung nach Cyber Risk Rating und Vorbereitung NIS“ mit einem Auftragsvolumen von 33.000 EUR ab.

Das Security–Management–System–Paket bestand aus der Software, einer Administrator– und drei Anwenderlizenzen sowie der Modellierung. Dieses Sicherheitssystem war zur Zeit der Gebarungsüberprüfung implementiert und einsatzbereit, aber nicht operativ in Verwendung. Laut Auskunft der IT–Abteilung hänge ein Einsatz des Produkts von den verfügbaren Lizenzen sowie von der Entscheidung der IT–Abteilungsleitung und des damals noch nicht besetzten Chief Information Security Officers (CISO) ab.

Das Land Kärnten bezahlte die Leistungen aus dem Beratervertrag in drei Tranchen: 9.900 EUR als Anzahlung mit der Auftragsvergabe, 13.200 EUR Ende April 2022 und weitere 9.900 EUR Anfang Juni 2023. Für die Zahlungen von April und Juni 2022 lagen Leistungsnachweise mit einer groben Darstellung des Leistungsumfangs vor. Eine Aufstellung der geleisteten bzw. noch offenen Stunden konnte das Land dem

RH nicht übermitteln. Laut Angaben des Landes Kärnten war mit Dezember 2023 das Stundenkontingent zur Unterstützung und Betreuung noch nicht zur Gänze abgerufen.

(3) Die Angreifer des Cyber–Angriffs kontaktierten das Land Kärnten nicht direkt. Die Lösegeldforderungen und in der Folge weitere Mitteilungen zu den illegal kopierten Daten wurden im Darknet veröffentlicht. Das Land Kärnten leistete keine Lösegeldzahlungen.

24.2 (1) Der RH hielt kritisch fest,

- dass das Land Kärnten die beschaffte Software „Security Management System“ nicht operativ einsetzte,
- dass Zahlungen zum Beratervertrag zur „Konformitätsbewertung nach Cyber Risk Rating und Vorbereitung NIS“ teilweise vor Leistungserbringung erfolgten und
- dass die Dokumentation der Leistungserbringung aus dem Beratervertrag mangelhaft war.

Er empfahl dem Land Kärnten, die Notwendigkeit und Eignung von IT–Softwarelösungen vor deren Beschaffung zu evaluieren. Zahlungen im Zusammenhang mit Beraterverträgen wären erst nach Leistungserbringung durchzuführen. Die Dokumentation der Leistungserbringung sollte genaue Angaben zu den geleisteten Stunden (Anzahl und Leistungszeitpunkt) enthalten.

(2) Der RH hob positiv hervor, dass das Land Kärnten keine Lösegeldzahlungen leistete, da diese einen Anreiz für potenzielle weitere Cyber–Angriffe bieten könnten.

24.3 Das Land Kärnten teilte in seiner Stellungnahme mit, dass in der Abteilung 1 – Landesamtsdirektion (siehe Abbildung 2 in TZ 7) grundsätzlich der vom RH empfohlenen Vorgangsweise entsprochen werde und dies auch in den Durchführungsbestimmungen zum Landesvoranschlag 2022 genau geregelt sei. Die Einführung der Software „Security Management System“ habe der damalige IT–Leiter veranlasst, es habe auch eine Evaluierung mehrerer Anbieter stattgefunden und die Abrechnung und Bezahlung seien gemäß den Durchführungsbestimmungen erfolgt. Da die Akzeptanz der Software bei den Mitarbeitern nicht gegeben gewesen sei, habe sich das Land Kärnten gegen eine weitere Verwendung entschieden.

24.4 Der RH entgegnete dem Land Kärnten, dass Zahlungen im Zusammenhang mit Beraterverträgen deshalb erst nach Leistungserbringung erfolgen sollten, da erst durch eine genaue Stundenabrechnung die Zahlungssumme bestimmt werden kann. An– und Vorauszahlungen sollten daher nur in einem Mindestmaß getätigt werden.

Zusammenarbeit mit anderen Akteuren

Koordinationsgremien im Bereich E–Government

25.1 (1) Im Rahmen des Cyber–Angriffs arbeitete das Land Kärnten mit den nationalen Gremien zusammen, indem es die vorgesehenen Meldungen erstattete und die Informationsweitergabe an die ermittelnden Behörden sicherstellte (TZ 22).

(2) Zur Zusammenarbeit bei der Weiterentwicklung des E–Governments und zur Koordination und Vernetzung im Bereich der Cyber–Sicherheit stand dem Land die Teilnahme in mehreren Gremien offen (siehe im Folgenden).

Wesentliche Änderungen in der Zusammenarbeit des Landes Kärnten mit anderen Akteuren aufgrund des Cyber–Angriffs konnte der RH nicht feststellen.

(a) Das Gremium Bund–Länder–Städte–Gemeinden (**BLSG**) diente der Zusammenarbeit der öffentlichen Verwaltung im Bereich E–Government. In diesem Rahmen fanden mehrmals jährlich Sitzungen

- der Kooperation BLSG,
- der Arbeitsgruppenleiter und
- der Verwaltungsarbeitsgruppe

statt. Vertreterinnen und Vertreter von Bund, Ländern, Städten und Gemeinden hatten die Möglichkeit, in diesen Gremien mitzuwirken und darüber hinaus in vier permanenten BLSG–Arbeitsgruppen[34] und individuell eingerichteten Projektgruppen u.a. gemeinsame Empfehlungen und Standards zu verschiedenen Themen zu erarbeiten.

Das Land Kärnten nahm im überprüften Zeitraum regelmäßig an den Sitzungen der Verwaltungsarbeitsgruppe teil. Es gab darüber hinaus an, dass ein Vertreter des Landes an fast allen Sitzungen der Kooperation BLSG und der Arbeitsgruppenleiter teilgenommen habe. Zur Zeit der Gebarungsüberprüfung war das Land Kärnten in keiner BLSG–Arbeitsgruppe vertreten.

