LD31 –16.01/02.003 Kiel, 28. August 2006

Kurzgutachten

über das Auditverfahren gemäß § 43 Abs. 2 LDSG

Landesnetz Schleswig-Holstein

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Behördenaudits 3

2 Feststellungen zu den sicherheitstechnischen Elementen des Landesnetzes 4
2.1 Zweck und Ausprägung 4
2.2 Betreiber 5
2.3 Dienstleister 6
2.4 Nutzer 6
2.5 Landesnetzkomponenten 8
2.5.1 Netzinfrastruktur 8
2.5.2 Backbone 8
2.5.3 Anschlussleitung 9
2.5.4 Zugangsrouter 10
2.5.5 MPLS-VPN 10
2.5.6 Quality of Service 10
2.5.7 Voice-Transport 11
2.5.8 Geschlossene Benutzergruppen (GBG) 11
2.5.9 Verbindungsfirewall 12
2.5.10 Übergaberouter 13
2.5.11 Berichtswesen und Kontrolle 13
2.6 Landesnetzmanagement 14
2.6.1 T-Systems ES 14
2.6.2 Dataport 15
2.7 Verträge und Vereinbarungen 17
2.7.1 Betreibervertrag zwischen Finanzministerium und Dataport 17
2.7.2 Verträge zwischen Finanzministerium und T-Systems ES 17
2.7.3 Ausführungsbestimmungen für Landesbehörden 18
2.7.4 Nutzervertrag für Kommunalbehörden und sonstige Stellen 18
2.8 Generaldokumentation des Landesnetzes 19

3 Datenschutz-Managementsystem im laufenden Betrieb 20
3.1 Sicherheitsziele 20
3.2 Sicherheitskonzept 20
3.2.1 Übergreifendes Sicherheitskonzept des Finanzministeriums 20
3.2.2 Sicherheitskonzept Dataport 22
3.2.3 Sicherheitskonzept T-Systems ES 23
3.3 Sicherheitsmanagement 25

4 Datenschutzrechtliche Bewertung 26
4.1 Daten verarbeitende Stelle 26
4.2 Auftragsdatenverarbeitung 27
4.3 Zusammenfassende Bewertung 27

1 Gegenstand des Datenschutz-Behördenaudits

Das Unabhängige Landeszentrum für Datenschutz (ULD) und das Innenministerium Schleswig-Holstein haben am 01.08.2002 vereinbart, das „integrierte Sprach- und Datennetz der schleswig-holsteinischen Landesverwaltung (Landesnetz)“ einem Behördenaudit zu unterziehen. Die Betreiberfunktion für das Landesnetz wurde im Jahr 2003 an das Finanzministerium übertragen.[1]

Der Betreiber des Landesnetzes hat folgende Datenschutzziele festgelegt:[2]

- Herstellung einer sicheren und flächendeckenden Kommunikationsinfrastruktur (Landesnetz) für die öffentlichen Verwaltungen in Schleswig-Holstein,
- Transport von Daten und Sprache in einheitlicher digitaler Struktur in einem von unbekannten Teilnehmern abgeschotteten Landesnetz,
- Schutz der im Landesnetz übertragenen Daten vor Angriffen aus dem Internet und vor Angriffen aus angeschlossenen Nutzernetzen,
- einfache und revisionssichere Kontrolle der festgelegten Sicherheitsmaßnahmen durch den Nutzer,
- Integration eines qualifizierten und übergreifenden Sicherheitsmanagement für die Umsetzung der Sicherheitsprozesse sowie
- eine umfassende und nachvollziehbare Dokumentation über den Aufbau und den Betrieb des Landesnetzes.

Die netztechnische Planung und Realisierung des Landesnetzes sowie die Einrichtung eines umfassenden Netzwerkmanagements stützt sich auf folgende Regelungen und Maßnahmen:

---

[1] Die Zuständigkeit für das Landesnetz ist während des Auditverfahrens vom Innenministerium auf das Finanzministerium übergegangen (Organisationserlass der Ministerpräsidentin über die Geschäftsverteilung der Landesregierung, Vom 8. Juli 2003 –StK 111 – 012.01 der Ministerpräsidentin.

[2] Finanzministerium, Sicherheitsmanagement für das Landesnetz.

a) Beachtung von Rechtsvorschriften, Richtlinien und sonstigen Arbeitsanweisungen zur Datensicherheit und zur Ordnungsmäßigkeit der Datenverarbeitung,

b) Festlegung von Zuständigkeiten sowie die Abgrenzung der Verantwortung der beteiligten Betreiber, Dienstleister und Nutzer,

c) Ausgestaltung der technischen und organisatorischen Maßnahmen zur Datensicherheit der für das Landesnetz eingesetzten IT-Systeme und der über das Landesnetz kommunizierten Daten,

d) Definition der Maßnahmen zur Überwachung der auf den Landesnetzkomponenten durchgeführten administrativen Aktivitäten,

e) Einführung eines übergreifenden Sicherheitsmanagement für die dauerhafte Aufrechterhaltung der festgelegten Sicherheitsmaßnahmen sowie

f) Gewährleistung der Vollständigkeit der Dokumentation über die Landesnetzkomponenten sowie über die aufbau- und ablauforganisatorischen Strukturen bei dem Finanzministerium und bei seinen Dienstleistern Dataport und T-Systems Enterprise Services GmbH[3].

Mit der Umsetzung der festgelegten Ziele hat das Finanzministerium die Dienstleister Dataport und T-Systems ES betraut.

2 Feststellungen zu den sicherheitstechnischen Elementen des Landesnetzes

2.1 Zweck und Ausprägung

Aufgabe des Landesnetzes ist es, den Datentransport zwischen definierten Anschlüssen und ausschließlich genehmigten Teilnehmern (Nutzern) zur Verfügung zu stellen. Der Datentransport erfolgt aufgrund der abgesicherten Netzinfrastruktur unverschlüsselt. Es findet keine Speicherung der zu übertragenden Daten statt. Neben dem Transport von Daten wird über das Landesnetz auch Sprache in digitalisierter Form übertragen. Die Bereitstellung von Sprachdiensten erfolgt derzeit nur für die Landesbehörden.