(b) Aufgabe der Länderarbeitsgruppe (LAG) waren der Austausch zu länderspezifischen Angelegenheiten und Kooperationsmöglichkeiten zwischen den Ländern. Das Land Kärnten teilte mit, im überprüften Zeitraum an fast jeder Sitzung der Länderarbeitsgruppe teilgenommen zu haben; eine Dokumentation der Teilnahme konnte das Land Kärnten nicht in allen Fällen vorlegen.

[34] Infrastruktur/Interoperabilität (AG–II), Integration/Zugänge (AG–IZ), Recht/Sicherheit (AG–RS) und Präsentation/Standarddaten (AG–PS)

(c) Die im März 2023 veröffentlichte E–Government–Strategie Österreich 2023[35] wurde in Zusammenarbeit von Bund, Ländern, Städten und Gemeinden entwickelt. Das Land Kärnten arbeitete aktiv an der Strategie mit: Es übernahm eine leitende Rolle im Thema „Standards" und war in fünf weiteren Arbeitsgruppen vertreten.

25.2 Der RH anerkannte, dass das Land Kärnten im überprüften Zeitraum regelmäßig an den Sitzungen der Verwaltungsarbeitsgruppe des Gremiums BLSG teilnahm.

Er stellte kritisch fest, dass das Land Kärnten keine vollständige Dokumentation über seine Teilnahme an den Sitzungen der Kooperation BLSG, der Arbeitsgruppenleiter und der Länderarbeitsgruppe zur Verfügung stellte. Er hob die Relevanz dieser Sitzungen für den Austausch und die Zusammenarbeit zwischen Bund, Ländern, Städten und Gemeinden bzw. zwischen den Ländern hervor.

Der RH empfahl dem Land Kärnten, regelmäßig an den Sitzungen der Kooperation BLSG und der Arbeitsgruppenleiter sowie an den Sitzungen der Länderarbeitsgruppe teilzunehmen und sicherzustellen, dass relevante Informationen über die Sitzungen (Teilnahme, Unterlagen) innerhalb der Organisationseinheit zur Verfügung stehen.

Der RH wies kritisch darauf hin, dass das Land Kärnten zur Zeit der Gebarungsüberprüfung in keiner BLSG–Arbeitsgruppe vertreten war. Vor dem Hintergrund des Cyber–Angriffs 2022 erachtete er insbesondere eine Teilnahme des Landes Kärnten an der Arbeitsgruppe Recht/Sicherheit für den gegenseitigen Erfahrungsaustausch und den Erkenntnisgewinn als zweckmäßig.

Der RH empfahl dem Land Kärnten, die aktive Mitwirkung des Landes an den BLSG–Arbeitsgruppen – insbesondere an der Arbeitsgruppe Recht/Sicherheit – zu evaluieren.

Der RH anerkannte die aktive Mitwirkung des Landes Kärnten bei der Entwicklung der E–Government–Strategie Österreich 2023.

25.3 Das Land Kärnten gab in seiner Stellungnahme an, dass der IT–Leiter und sein Stellvertreter regelmäßig an den vom RH angeführten BLSG–Gremien teilnähmen. Eine protokollarische Austauschplattform existiere auf dem eGov–Referenceserver, der von der Stadt Wien gehostet werde. Alle Sitzungsprotokolle seien dort für Berechtigte verfügbar.

[35] https://www.digitalaustria.gv.at/dam/jcr:25902ce4-1087-4aa6-8b87-864770bfbc68/E-GovernmentStrategieOesterreich2023-bf.pdf (abgerufen am 19. August 2024)

25.4 Der RH hielt gegenüber dem Land Kärnten erneut fest, dass das Land Kärnten keine vollständige Dokumentation über seine Teilnahme an den Sitzungen der Kooperation BLSG, der Arbeitsgruppenleiter und der Länderarbeitsgruppe zur Verfügung stellte und zur Zeit der Gebarungsüberprüfung in keiner BLSG–Arbeitsgruppe vertreten war. Er betonte noch einmal die Relevanz dieser Sitzungen für den gegenseitigen Erfahrungsaustausch und die Zusammenarbeit zwischen Bund, Ländern, Städten und Gemeinden bzw. zwischen den Ländern und hielt seine Empfehlungen daher aufrecht.

Nationale Strukturen zur Koordination der Cyber–Sicherheit

26.1 (1) Der RH hatte in seinem Bericht „Koordination der Cyber–Sicherheit“ (Reihe Bund 2022/13, TZ 9 und TZ 10) die bestehenden nationalen Strukturen dargestellt. Auf strategischer Ebene waren auf Grundlage der Cybersicherheitsstrategie 2021 Gremien Cyber Sicherheit Steuerungsgruppe und Cyber Sicherheit Plattform eingerichtet:

(a) Die Cyber Sicherheit Steuerungsgruppe war für die strategische Koordination von Maßnahmen zur Cyber–Sicherheit zuständig und überwachte die Umsetzung der Cybersicherheitsstrategie 2021.[36] Die Geschäftsordnung der Cyber Sicherheit Steuerungsgruppe ermöglichte die Teilnahme von Landesvertreterinnen und –vertretern je nach zu behandelndem Thema. Im überprüften Zeitraum fanden vier Sitzungen der Cyber Sicherheit Steuerungsgruppe statt; zu diesen waren die Länder nicht eingeladen.

(b) Die Cyber Sicherheit Plattform sollte einen periodischen Informationsaustausch zwischen öffentlicher Verwaltung, Wirtschaft und Wissenschaft zu wesentlichen Fragen der Cyber–Sicherheit gewährleisten. Die Mitgliedschaft war nicht organisations– sondern personenbezogen. Bis Dezember 2023 waren keine Bediensteten des Landes Kärnten Mitglied in der Cyber Sicherheit Plattform.

[36] Die Cyber Sicherheit Steuerungsgruppe bestand aus Vertreterinnen und Vertretern des Innen–, Außen– und Justizministeriums, den Vorsitz führte das Bundeskanzleramt.

(2) Auf operativer Ebene bestanden die nationalen Koordinierungsstrukturen für Cyber–Sicherheit aus einem „inneren Kreis“ und einem „äußeren Kreis“ (§ 7 NISG)

- Der Innere Kreis der Operativen Koordinierungsstruktur (**IKDOK**) war als zentrales interministerielles Gremium der Cyber–Sicherheit für die Lagebilderstellung und –erörterung über Risiken, Vorfälle und Cyber–Angriffe sowie im Cyber–Krisenfall zuständig.
- Die Operative Koordinierungsstruktur (**OpKoord**) hatte zur Aufgabe, ein gesamtheitliches Lagebild zu erörtern, das auch freiwillige Meldungen enthielt.

In beiden Koordinierungsgremien waren die Länder grundsätzlich nicht als Teilnehmer vorgesehen.[37] Zur Information der Länder fand seit April 2023 monatlich ein Länderbriefing durch den IKDOK in Form von Videokonferenzen statt; bis November 2023 nahm das Land Kärnten an fünf der acht bis dahin abgehaltenen Videokonferenzen teil.

26.2 (1) In seinem Bericht „Koordination der Cyber–Sicherheit“ hatte der RH die Cyber Sicherheit Steuerungsgruppe als grundsätzlich geeignetes Gremium zur gesamtstaatlichen Koordination der Cyber–Sicherheit beurteilt und die Cyber Sicherheit Plattform als geeignetes Gremium zur Erreichung der Ziele Vernetzung und Informationsaustausch zur Cyber–Sicherheit in Verwaltung, Wirtschaft und Wissenschaft. Der RH stellte nunmehr kritisch fest,

- dass die Länder im überprüften Zeitraum nicht zu den Sitzungen der Cyber Sicherheit Steuerungsgruppe eingeladen wurden, obwohl die Geschäftsordnung dieses Gremiums die Möglichkeit dazu vorsah, und
- dass bis Dezember 2023 keine Bediensteten des Landes Kärnten Mitglied in der Cyber Sicherheit Plattform waren.

Der RH empfahl dem Land Kärnten, zum Zweck der Vernetzung und des Informationsaustauschs eine Bedienstete bzw. einen Bediensteten des Landes Kärnten, die bzw. der mit dem Bereich Cyber–Sicherheit vertraut ist – wie etwa den Chief Information Security Officer (CISO) –, in die Cyber Sicherheit Plattform zu entsenden.

[37] Der IKDOK setzte sich unter Leitung des Innenministeriums aus den Vertreterinnen und Vertretern des Bundeskanzleramts, des Verteidigungsministeriums und des Außenministeriums zusammen. Die OpKoord bestand aus Vertreterinnen und Vertretern des IKDOK und der nach dem NISG festgestellten und eingerichteten Computer–Notfallteams. Anlassbezogen konnten zusätzlich auch Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen der öffentlichen Verwaltung miteinbezogen werden, wenn deren Wirkungsbereich von einem Risiko, Vorfall oder Cyber–Angriff betroffen war.

(2) Der RH hielt fest, dass das Land Kärnten bis November 2023 an fünf von acht Videokonferenzen des IKDOK zur Information der Länder teilnahm. Aus Sicht des RH war eine regelmäßige Teilnahme an den Videokonferenzen für das Land Kärnten wesentlich, um über die aktuelle Bedrohungslage im Bereich Cyber–Sicherheit informiert zu sein.

Er empfahl dem Land Kärnten, weiterhin und regelmäßig an den Videokonferenzen des IKDOK zur Information der Länder teilzunehmen.

26.3 Laut Stellungnahme des Landes Kärnten nehme der Chief Information Security Officer (CISO) des Landes Kärnten die Vernetzung und den Informationsaustausch in der Cyber Sicherheit Plattform wahr. Der Empfehlung zur Teilnahme an Videokonferenzen des IKDOK werde Folge geleistet.

26.4 Der RH anerkannte die nunmehrige Mitwirkung des mit Jänner 2024 eingerichteten Chief Information Security Officers (CISO) des Landes Kärnten an der Cyber Sicherheit Plattform.

Vernetzungs– und Informationsinitiativen der Computer–Notfallteams

27.1 (1) Zur Gewährleistung der Sicherheit von Netz– und Informationssystemen sah das NISG die Einrichtung eines nationalen Computer–Notfallteams (CERT.at) und eines Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) vor.

Das CERT.at stellte eine Drehscheibe für technische Informationen dar. Es gab Warnungen über kritische Schwachstellen und Sicherheitslücken in Software und Computernetzen heraus und unterstützte allgemein bei der Prävention von Cyber–Angriffen. Mit Unterstützung des Bundeskanzleramts betrieb CERT.at die Initiative Austrian Trust Circle, eine nationale Vernetzungsplattform für Informationsaustausch im Bereich IT–Sicherheit. Zielgruppe waren die strategischen Infrastrukturen und die öffentliche Verwaltung in Österreich. Das Land Kärnten war seit September 2022 Mitglied beim Austrian Trust Circle und nahm an drei von sechs Treffen teil.