[3] Im Folgenden nur noch mit T-Systems ES bezeichnet.

Das Landesnetz dient dem Zweck,

- eine flächendeckende, einheitliche und multimediale Kommunikationsinfrastruktur für die öffentlichen Verwaltungen in Schleswig-Holstein herzustellen,

- Daten und Sprache einheitlich digital zu transportieren, so dass ein modernes, integriertes und standardisiertes Transportnetz für die Verwaltungen entsteht,

- durch die einheitliche Anschlusstechnik und flächendeckende Verfügbarkeit übergreifende Verwaltungsprozesse (E-Government) in Schleswig-Holstein sicherzustellen und

- eine Kommunikationslösung und die damit verbundenen Prozesse einfach, beherrschbar und wirtschaftlich anzubieten.

2.2 Betreiber

Das Landesnetz wird vom Land Schleswig-Holstein, vertreten durch das Finanzministerium (FM), betrieben. Das Land Schleswig-Holstein besitzt keine eigenen Netzleitungen, daher bedient es sich zur Leistungserbringung der Dienstleister Dataport sowie T-Systems ES.

Die datenschutzrechtliche Verantwortung für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung trägt das Finanzministerium Schleswig-Holstein. Innerorganisatorisch ist für die Einhaltung der jeweils anzuwendenden Vorschriften zum Datenschutz und zur Datensicherheit für das Landesnetz im Finanzministerium das Referat „Ressortübergreifendes operatives IT-Management, Landessprach- und Datennetz“ (VI 54) zuständig und verantwortlich.

Die Überwachung und Prüfung des in dem für das Landesnetz erstellten Sicherheitskonzepts festgelegten Sicherheitsmaßnahmen obliegt dem im Referat VI 54 eingerichteten Sicherheitsmanagement.

2.3 Dienstleister

Der operative Betrieb des Landesnetzes wird von den vom FM beauftragten Dienstleistern T-Systems ES und Dataport sichergestellt.

Aufgabe von T-Systems ES ist die Bereitstellung und der Betrieb von Übertragungsleistungen und –schnittstellen zum Transport von IP-Datenströmen zwischen den vom FM benannten Kommunikationspartnern. Hierzu übernimmt T-Systems ES die Aufgabe der Bildung von so genannten virtuellen Gruppen (VPN), die mit Hilfe von MPLS-Technologie voneinander abgeschottet werden. T-Systems ES lässt diese Leistungen durch Einheiten des Konzerns Deutsche Telekom AG erbringen. Zwischen dem FM und T-Systems ES sind Vereinbarungen über die Leistungen und damit die Aufgaben der T-Systems ES und seiner eingesetzten „Subunternehmer“ getroffen worden.

Aufgabe von Dataport ist die Bereitstellung und der Betrieb der Übergaberouter beim Nutzer und der Verbindungsfirewall, über die Kommunikationsbeziehungen zwischen den Nutzern am Landesnetz untereinander und Netzübergänge realisiert werden. Die Einstellungen der Kommunikationsparameter am Übergaberouter und der Verbindungsfirewall erfolgen im Auftrag des Nutzers. Das FM gibt die Grundkonfiguration der Router in Form von generellen Einstellungen vor. Die konkrete Ausgestaltung der Routerkonfiguration wird entsprechend der Beauftragung durch den Nutzer von Dataport vorgenommen und dem Nutzer anschließend in einem gesonderten Bericht dargestellt. Das FM hat das Recht sich diese Berichte ebenfalls vorlegen zu lassen. Darüber hinaus überwacht Dataport die Gesamtleistung des LN am Übergabepunkt (Verfügbarkeit, Quality of Service, Kommunikationspolicy, Sicherheitseinstellungen).

Dataport ist autorisiert, optionale Dienstleistungen für die Nutzer im Landesnetz nach Abstimmung mit dem FM anzubieten.

2.4 Nutzer

Die angeschlossenen Organisationen (Nutzer) nutzen das Landesnetz für den Datentransport im Rahmen ihrer Fachanwendungen und für den Austausch von Verwaltungsinformationen. Anschlussberechtigt sind

- Landesbehörden,

- Anstalten, Stiftungen und sonstige Körperschaften des öffentlichen Rechts soweit sie der Aufsicht des Landes unterliegen,

- Kommunalbehörden, wie Kreise, kreisfreie Städte, Gemeinden und Ämter sowie

- Einrichtungen mit mindestens 51 % Landes- oder Kommunalbeteiligung oder denen mindestens 50 % Landes- oder Kommunalaufgaben übertragen wurden.

Bei einem Anschluss an das Landesnetz hat der Nutzer folgende Anforderungen zu berücksichtigen:

- Bei der Nutzung des Landesnetzes werden die Daten des Nutzers unverschlüsselt transportiert. Sollte die Sicherheitsbetrachtung des Nutzers für die Verarbeitung seiner personenbezogenen Daten einen höheren Schutz erfordern, hat er weitergehende Sicherheitsmaßnahmen in eigener Zuständigkeit zu treffen.

- Der Nutzer hat eigenverantwortlich in einem Sicherheitskonzept die technischen und organisatorischen Sicherheitsmaßnahmen für die automatisierte Datenverarbeitung in seinem Verantwortungsbereich festzulegen, um den Schutz seiner internen Datenverarbeitung und der von ihm über das Landesnetz kommunizierten Daten zu gewährleisten.

- Die für den Datentransport eingesetzten IT-Systeme (Leitungsnetz, Netzübergabeeinrichtungen) stehen in der Verantwortung des FM. Eine Administration durch den Nutzer ist ausgeschlossen.

- Der Übergaberouter, der das lokale Netz des Nutzers mit dem Landesnetz verbindet, ist für die Einstellung der Kommunikationsbeziehungen mit Filterfunktionalitäten ausgestattet. Die Filter werden von Dataport nach den Vorgaben des Nutzers eingestellt.

- Die Konfiguration des Übergaberouters sowie die Sicherheitseinstellungen sind für den jeweils betroffenen Nutzer transparent und jederzeit kontrollierbar.

2.5 Landesnetzkomponenten

2.5.1 Netzinfrastruktur

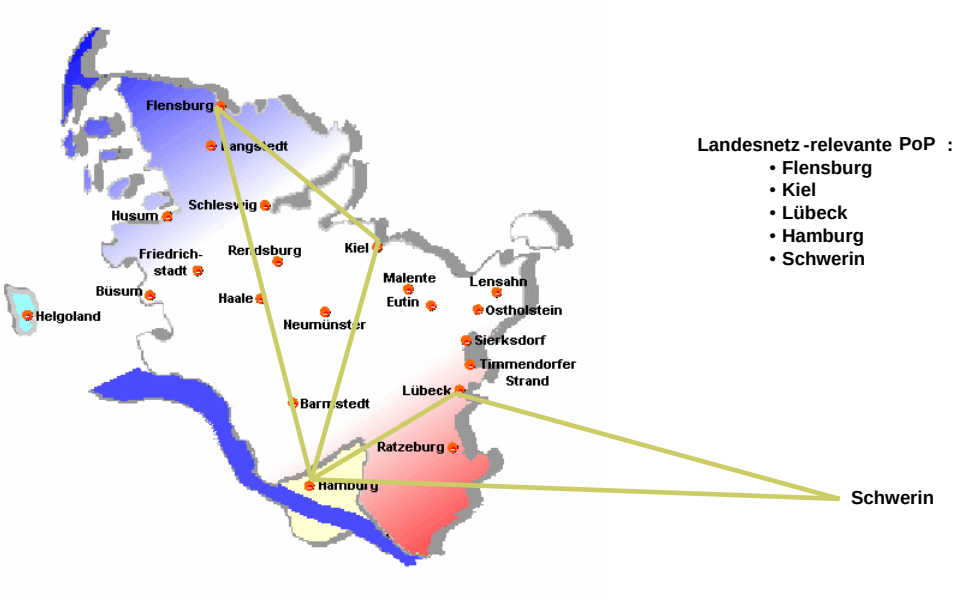
Die physikalische Netzinfrastruktur wird vom FM als kundenspezifische Netzdienstleistung bei T-Systems ES angemietet. T-Systems ES hat das Produkt „Kommunikationsnetz Schleswig-Holstein“ (KNSH) entwickelt und stellt in Zusammenarbeit mit anderen Einheiten des Konzerns Deutsche Telekom AG den Transport von IP-Datenströmen zwischen den vom FM benannten Anschlusspunkten bereit. Basis der physikalischen Netzinfrastruktur ist der MPLS-Backbone der Deutschen Telekom AG, von dem mehrere Konzentrationsstandorte (PoPs) zur Realisierung der Übertragungsleistung genutzt werden. Anschlussleitungen (Local Loop) in unterschiedlicher technischer Ausprägung stellen die Verbindung vom Backbone zum Zugangsrouter des Nutzers her.

2.5.2 Backbone

Die Deutsche Telekom AG betreibt einen leistungsfähigen und vollredundanten Backbone zwischen derzeit 74 Standorten bundesweit. Diese 74 Standorte (nachfolgend „Point of Presence“ oder „PoP“ genannt) sind in sich ebenfalls vollredundant ausgelegt. Die PoPs übernehmen einerseits die Aufgabe der Verkehrslenkung über den Backbone und bilden andererseits den Anschlusspunkt der regionalen Local Loops (Anschlussleitungen) zu den Kundenlokationen.

Als Übertragungsverfahren und zur Trennung der verschiedenen Nutzergruppen der Deutsche Telekom AG kommt im gesamten Backbone das Verfahren Multi Protocol Label Switching (MPLS) zum Einsatz. Ebenso sind netzweit so genannte Quality of Service (QoS) Mechanismen implementiert, um zeit- oder verlustkritischen Kundenapplikationen entsprechend optimierte Übertragungsparameter zur Verfügung zu stellen.

T-Systems ES nutzt derzeit fünf der PoP-Standorte zur Realisierung der Übertragungsleistung des KNSH. Diese Standorte sind Hamburg, Lübeck, Kiel und Flensburg. Der PoP Schwerin wird ausschließlich für das Ersatzrouting im Fehlerfall der Strecke Hamburg-Lübeck benötigt.



Horst Rischbode, T-Systems Enterprise Services GmbH
Network Solutions & Service Management

Abb.: MPLS-Backbone Schleswig-Holstein

2.5.3 Anschlussleitung

Die Anschlussleitungen stellen die Verbindung der einzelnen KNSH-Standorte zu den PoP-Standorten des Backbones her. Derzeit werden auf der Anschlussleitung je nach Nutzungsanforderung symmetrische Übertragungsverfahren wie HDLC (High Data Level Link Control) bzw. SDSL (Symmetric Digital Subscriber Line) oder asymmetrische Übertragungsverfahren wie ADSL (Asymmetric Digital Subscriber Line) eingesetzt. Anders als in Einwahlnetzen von Internet Service Providern kommt eine fest geschaltete Verbindung zwischen PoP und Kundenstandort zum Einsatz. Es findet also keine dynamische Vergabe von IP-Adressen statt, sondern es besteht eine Punkt-zu-Punkt-Verbindung zwischen dem PoP und dem Kunden-Standort mit fest zugeordneten IP-Adressen der jeweiligen Kommunikationspartner.

2.5.4 Zugangsrouter

Der Zugangsrouter stellt mehrere Funktionen bereit. Er bildet die benötigten Zugangsschnittstellen für einen KNSH-Standort und ordnet diese den verschiedenen MPLS-VPN zu. Des Weiteren stellt er die Schnittstelle und geeignete Übertragungsverfahren für die Anschlussleitungen zur Verfügung. Zusätzlich übernimmt der Zugangsrouter die Qualifizierung und Zuordnung zu verschiedenen Verkehrsklassen der über die Kundenschnittstelle eintreffenden Datenpakete und sorgt für die priorisierungsgerechte Weiterleitung dieser Pakete.