(2) Das GovCERT war zur Unterstützung bei der Prävention und Bewältigung von Risiken, Vorfällen und Cyber–Angriffen der öffentlichen Verwaltung eingerichtet. Es konnte seine Aufgaben auch gegenüber Einrichtungen, die nicht vom NISG erfasst waren bzw. die sich den Verpflichtungen des NISG nicht unterwarfen (z.B. Länder), wahrnehmen. Die Länder waren demnach auch zur Teilnahme an der Informationsdrehscheibe des GovCERT berechtigt, die einen Rahmen für den Austausch über IT–

sicherheitsrelevante Informationen bot. Das Land Kärnten war zur Zeit der Gebarungsüberprüfung in die Informationsdrehscheibe des GovCERT eingebunden.[38]

(3) Für Unternehmen und sonstige Organisationen (z.B. öffentliche Einrichtungen) bestand darüber hinaus die Möglichkeit, ein Computer–Notfallteam für die eigene IT–Infrastruktur einzurichten. Diesen Computer–Notfallteams stand auch eine Teilnahme am CERT–Verbund Austria offen, einer freiwilligen Kooperationsplattform von österreichischen Computer–Notfallteams zum Informationsaustausch und zur Vernetzung im IKT–Bereich. Das Land Kärnten verfügte über kein eigenes Computer–Notfallteam und nahm daher nicht am CERT–Verbund Austria teil.

27.2 Der RH wertete positiv, dass das Land Kärnten nunmehr in die Informationsdrehscheibe des GovCERT eingebunden und dass es seit September 2022 auch Mitglied beim Austrian Trust Circle war. Er hielt jedoch kritisch fest, dass das Land an lediglich drei von sechs Treffen des Austrian Trust Circle teilnahm. Der RH erachtete die Teilnahme des Landes Kärnten an diesen Treffen als zweckmäßig für den Informationsaustausch im Bereich IT–Sicherheit.

Er empfahl dem Land Kärnten, an den Treffen des Austrian Trust Circle teilzunehmen.

27.3 Das Land Kärnten teilte in seiner Stellungnahme mit, dass der Chief Information Security Officer (CISO) des Landes Kärnten an Treffen des Austrian Trust Circle teilnehme.

27.4 Der RH begrüßte die nunmehrige Teilnahme des mit Jänner 2024 eingerichteten Chief Information Security Officers (CISO) des Landes Kärnten an den Treffen des Austrian Trust Circle.

[38] In seinem Bericht „Koordination der Cyber–Sicherheit“ (Reihe Bund 2022/13, TZ 19) hatte der RH festgestellt, dass das Land Kärnten im März 2021 noch nicht in die Informationsdrehscheibe des GovCERT eingebunden gewesen war.

Nationale Zusammenarbeit bei Cyber–Angriffen in Landesverwaltungen

28.1 Schwerwiegende Cyber–Angriffe in Landesverwaltungen erfordern eine Zusammenarbeit auf Bundes– und Landesebene. Beispielsweise waren verschiedene Meldungen an Bundesbehörden vorgesehen bzw. auf Bundesebene Gremien zur Gewährleistung der Cyber–Sicherheit eingerichtet:

(1) Die Einrichtungen der Länder konnten Meldungen von Risiken, Vorfällen und Cyber–Angriffen als freiwillige Meldungen im Sinne des NISG erstatten. Zuständig für deren Entgegennahme und Weiterleitung an die NIS–Behörde im Innenministerium war das Computer–Notfallteam der öffentlichen Verwaltung (GovCERT). Die eingegangenen Meldungen über Risiken, Vorfälle und Cyber–Angriffe waren Grundlage für das vom Innenminister regelmäßig zu erstellende Cyber–Lagebild.

Zur Analyse und Bewertung der Meldungen war der Innenminister außerdem verpflichtet, ein „NIS–Meldeanalysesystem" zu betreiben. Dies war eine IKT–Lösung zur Analyse von Angriffen, um Erkenntnisse daraus gewinnen und darauf aufbauend Präventions– und Abwehrmaßnahmen entwickeln zu können. Seit 2021 war eine Grundfunktion in Betrieb, die durch eine erst in Entwicklung befindliche Softwarelösung verbessert und ergänzt werden sollte.

(2) Als Verantwortliche gemäß DSGVO waren die Länder verpflichtet, die Verletzung des Schutzes personenbezogener Daten binnen 72 Stunden nach Bekanntwerden der Datenschutzbehörde zu melden. Diese hatte zu prüfen, ob der Verantwortliche geeignete Maßnahmen zur Behebung der Verletzung und zur Abmilderung möglicher nachteiliger Auswirkungen ergriffen hatte.

(3) Bestand der Verdacht einer Straftat, die den gesetzmäßigen Wirkungsbereich einer Behörde oder Dienststelle der Länder betraf, waren diese gemäß § 78 Strafprozessordnung[39] verpflichtet, Anzeige an die Kriminalpolizei oder die Staatsanwaltschaft zu erstatten. Das im Bundeskriminalamt eingerichtete Cybercrime Competence Center war als nationale Koordinierungs– und Meldestelle im Bereich Cyberkriminalität zuständig.[40]

(4) Die in den Landespolizeidirektionen eingerichteten Landesämter für Verfassungsschutz und Terrorismusbekämpfung leisteten bei Cyber–Angriffen in verfassungsmäßigen Einrichtungen (z.B. Landesregierungen) die Ermittlungsarbeit und Beweis-

[39] BGBl. 631/1975 i.d.g.F.

[40] Der RH verwies dazu auf die Darstellung der Organisation und Aufgaben des Cybercrime Competence Centers in seinem Bericht „Prävention und Bekämpfung von Cyberkriminalität" (Reihe Bund 2021/23, TZ 26, TZ 27) sowie in der zugehörigen Follow–up–Überprüfung (Reihe Bund 2024/18).

mittelsicherung. Das Cyber Security Center in der Direktion Staatsschutz und Nachrichtendienst des Innenministeriums bildete im Anlassfall die Schnittstelle zu internationalen Strafverfolgungsbehörden und stellte sein Fachwissen zur Verfügung.