2.5.5 MPLS-VPN

Auf Basis des MPLS-Verfahrens werden dem Finanzministerium verschiedene Virtual Private Networks (MPLS-VPN) angeboten. Diese MPLS-VPN erlauben eine vollständige logische Trennung des Datenverkehrs von verschiedenen Teilnehmergruppen. Derzeit besteht das KNSH aus 33 unabhängigen MPLS-VPN, die exklusiv dem Finanzministerium zur Bildung von geschlossenen Benutzergruppen (GBG) angeboten werden. Dabei sind 32 MPLS-VPN dem reinen Datentransport vorbehalten. Ein MPLS-VPN steht exklusiv dem Transport von Voice Paketen mit der Technik Voice over IP (VoIP) zur Verfügung.

Das Finanzministerium legt mit der Auftragserteilung einer Zugangsschnittstelle fest, welchem MPLS-VPN diese Zugangsschnittstelle zugeordnet werden soll. Alle Datenpakete, die dieser Zugangsschnittstelle von Kundenseite angeliefert werden, sind diesem MPLS-VPN zuzuordnen.

2.5.6 Quality of Service

Innerhalb der MPLS-VPN, die dem Datentransport vorbehalten sind, stehen dem Finanzministerium verschiedene Verkehrsklassen zur Verfügung. Zwischen den folgenden Verkehrsklassen wird unterschieden:

- Standard: Best-Effort-Transport ohne Qualitätsparameter
- Premium: Priorisierter Transport mit Qualitätsparametern
- Multimedia: Priorisierter Transport mit Qualitätsparametern

Die Verkehrsklasse Multimedia ist qualitativ über der Verkehrsklasse Premium angesiedelt und ermöglicht den priorisierten Transport von Datenpaketen, die sowohl zeit- als auch verlustkritischen Applikationen zur Kommunikation dienen.

2.5.7 Voice-Transport

Das KNSH bietet ein MPLS-VPN exklusiv zur Übertragung von Voice-Paketen auf Basis der Voice over IP (VoIP) Technologie. Dieses dient der Kopplung der TK-Systeme der angeschalteten Organisationseinheiten.

Jeglicher Verkehr, der über die dazu bereitgestellten Zugangsschnittstellen an das MPLS-VPN Voice des KNSH herangeführt wird, wird in der Verkehrsklasse Voice übertragen. Diese ist qualitativ über den Verkehrsklassen Standard, Premium und Multimedia angesiedelt.

Zur Realisierung des Voice-Transports zwischen klassischen TK-Systemen muss eine Umsetzung der angelieferten Signale auf IP-Pakete erfolgen. Diese Aufgabe übernehmen die H.323-Voice-Gateways. Um den technischen und organisatorischen Aufwand zu minimieren, streben die Vertragspartner Finanzministerium und T-Systems ES an, je nach technischem Leistungsstand der zur Verfügung stehenden Komponenten und der betriebswirtschaftlichen Umsetzbarkeit die Funktion der H.323-Voice-Gateways in die Komponente Zugangsrouter zu überführen. Diese Designänderung ist anzeigepflichtig gegenüber dem Finanzministerium.

2.5.8 Geschlossene Benutzergruppen (GBG)

Die technische Grundlage einer GBG bildet das MPLS-Verfahren. Die physikalische Separierung der MPLS-VPN erfolgt am Zugangsrouter der T-Systems ES. Über die Zugangsschnittstellen werden die GBG beim Nutzer durch den Übergaberouter und an zentraler Stelle durch die Verbindungsfirewall abgeschlossen. Das Finanzministerium legt mit der Auftragserteilung einer Zugangsschnittstelle fest, welchem MPLS-VPN diese Zugangsschnittstelle zugeordnet werden soll. Alle Datenpakete, die dieser Zugangsschnittstelle angeliefert werden, sind somit einem MPLS-VPN zugeordnet.

Durch die Bildung einer GBG wird eine zweckmäßige Administration und effektive Abschottung von Nutzergruppen im Landesnetz erreicht. Für das Landesnetz werden GBG bereitgestellt, um

- organisatorische oder anwendungsspezifische Gruppierungen zu erlauben,
- eine Lastverteilung an den Übergabeeinrichtungen zu erreichen,
- Filtereinstellungen nutzerspezifisch umzusetzen und
- Transparenz und Klarheit in die Struktur des Landesnetzes zu bringen.

Die GBG-übergreifende Kommunikation erfolgt nur über die zentrale Verbindungsfirewall. Ein vom Nutzer ernannter Kommunikationskoordinator beauftragt Dataport mit der Einrichtung der Kommunikationsparameter zur Umsetzung einer GBG-übergreifenden Kommunikation.

2.5.9 Verbindungsfirewall

Die Verbindungsfirewall besteht aus einer Zusammenschaltung von Firewalls der Firma Cisco (PIX-Firewall). Die Funktionen der PIX-Firewalls enthalten umfangreiche und integrierte Sicherheitsdienste. Die physikalische Anbindung des Landesnetzes an die PIX-Firewalls erfolgt über dedizierte physikalische Ports. Jede GBG hat genau einen Port an einer PIX-Firewall. Die dem Landesnetz abgewandten Schnittstellen der PIX-Firewalls sind durch einen gemeinsamen Switch im Rechenzentrum (RZ) verbunden. Über diesen Switch erfolgt die GBG-übergreifende Kommunikation falls zwei Kommunikationspartner nicht an derselben PIX-Firewall angebunden sein sollten. Außerdem bindet dieser Switch die von Dataport angebotenen Dienste an das Landesnetz an.

Die Einstellung der Kommunikationsparameter erfolgt durch das Werkzeug „NetSPoC“. Abweichungen sind nur im Rahmen der Störungsbeseitigung zulässig. Die PIX-Firewalls sind so konfiguriert, dass Zugriffe ausschließlich aus dem Administrationssegment bei Dataport möglich sind. Bei der Erstinstallation und im Störungsfall werden Zugriffe über die Konsole am Standort der Systeme im Dataport-Rechenzentrum (RZ) Altenholz durchgeführt.

2.5.10 Übergaberouter

Jeder Nutzer erhält einen durch Dataport bereitgestellten Übergaberouter. Je nach Anschlussanforderung können unterschiedliche Gerätetypen zum Einsatz kommen. Die grundsätzlichen Funktionalitäten sind jedoch gleich. Die Hardwarebasis des Übergaberouters ist ein Router der Firma Cisco. Dieser ist im Landesnetzschrank (19“-Schrank) zugangsgesichert beim Nutzer eingebaut.