(5) Bei schwerwiegenden Cyber–Angriffen hatte der Innenminister zu entscheiden, ob eine Cyber–Krise[41] festzustellen war. Dabei beriet ihn der Cyberkrisenmanagement–Koordinationsausschuss. Dieser Ausschuss bestand aus je einer Vertreterin bzw. einem Vertreter von Innenministerium, Verteidigungsministerium, Außenministerium und Bundeskanzleramt; erforderlichenfalls konnte er u.a. um Landesvertreterinnen bzw. –vertreter erweitert werden. Die operative Unterstützung des Koordinationsausschusses im Cyber–Krisenmanagement oblag dem IKDOK. Es bestand jedoch keine rechtliche Verpflichtung der Länder, dem IKDOK die notwendigen Informationsgrundlagen zur Verfügung zu stellen.

(6) Behörden und Organe der Länder waren gemäß Wehrgesetz 2001[42] in ihrem jeweiligen Wirkungsbereich zur Anforderung einer Assistenzleistung des Österreichischen Bundesheeres berechtigt.[43] Dies konnte auch die Unterstützung bei der Bekämpfung der Auswirkungen schwerwiegender Cyber–Angriffe umfassen. Im Bericht „Koordination der Cyber–Defence“ (Reihe Bund 2023/30, TZ 16) hatte der RH festgestellt, dass im Verteidigungsministerium die Einrichtung von ständig verfügbaren Cyber–Einsatzteams (Rapid Response Teams) in Planung war.

(7) Im Zusammenhang mit der Bewältigung der Cyber–Krise im Außenministerium im Dezember 2019 erstellte das Bundeskanzleramt einen „Lessons Learned“–Bericht. Laut diesem Bericht hätte der Einsatz eines ständig verfügbaren Einsatzteams (Rapid Response Team) und eines Security Operations Centers (SOC) bereits zu Beginn des Angriffs zu einer rascheren Behebung der Cyber–Krise beigetragen. Ein permanent verfügbares nationales Cyber–Einsatzteam (Rapid Response Team) und ein Security Operations Center im Sinne einer staatlichen Cyber–Sicherheitsleitstelle waren im Dezember 2023 noch nicht eingerichtet.

41 Das NISG (§ 3 Z 22) definierte die Cyber–Krise als „ein[en] oder mehrere Sicherheitsvorfälle, die eine gegenwärtige und unmittelbare Gefahr für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen darstellen und schwerwiegende Auswirkungen auf die Gesundheit, die Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen nach sich ziehen können“.

42 BGBl. I 146/2001 i.d.g.F.

43 Dies unter der Voraussetzung, dass die originär zuständige Stelle die konkrete Aufgabe weder mit eigenen Mitteln noch unter Heranziehung kurzfristig aufgebotener Mittel bewältigen konnte. Diese Aufgabe umfasste den Schutz der verfassungsmäßigen Einrichtungen (inklusive der Verfassungsordnung an sich) und ihrer Handlungsfähigkeit, den Schutz der demokratischen Freiheiten der Einwohnerinnen und Einwohner und die Aufrechterhaltung der Ordnung und Sicherheit im Inneren.

28.2 (1) Aus Sicht des RH war die Zusammenarbeit mit den Bundesbehörden und Cyber–Gremien wesentlich, um die Auswirkungen von Cyber–Angriffen zu verhindern oder möglichst gering zu halten. Der RH identifizierte für die Bewältigung zukünftiger Cyber–Angriffe folgende Anlaufstellen, die Unterstützung leisten können bzw. für weitere staatliche Stellen Informationen weiterverarbeiten können:

- NIS–Behörde im Innenministerium:
  Die freiwillige Meldung von Risiken, Vorfällen und Cyber–Angriffen durch die Einrichtungen der Länder trägt dazu bei, einen gesamthaften Überblick über die aktuelle Bedrohungslage im Bereich Cyber–Sicherheit für die Empfänger des Cyber–Lagebilds zu schaffen.
- Datenschutzbehörde:
  Eine enge Zusammenarbeit zwischen den betroffenen Einrichtungen der Länder und der Datenschutzbehörde soll den Schutz personenbezogener Daten auch nach einer Verletzung wiederherstellen bzw. zukünftig absichern.
- Cybercrime Competence Center:
  Als nationale Koordinierungs– und Meldestelle im Bereich Cyberkriminalität ist das im Bundeskriminalamt eingerichtete Cybercrime Competence Center zuständig.
- Cyber Security Center:
  Die Landesämter für Verfassungsschutz und Terrorismusbekämpfung leisten bei Cyber–Angriffen in verfassungsmäßigen Einrichtungen die Ermittlungsarbeit und Beweismittelsicherung. Das Cyber Security Center in der Direktion Staatsschutz und Nachrichtendienst des Innenministeriums bildet im Anlassfall die Schnittstelle zu internationalen Strafverfolgungsbehörden und stellt Fachwissen zur Verfügung.
- Cyberkrisenmanagement–Koordinationsausschuss:
  Bei der Bewältigung von schwerwiegenden Cyber–Angriffen ist der Koordinationsausschuss ein geeignetes Gremium zur Beratung des Innenministers.
- Assistenzleistung des Österreichischen Bundesheeres:
  Bei schwerwiegenden Cyber–Angriffen können Behörden und Organe der Länder eine Assistenzleistung bei der Bekämpfung der Auswirkungen anfordern.