Der Übergaberouter ist die Basis für die Überwachung und Visualisierung der Betriebseigenschaften des Landesnetzes für das Finanzministerium und jeden Nutzer und damit notwendiges Betriebselement. Er übernimmt folgende Aufgaben und Funktionen:

- Schutz des LAN des Nutzers vor nicht beauftragter Kommunikation aus dem Landesnetz,

- Schutz des Landesnetzes vor dem LAN des Nutzers und

- Bereitstellung und Überwachung der Übergabeschnittstellen zum LAN des Nutzers und dem Zugangsrouter von T-Systems ES.

Der Übergaberouter stellt zum Zugangsrouter und zum LAN des Nutzers Schnittstellen bereit. Auf allen Routern ist als Betriebssystem das Cisco IOS im Einsatz. An dem Übergaberouter ist das LAN des Nutzers unmittelbar angeschlossen. Die Nutzer erhalten die Möglichkeit, sich durch ein Revisionstool „LandesNetzRouterControl“ (LNRC) zeitnah über Änderungen der Routerkonfiguration ihres jeweiligen Übergaberouters zu informieren.

2.5.11 Berichtswesen und Kontrolle

Die Nutzer beauftragen Dataport mit der Administration der Kommunikationsparameter. Entscheidend ist dabei, dass die Nutzer die korrekte Umsetzung ihrer Aufträge kontrollieren können und dass die Arbeit von Dataport im Rahmen einer Revision überprüft werden kann.
Das Berichtswesen hat zum Ziel, die Umsetzung der Aufträge transparent, lesbar und verständlich darzustellen. Die Berichte enthalten Informationen über Kommunikationsparameter zwischen Nutzern des LN untereinander sowie die Kommunikationsparameter zwischen Nutzern des LN und Dataport.

Berichtsempfänger sind jeweils die Kommunikationskoordinatoren und die Nutzer, für die ein Kommunikationskoordinator tätig ist, sofern keine abweichende Vereinbarung zwischen Nutzer und Koordinator existiert. Alle Berichtsempfänger sind in einer Standortliste aufgeführt. Inhalt und Form der Berichte sind zwischen dem FM und Dataport vereinbart. Änderungen sind nur im Auftrag oder mit Einverständnis des FM zulässig.

Der Nutzer wird nach der Erstbeauftragung seines Anschlusses über die tatsächlich eingestellten Kommunikationsbeziehungen im Wege des Berichtswesens unterrichtet, so dass er seinen Auftrag mit den tatsächlichen Einstellungen vergleichen kann.

Einmal täglich wird nachts die Konfiguration der Kommunikationsbeziehungen der definierten Netzkomponenten im Landesnetz automatisiert durch ein Programm abgeholt und aus ihnen Berichte generiert. Die erzeugten Dateien werden versionsverwaltet gespeichert, so dass ein Vergleich mit dem Stand des Vortages möglich ist. Bei Abweichungen wird automatisch ein neuer Bericht generiert und per E-Mail an den zuständigen Kommunikationskoordinator versendet, so dass die Berichte den Empfängern am nächsten Morgen zur Kontrolle vorliegen. Für die erzeugten Berichte existiert eine Historie über einen Zeitraum von mindestens vier Wochen.

Es besteht für das Sicherheitsmanagement die Möglichkeit, Kommunikationseinstellungen von der Beauftragung über die technische Umsetzung bis zur aktiven Nutzung zu kontrollieren.

2.6 Landesnetzmanagement

2.6.1 T-Systems ES

Das Netzwerkmanagement der Deutschen Telekom AG wird für das KNSH an den Standorten Ulm und Stuttgart ausgeführt. Es gliedert sich in die Bereiche Konfigurationsmanagement und Faultmanagement. Zu den Aufgaben des Netzmanagements gehören:

- Einrichtung und Änderung der Servicedaten auf Port- und Knotenebene,
- Durchführung von Software-Upgrades,
- Erfassung von Alarmen und Systemmeldungen sowie
- Eingrenzung und Beseitigung von Störungen.

Durch eine regelmäßige Überprüfung der zentralen Netzfunktionen und Bewertung des Netzverhaltens wird die Netzqualität sichergestellt. Alle aktiven Komponenten des KNSH werden über das Konfigurationsmanagement verwaltet.

Das Faultmanagement umfasst sowohl die Netzplattform des MPLS-Backbones, bestehend aus Vermittlungsrechnern, Verbindungsleitungen und den peripheren und zentralen Steuerungssystemen, als auch die Zugangs- und Backbonerouter sowie Voice-Gateways des KNSH.
Alle Meldungen der aktiven Komponenten des KNSH (z.B. SNMP-Informationen) werden von den Administratoren zur Fehlererkennung herangezogen. Die ständige Auswertung und Bewertung der Meldungen durch die Administratoren ermöglicht eine schnelle Einleitung von Folgemaßnahmen. Nach Erkennen einer Störung erfolgt unverzüglich eine Störungseingrenzung durch Systemabfragen und Evaluierung der Konfigurationsparameter auf Plattform- und Zugangs- bzw. Backbonerouterebene. Das Faultmanagement behebt die Störung, sofern die Ursache im Konfigurationsbereich des Zugangsrouters oder der Netzplattform des MPLS-Backbones angesiedelt ist.

Administrative Zugriffe auf die aktiven Komponenten (z.B. zum Zwecke des Konfigurationsmanagements) werden über ein TACACS+ - System realisiert. Jeder Administrator wird über eine eindeutige Kennung identifiziert. Der Personenkreis der Administratoren ist auf das erforderliche Mindestmaß begrenzt. Administrative Zugriffe und Aktionen werden entsprechend einer Konzernrichtlinie der Deutsche Telekom AG protokolliert und archiviert.

2.6.2 Dataport

Im Landesnetz werden von Dataport die Übergaberouter bei den Nutzern sowie die Verbindungsfirewall im Rechenzentrum von Dataport administriert.

Die Administration bezieht sich auf das Update der Betriebssysteme, die Erstinstallation und Fortschreibung der Kommunikationsparameter sowie die Entstörung und Überwachung.