(2) Für eine effiziente staatliche – gebietskörperschaftenübergreifende – Cyber–Sicherheitsvorsorge wären nach Ansicht des RH noch weitere Umsetzungsschritte erforderlich:

- Fertigstellung und Einsatz eines NIS–Meldeanalysesystems,
- Weiterentwicklung des Cybercrime Competence Centers,
- Definition eines Informationsaustauschs mit dem IKDOK zur Unterstützung des Cyberkrisenmanagement–Koordinationsausschusses,
- Einrichtung eines ständig verfügbaren nationalen Cyber–Einsatzteams (Rapid Response Team) im Innen– bzw. Verteidigungsministerium und
- Einrichtung eines Security Operations Centers als staatliche Cyber–Sicherheitsleitstelle.[44]

Der RH hielt fest, dass die Zusammenarbeit auf nationaler Ebene im Wege von Meldungen, Ansuchen um Unterstützung und dem Austausch von Informationen erfolgen kann.

Er empfahl dem Land Kärnten, die vom Bund gesetzten Maßnahmen und Initiativen für eine gesamtstaatliche Verbesserung der Cyber–Sicherheitsvorsorge zu unterstützen.

28.3 Das Land Kärnten sagte die Umsetzung zu.

[44] Der RH verwies dazu auf die Empfehlungen in seinem Bericht „Koordination der Cyber–Sicherheit“ (Reihe Bund 2022/13),
- ein nationales Cyber–Einsatzteam in Abstimmung mit dem in der Landesverteidigung geplanten Cyber–Einsatzteam zu schaffen (TZ 25) sowie
- eine staatliche Cyber–Sicherheitsleitstelle mit Einsatzzentrale einzurichten, in die das Cyber–Einsatzteam zu integrieren wäre (TZ 26).

Schlussempfehlungen

29 Zusammenfassend empfahl der RH dem Land Kärnten:

(1) Der Grundsatz der Amtsverschwiegenheit (bzw. der erforderlichen Geheimhaltung nach dem Informationsfreiheitsgesetz) wäre durch für alle Bedienstete geltende, konkretisierende Regelungen näher auszuführen. Einheitliche Vorgaben

- zur Klassifizierung von Informationen (Einteilung z.B. nach dem Vertraulichkeitsgrad),
- zur Kennzeichnung der Klassifikationsstufe,
- zu den anzuwendenden organisatorischen und technischen Sicherheitsmaßnahmen (beispielsweise Verschlüsselung, Einschränkung der elektronischen Verarbeitung, Schulungen) und
- zur Verantwortung für die Durchführung

sollten in einem organisationsweiten, von zentraler Stelle verantworteten Grundlagendokument erlassen bzw. ergänzt werden. Dies wäre auch im Hinblick auf die Anforderungen der NIS–2–Richtlinie zweckmäßig. (TZ 3)

(2) Das Land Kärnten sollte sich auf die Anforderungen durch die Umsetzung der NIS–2–Richtlinie vorbereiten und den nationalen Umsetzungsprozess begleiten, um die wesentlichen Themen – wie Risikomanagement, Notfallvorsorge, Krisenmanagement, Verantwortung der Leitungsebene, Informationsklassifizierung – zeitgerecht zu berücksichtigen. Dabei wäre eine Zusammenarbeit mit den in gleicher Weise betroffenen anderen Bundesländern anzustreben. (TZ 4)

(3) Es wäre darauf hinzuwirken, dass auch auf Landesebene den Verpflichtungen gemäß dem Netz– und Informationssystemsicherheitsgesetz (NISG) zu Sicherheitsvorkehrungen für die Netz– und Informationssysteme bestmöglich entsprochen wird. Dies mit dem Ziel, zu einem einheitlichen Schutzniveau im Cyber–Bereich auf Ebene aller Gebietskörperschaften beizutragen. (TZ 4)

(4) Die IT–Sicherheitsstrategie des Landes Kärnten wäre unter Berücksichtigung der IT–Strategie des Landes aus 2023 zu aktualisieren und ihre Aktualität zukünftig regelmäßig zu überprüfen. Insbesondere wären in der IT–Sicherheitsstrategie

- die Verantwortung der obere Leitungsebene für die IT–Sicherheit ausdrücklich festzulegen,
- die Grundzüge des Risikomanagementprozesses zu dokumentieren,

- die Hinweise für alle Bediensteten zum Vorgehen bei Cyber–Angriffen zu konkretisieren und
- Regelungen zur Zusammenarbeit mit bestehenden Gremien zur Cyber–Sicherheit aufzunehmen.

Dies wäre auch im Hinblick auf die Umsetzung der NIS–2–Richtlinie zweckmäßig. (TZ 5)

(5) Die Risikoanalysen für die allgemeinen IT–Risiken wären jedenfalls um Bedrohungen aus Cyber–Angriffen zu erweitern. (TZ 6)

(6) Die IT–Systeme wären nach der Höhe des Risikos und den möglichen Auswirkungen einer Störung auf die Verwaltungstätigkeit festzulegen. Die Risikoanalysen einzelner IT–Systeme mit hohem Risiko wären in kürzeren Abständen (z.B. jährlich oder alle drei Jahre) zu überprüfen und gegebenenfalls zu aktualisieren. (TZ 6)

(7) In der IT–Sicherheitsstrategie wäre ein regelmäßiges, standardisiertes Berichtswesen zur IT–Sicherheit – unter Einbeziehung der oberen Leitungsebene (Leitung Landesamtsdirektion, zuständiges Mitglied der Landesregierung) als Berichtsempfänger – festzulegen. Dies wäre auch im Hinblick auf die Überwachungspflichten der Leitungsorgane nach der NIS–2–Richtlinie (Art. 20 Abs. 1) zweckmäßig. (TZ 6)