Die Erstinstallation und Fortschreibung der Kommunikationsparameter geschieht, indem auf den Übergaberoutern und der Verbindungsfirewall Filterregeln konfiguriert werden. Der administrative Zugriff erfolgt automatisiert per Fernkonfiguration oder in Notfällen über den Konsolenport am Gerät.

Für das Landesnetz sind von Dataport die folgenden Netzwerkmanagementleistungen implementiert:

- Verfügbarkeitsüberwachung („Lebendüberwachung“) der Netzwerk-Komponenten über ein regelmäßiges Polling,

- Ereignis-Management, Alarmierung (Generierung Trouble-Ticket) und die Veranlassung von Aktionen bei bestimmten Ereignissen,

- Monitoring im Störungsfall oder zur Untersuchung von neu ins Netz eingebundenen Komponenten,

- Konfiguration von Netzwerkkomponenten über zentrale Mechanismen,

- Dokumentation des Netzes, der Geräte und der sie verbindenden Leitungen,

- Administration und Konfiguration der aktiven Netzwerkkomponenten,

- Speicherung der im Netzwerk eingesetzten Betriebssysteme und Konfigurationsdateien der aktiven Netzwerkkomponenten,

- Messungen ausgewählter Parameter des Netzwerkes, um Aussagen über den Zustand und die Auslastung der Leitungen und der Geräte treffen zu können,

- Aufstellung von Statistiken (Ausfall, Auslastung, Auftreten spezieller Ereignisse),

- Überwachung der Verfügbarkeiten der Netzkomponenten,

- Alarmierungen bei Über- oder Unterschreiten von kritischen Parametern,

- Zugangsbeschränkung für die Konfiguration der aktiven Netzwerkkomponenten und der Netzwerkmanagementsysteme,

- Dokumentation (Change-Audit) der an den aktiven Netzwerkkomponenten getätigten Änderungen und der im Netzwerk aufgetretenen Ereignisse.

Für den Nutzer des Landesnetzes stellt Dataport den Webdienst LNWeb-View zur Verfügung. Hier findet der Nutzer Leistungs- und Konfigurationsdaten sowie betriebliche Informationen zu seinem Anschluss.

2.7 Verträge und Vereinbarungen

2.7.1 Betreibervertrag zwischen Finanzministerium und Dataport

Zwischen dem Finanzministerium und Dataport wurde ein Vertrag über den Betrieb des Landesnetzes Schleswig-Holstein am 7.12.2000 geschlossen („Betreibervertrag“). Seit der Inbetriebnahme hat das Landesnetz eine Vielzahl technischer und organisatorischer Fortentwicklungen erfahren, so dass der Betreibervertrag durch so genannte „Nachträge“ ergänzt worden ist. Die Regelungen aus den Nachträgen wurden mit dem Ursprungsvertragstext zu einer konsolidierten „Lesefassung“ zusammengefasst.

2.7.2 Verträge zwischen Finanzministerium und T-Systems ES

Das Kabinett des Landes Schleswig-Holstein hat am 16.06.1999 entschieden, das Projekt „Landessprachnetz“ zu realisieren. Das zuständige Finanzministerium hat T-Systems ES mit der Planung, den Aufbau und den Betrieb einer landesweiten Kommunikationsinfrastruktur für Sprache für alle Dienststellen des Landes beauftragt. Der Leistungsumfang umfasste zunächst, den Telekommunikationspark des Landes grundlegend zu modernisieren und zu einem landesweiten Sprachnetz zu erweitern. Die Vereinbarungen wurden seinerzeit in einem Rahmenvertrag festgelegt.

Auf der Basis des Kabinettsbeschluss des Landes Schleswig-Holstein vom am 22.02.2000 zur Errichtung einer einheitlichen Netzplattform für Sprach- und Datendienste und zur Vernetzung der Landesdienststellen haben die Vertragsparteien den Vertrag „TDN Land 2“ abgeschlossen. Ergänzend regeln die Parteien in dem Rahmenvertrag „Privacy Sprach- und Datennetz“ die spezifischen Anforderungen an den Datenschutz und die Datensicherheit für die im Rahmen des KNSH zu erbringende Datenverarbeitung. Der Vertrag konkretisiert insbesondere die datenschutzrechtlichen Erfordernisse der Auftragsdatenverarbeitung nach § 17 LDSG.

2.7.3 Ausführungsbestimmungen für Landesbehörden

In Ausführungsbestimmungen hat das Finanzministerium für die Landesbehörden den Anschluss an das Landesnetz geregelt. Mit Schreiben vom 28. Juli 2006 hat der zuständige Leiter der Abteilung V des Finanzministeriums die Generaldokumentation mit dem Status einer Ausführungsbestimmung im Sinne der IT-Richtlinien versehen und sie zum 1. August 2006 in Kraft gesetzt. Gleichzeitig wurden die bisherigen „Rahmenbedingungen (Organisation, Technik und Betrieb) Version 17 Stand 20.12.2000“ sowie die „Anschlussbedingungen und Leistungen Version 14 Stand 20.12.2000“ aufgehoben.

Die Regelungen der Generaldokumentation sind somit für die Landesbehörden verpflichtend und deshalb von ihnen einzuhalten.

2.7.4 Nutzervertrag für Kommunalbehörden und sonstige Stellen

Der Nutzervertrag regelt die Nutzung des Landesnetzes zwischen dem Land (Finanzministerium) und den Kommunen bzw. ihren Einrichtungen (LN-Nutzer). Das Finanzministerium stellt dem LN-Nutzer folgende Leistungen zur Verfügung:

- Anschluss an das Landesnetz,
- Kontrollmöglichkeiten über seine Kommunikationsparameter,
- Einstellungen der von ihm beauftragten Kommunikationsbeziehungen,
- die von ihm beauftragte Bandbreite sowie

- die Umsetzung organisatorischer und technischer Sicherheitsmaßnahmen.

Der LN-Nutzer benennt für die Ausführung der Leistungen einen Kommunikationskoordinator.

2.8 Generaldokumentation des Landesnetzes

Die Dokumentation des LN wurde im Rahmen des Auditprozesses in einem erheblichen Umfang ergänzt und in eine modulare und damit übersichtliche Form gebracht.

Die Generaldokumentation des Landesnetzes bildet auf einem hohen qualitativen Niveau die technische und organisatorische Grundlage für die Verfahrensweise und die Arbeitsabläufe im Landesnetz. Sie beinhaltet die ganzheitliche Sicht der Prozesse für das Landesnetz Schleswig-Holstein aus Kunden- und Betreibersicht für den Transport von Daten über das Landesdatennetz und besteht aus folgenden Komponenten:

- Teil 1: Beschreibung der IT-Systeme
- Teil 2: Sicherheitskonzept
- Teil 3: Weiterführende Dokumentation
- Teil 4: Verträge mit Dataport
- Teil 5: Verträge mit T-Systems ES
- Teil 6: Verträge mit den Nutzern

Die Generaldokumentation entspricht den Anforderungen der Datenschutzverordnung.

3 Datenschutz-Managementsystem im laufenden Betrieb

3.1 Sicherheitsziele

Das Finanzministerium hat für das Landesnetz Sicherheits- und Datenschutzziele formuliert, die durch geeignete Sicherheitsmaßnahmen und ein angemessenes Sicherheitsmanagement erreicht werden müssen.

Alle Komponenten des Landesnetzes müssen ein einheitliches, hohes Sicherheitsniveau bereitstellen. Das Sicherheitsniveau wird bezüglich des Schutzes der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit der über das Landesnetz übermittelten Daten ermittelt**.**

Zur Erreichung dieses Sicherheitsniveaus stellt das Finanzministerium als Betreiber Sicherheitsdienstleistungen bereit. Diese Dienstleistungen werden anteilig von Dataport und T-Systems ES erbracht.

3.2 Sicherheitskonzept

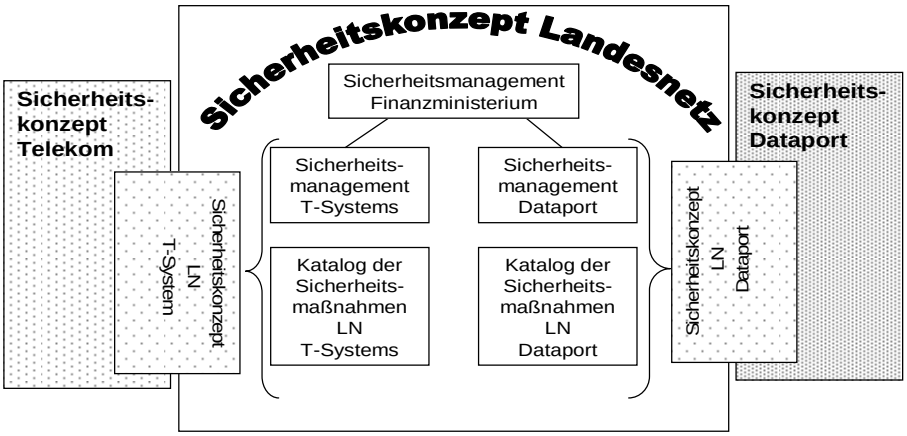
3.2.1 Übergreifendes Sicherheitskonzept des Finanzministeriums

Das Finanzministerium stellt in einem übergreifenden Sicherheitskonzept dar, welche technischen und organisatorischen Maßnahmen getroffen wurden, um insbesondere die Anforderungen der §§ 5 und 6 LDSG zu erfüllen.

Das übergreifende Sicherheitskonzept des Finanzministeriums besteht aus folgenden Konzepten und Dokumenten:

- dem Sicherheitsmanagement des Finanzministeriums
- dem Sicherheitsmanagement der Dienstleister
- dem Katalog der Sicherheitsmaßnahmen (KdS) des Finanzministeriums und der Dienstleister für das Landesnetz
- den Sicherheitskonzepten der Dienstleister

Eine dem Konzept für das übergreifende Sicherheitsmanagement entnommene Grafik verdeutlicht das Zusammenführen der unterschiedlichen Konzepte und Prozesse in der Sicherheitskonzeption des Finanzministeriums:



In den nachfolgenden Abschnitten wird jeweils detailliert auf die Sicherheitskonzepte der Dienstleister Dataport und T-Systems ES eingegangen. Insbesondere werden dort die für die Auditierung entscheidenden Sicherheitsmaßnahmen kurz aufgeführt.

Das Finanzministerium hat über die Sicherheitsmaßnahmen der Dienstleister des Landesnetzes hinaus eigene Sicherheitsmaßnahmen definiert:

- Das Finanzministerium hat für das Landesnetz ein Sicherheitsmanagement eingerichtet.

- Zur Kontrolle der Leistungserbringung, insbesondere der Sicherheitsmaßnahmen, werden durch das Finanzministerium als Auftraggeber regelmäßige Audits im Abstand von maximal zwei Jahren im Wirkungsbereich der Dienstleister durchgeführt. Die Ergebnisse der Audits werden in der Sicherheitsdokumentation dokumentiert.

- Zur Behandlung von Sicherheitsvorfällen besteht ein Konzept mit detaillierten Vorgaben zur Bearbeitung und Dokumentation von Sicherheitsvorfällen. Insbesondere werden auch unvorhergesehene Ereignisse, für deren Behandlung keine konkrete Vereinbarung getroffen wurde, als Sicherheitsvorfälle behandelt.

- Die Herstellung von Kommunikationsbeziehungen müssen vom Nutzer beauftragt werden. Das Finanzministerium verpflichtet deshalb die Nutzer, einen Kommunikationskoordinator verbindlich zu benennen, von dem der Beauftragungsprozess ausgeht. Der Nutzer und sein Kommunikationskoordinator werden über den Beauftragungsprozess in Kenntnis gesetzt. Die Änderungen werden ihnen im Rahmen des Berichtswesens schriftlich mitgeteilt.

- Direkte Verbindungen mit dem Internet über das Landesnetz können durch die Nutzer nicht beauftragt werden.

- Verbindungen mit Netzen, die nicht zu einem Nutzer gehören und nicht von Dataport verwaltet werden, müssen vom Finanzministerium insbesondere unter Sicherheitsgesichtspunkten geprüft und genehmigt werden.