(8) Frei werdende Stellen in leitenden Positionen wären so bald als möglich und – in Anlehnung an die Bestimmungen zur Ausschreibung von bestimmten Leitungsfunktionen gemäß dem Kärntner Objektivierungsgesetz – im Idealfall bereits sechs Monate vor dem bekannten Ausscheiden auszuschreiben, um eine nahtlose Nachbesetzung der Stelle zu ermöglichen. (TZ 7)

(9) Gemäß den Vorgaben des Österreichischen Informationssicherheitshandbuchs wäre ein Informationssicherheitsmanagement–Team einzurichten; dabei wäre auf eine zweckentsprechende Einbindung der Anwenderinnen und Anwender sowie der nachgeordneten Dienststellen zu achten. (TZ 9)

(10) Auch im Hinblick auf die bevorstehende Umsetzung der NIS–2–Richtlinie wären das Informationssicherheitsniveau der externen Dienstleister in eine Risikobeurteilung einfließen zu lassen, adäquate Maßnahmen zu treffen und die Regelung zur Beaufsichtigung und Überwachung von externen Dienstleistern so bald als möglich in Kraft zu setzen. (TZ 11)

(11) Die Datenschutzinformation aus dem Jahr 2018 an neu eintretende Bedienstete wäre zu aktualisieren. (TZ 11)

(12) Bei einer zukünftig erforderlichen Neuausstattung der IT–Arbeitsplätze wären Bedienstete mit regelmäßiger Telearbeit mit mobilen Endgeräten auszustatten. (TZ 12)

(13) Sicherheitsrichtlinien zur Nutzung der im Land Kärnten eingesetzten Videokonferenzlösung wären zu erstellen und in Kraft zu setzen. Die Anleitung zur Nutzung der Videokonferenzlösung wäre zu aktualisieren und den Bediensteten zur Kenntnis zu bringen. (TZ 12)

(14) Konkrete Regelungen für die dienstliche Nutzung einer privaten IT–Ausstattung (z.B. Nutzung als Thin–Client) wären zu erlassen und den Bediensteten zur Kenntnis zu bringen. (TZ 13)

(15) Die schriftliche Dokumentation über Umsetzung und Ausgestaltung der IT–Sicherheitsmaßnahmen wäre für die zentralen IT–Komponenten zu vervollständigen – auch im Hinblick auf die Anforderungen durch die NIS–2–Richtlinie. Eine umfassende Dokumentation sollte die Nachvollziehbarkeit der Funktionsweise der IT–Systeme gewährleisten. (TZ 14)

(16) Die schriftliche Dokumentation über Umsetzung und Ausgestaltung der IT–Sicherheitsmaßnahmen wäre auch für die Arbeitsplatzrechner zu vervollständigen – auch im Hinblick auf die Anforderungen durch die NIS–2–Richtlinie. Eine umfassende Dokumentation sollte die Nachvollziehbarkeit der Funktionsweise der IT–Systeme gewährleisten. (TZ 15)

(17) Eine Zwei–Faktor–Authentifizierung wäre für alle IT–Arbeitsplätze einzuführen. (TZ 15)

(18) Es wäre zu evaluieren, ob eine USB–Port–Deaktivierung oder USB–Port–Kontrolle zu einer Erhöhung der IT–Sicherheit führt; gegebenenfalls wäre diese einzurichten. (TZ 15)

(19) Auf Basis einer umfassenden Risikoanalyse und der verfügbaren Ressourcen wären sowohl interne als auch externe IT–Sicherheitsüberprüfungen verstärkt und regelmäßig durchzuführen. Bei externen IT–Sicherheitsüberprüfungen wären die Auditoren regelmäßig zu wechseln, um die Unabhängigkeit der Prüfung zu gewährleisten und neue Sichtweisen einbringen zu können. (TZ 16)

(20) Ein umfassendes IT–Notfallhandbuch (inklusive überarbeiteter Anforderungen an das Notfallrechenzentrum) wäre zu erstellen; dieses sollte all jene Prozesse abbilden, die den Betrieb auch in Ausnahmesituationen aufrecht

halten können. Dabei sollten insbesondere die Notfallvorsorge und –bewältigung sowie Tests und Übungen berücksichtigt werden. (TZ 17)

(21) Der Sicherheits– und Notfallplan für das Rechenzentrum aus 2019, das Sicherungs– und Wiederherstellungskonzept aus 2014 sowie die Regelung für IT–Notfallnummern und Zutritt wären einer Qualitätsüberprüfung zu unterziehen und zu aktualisieren. Im Sicherheits– und Notfallplan für das Rechenzentrum wären die aktuellen Risikoanalysen und die Erfassung der Anforderungen an das Notfallrechenzentrum besonders zu beachten. (TZ 17)

(22) Für alle Bediensteten wären konkrete Regelungen zum Umgang mit digitalen, sensiblen, personenbezogenen und nicht personenbezogenen Daten im Netzwerk zu treffen und begleitende technische Maßnahmen umzusetzen, z.B. Verschlüsselung, Passwortschutz von Dokumenten, Klassifizierung von elektronischen Dokumenten, Ablage in besonders geschützten Bereichen. (TZ 20)

(23) Der „Leitfaden Krisenmanagement“ wäre im Sinne einer Qualitätssicherung zu aktualisieren. Die Erkenntnisse aus der Bewältigung des Cyber–Angriffs wären dabei zu berücksichtigen und einzuarbeiten. Insbesondere wären Beurteilungskriterien für das Vorliegen einer „Cyber–Krise“ aufzunehmen. (TZ 22)

(24) Die geplanten technischen und organisatorischen Maßnahmen zur Erhöhung der IT–Sicherheit wären zeitnah umzusetzen. (TZ 23)

(25) Die Notwendigkeit und Eignung von IT–Softwarelösungen wären vor deren Beschaffung zu evaluieren. Zahlungen im Zusammenhang mit Beraterverträgen wären erst nach Leistungserbringung durchzuführen. Die Dokumentation der Leistungserbringung sollte genaue Angaben zu den geleisteten Stunden (Anzahl und Leistungszeitpunkt) enthalten. (TZ 24)

(26) Das Land Kärnten sollte regelmäßig an den Sitzungen der Kooperation Bund–Länder–Städte–Gemeinden (BLSG) und der Arbeitsgruppenleiter sowie an den Sitzungen der Länderarbeitsgruppe teilnehmen und sicherstellen, dass relevante Informationen über die Sitzungen (Teilnahme, Unterlagen) innerhalb der Organisationseinheit zur Verfügung stehen. (TZ 25)

(27) Die aktive Mitwirkung des Landes Kärnten an den Arbeitsgruppen des Gremiums Bund–Länder–Städte–Gemeinden (BLSG) – insbesondere an der Arbeitsgruppe Recht/Sicherheit – wäre zu evaluieren. (TZ 25)

(28) Zum Zweck der Vernetzung und des Informationsaustauschs wäre eine Bedienstete bzw. ein Bediensteter des Landes Kärnten, die bzw. der mit dem Bereich Cyber–Sicherheit vertraut ist – wie etwa der Chief Information Security Officer (CISO) –, in die Cyber Sicherheit Plattform zu entsenden. (TZ 26)

(29) An Videokonferenzen des IKDOK (Innerer Kreis der Operativen Koordinierungsstruktur) zur Information der Länder wäre weiterhin und regelmäßig teilzunehmen. (TZ 26)

(30) An den Treffen des Austrian Trust Circle wäre teilzunehmen. (TZ 27)

(31) Die vom Bund gesetzten Maßnahmen und Initiativen für eine gesamtstaatliche Verbesserung der Cyber–Sicherheitsvorsorge wären zu unterstützen. (TZ 28)

Rechnungshof Österreich

Wien, im Oktober 2024
Die Präsidentin:

Dr. Margit Kraker

Anhang

Tabelle A: Dokumentierter Ablauf des Cyber–Angriffs

Zeitpunkt	Beschreibung
April 2022	Einfallszeitpunkt auf einem Arbeitsplatz eines Bediensteten; in der Folge fanden Anmeldeversuche auf Systeme des Landes Kärnten mit den Anmeldedaten des Bediensteten statt
	Übernahme eines höher privilegierten Admin–Accounts und Zugriffe auf Datenspeicher und weitere Systeme; Angreifer konnten damit die System–Umgebung ausspähen, verschiedene Hacker–Tools verteilen sowie System–Befehle absetzen
24. Mai 2022	das Land Kärnten erkannte Anomalien durch Aktivitäten im Netzwerk sowie Anmeldeprobleme und bereits teilweise erfolgte Verschlüsselungen von Arbeitsplatzrechnern sowie einzelner Server–Systeme
	Umsetzung von Sofortmaßnahmen: geordnetes Herunterfahren aller Systeme; Trennung der Netzwerkverbindungen; Sperre der Verbindungen von außen (ca. 180 Server–Systeme sowie ca. 3.100 Arbeitsplatzrechner betroffen)
	Kontaktaufnahme und Informationsweitergabe an: Landesamtsdirektor, Kriminalpolizei, Datenschutzbeauftragten, Systemverantwortliche
	Kontaktaufnahme mit externen Unternehmen und Auftrag zu Datenanalyse und forensischen Untersuchungen an ein spezialisiertes Unternehmen für IT–Forensik und IT–Sicherheit
	Meldung an die Datenschutzbehörde
	Auslesen der Lösegeldforderungen durch ein externes Unternehmen im Darknet
25. Mai 2022	interne Informationsweitergabe zum Cyber–Angriff
	Hochfahren der Systeme für die Erstellung von elektronischen Auszahlungsdaten (in isolierter Umgebung)
	Besprechungen mit Kriminalpolizei und Landesamt für Verfassungsschutz und Terrorismusbekämpfung
	Absetzung der NIS–Meldung über das Meldeportal GovCERT; eine Sofortunterstützung durch das GovCERT wurde nicht angefordert
	Beginn der Bereinigung bzw. Neuaufbau der Systeme
26. bis 31. Mai 2022	regelmäßige Arbeitsgespräche mit externen Unternehmen
	Neuaufbau der IT–Infrastruktur nach festgelegter Priorisierung
	Ausrollung der Software zur Bereinigung von Systemen auf Server und Clients
	Anzeige bei der zuständigen Staatsanwaltschaft
3. Juni 2022	Veröffentlichung von Daten des Landes Kärnten auf File–Sharing–Plattform durch die Hacker
	Information an den Landeshauptmann
	weitere Anzeige bei der Staatsanwaltschaft
7. Juni 2022	Aufnahme der Tätigkeiten der Cyber–Einsatz–Gruppe auf Ebene der Landesamtsdirektion
Juni 2022	sukzessive Wiederherstellung von betroffenen Systemen und Umsetzung der Sofortmaßnahmen
	Vorlage des forensischen Berichts des externen Dienstleisters an das Land Kärnten
18. Juli 2022	ergänzende Meldung an die Datenschutzbehörde
2. August 2022	Einstellung des Data–Breach–Verfahrens durch die Datenschutzbehörde
November 2022	Ende der Arbeit der Cyber–Einsatz–Gruppe
8. Jänner 2023	Vollbetrieb der IT–Systeme
6. November 2023	Einstellung des Ermittlungsverfahrens seitens der Staatsanwaltschaft

Quelle: Land Kärnten

R
H