3.2.2 Sicherheitskonzept Dataport

Dataport stellt in der Generaldokumentation des Landesnetzes, insbesondere im „Katalog der Sicherheitsmaßnahmen“ und im Konzept zum Sicherheitsmanagement Dataport dar, mit welchen Sicherheitsmaßnahmen die Sicherheitsziele des Finanzministeriums umgesetzt werden.

- Dataport stellt über ein landesnetzspezifisches Sicherheitsmanagement sicher, dass die für den Auditprozess wesentlichen Sicherheitsmaßnahmen umgesetzt werden. Darüber hinaus wird durch ein etabliertes Sicherheitsmanagement die Weiterentwicklung und Anpassung der Sicherheitsorganisation auf geänderte Rahmenbedingungen oder Nutzeranforderungen sichergestellt.

- Dataport etabliert durch eine Reihe von beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen ein der jeweiligen Landesnetzkomponente angemessenes Sicherheitsniveau bezüglich der physikalischen Sicherheit.

- Dataport stellt durch beschriebene geeignete technische und organisatorische Sicherheitsmaßnahmen sicher, dass ein unerlaubter Zugriff auf Systeme des Landesnetzes erkannt und verhindert wird.

- Dataport stellt die Zuverlässigkeit der Mitarbeiter initial durch eine Sicherheitsüberprüfung sicher. Alle Mitarbeiter werden auf die Einhaltung der Datenschutzgesetzgebung hingewiesen, entsprechend geschult und verpflichtet. Die jeweiligen Vorgesetzten kontrollieren die Einhaltung der landesnetzspezifischen Vorgaben sowie der hierzu erlassenen internen Arbeitsanweisungen.

- Dataport hat einen definierten Prozess zur Bearbeitung von Sicherheitsvorfällen eingerichtet. Eine Integration in das übergreifende Sicherheitsmanagement des Finanzministeriums ist sichergestellt.

- Dataport hat für die Administration der Landesnetzkomponenten funktionsfähige Revisionsmechanismen etabliert.

- Das Bereitstellen von Kommunikationsverbindungen erfolgt nur nach Beauftragung durch den Landesnetz-Nutzer. Hierzu hat Dataport einen standardisierten Prozess zur Bearbeitung der Aufträge und zur Dokumentation etabliert.

- Den Nutzern des Landesnetzes stehen mit dem Berichtswesen sowie dem LNRC Revisionsinstrumente zur Verfügung, um unabhängig von Dataport die korrekte Bearbeitung der Aufträge und der Administration der Übergaberouter zu kontrollieren.

- Sämtliche Konfigurationsänderungen werden seitens Dataport nicht manuell, sondern durch einen automatisierten Prozess gesteuert. Die Erzeugung der für die Kommunikationsverbindungen notwendigen Konfigurationsdirektiven sowie das Übertragen und Aktivieren auf den jeweiligen Komponenten erfolgt programmbasiert.

3.2.3 Sicherheitskonzept T-Systems ES

T-Systems ES stellt in einem Sicherheitskonzept dar, welche Sicherheitsmaßnahmen durch T-Systems ES und seine Unterauftragnehmer – insbesondere T-COM – getroffen wurden, um einen sicheren Betrieb des Landesnetzes zu gewährleisten.

- T-Systems ES stellt über ein Sicherheitsmanagement bei T-Systems ES mit definierter Integration in das konzernweite Sicherheitsmanagement

sicher, dass die für den Auditprozess wesentlichen Sicherheitsmaßnahmen umgesetzt werden. Darüber hinaus wird durch ein etabliertes Sicherheitsmanagement die Weiterentwicklung und Anpassung der Sicherheitsorganisation auf geänderte Rahmenbedingungen oder Nutzeranforderungen sichergestellt.

- T-Systems ES hat durch vertragliche Regelungen sichergestellt, dass Sicherheitsvorgaben des Finanzministeriums auch bei den Unterauftragnehmern T-Systems Business Services GmbH (T-Systems BS) und T-COM durchgesetzt werden.

- T-Systems ES, T-Systems BS und T-COM etablieren durch eine Reihe von Sicherheitsmaßnahmen ein der jeweiligen Landesnetzkomponente angemessenes Sicherheitsniveau bezüglich der physikalischen Sicherheit.

- T-Systems ES stellt durch geeignete Sicherheitsmaßnahmen sicher, dass ein unerlaubter Zugriff auf Systeme des Landesnetzes erkannt und verhindert wird.

- Alle Mitarbeiter werden auf die Einhaltung der Datenschutzgesetzgebung hingewiesen, entsprechend geschult und verpflichtet.

- T-Systems ES hat einen definierten Prozess zur Bearbeitung von Sicherheitsvorfällen eingerichtet. Eine Integration in das übergreifende Sicherheitsmanagement des Finanzministeriums ist ebenso sichergestellt wie eine funktionierende Kopplung der Sicherheitsmanagementprozesse von T-COM, T-Systems BS und T-Systems ES.

- Die Unterauftragnehmer T-Systems BS und T-COM führen im Rahmen des Telekom-weiten Sicherheitsprozesses jährlich regelmäßige und anlassbezogene Audits des gesamten Backbones inklusive der für das Landesnetz relevanten Komponenten durch.

- T-Systems ES führt zumindest jährlich regelmäßige Audits bezüglich der Umsetzung der Sicherheitsvorgaben des Finanzministeriums, der eigenen Sicherheitsmaßnahmen und der funktionierenden Sicherheitskonzeption der konzern-internen Dienstleister durch.

- T-Systems ES, T-Systems BS und T-COM nutzen für die koordinierte Bearbeitung von Sicherheitsvorfällen einen standardisierten und koordinierten Prozess.

- T-Systems ES, T-Systems BS und T-COM nutzen standardisierte Beauftragungs- und Änderungsprozesse sowohl für die Bearbeitung von Aufträgen des Finanzministeriums als auch für die interne Betriebssteuerung.

3.3 Sicherheitsmanagement

Das Finanzministerium hat zur Wahrnehmung der Aufgaben und Durchführung oder Kontrolle der notwendigen Prozesse die Rolle des Sicherheitsmanagers eingerichtet.

Der Sicherheitsmanager prüft und bewertet die für das Landesnetz getroffenen Sicherheitsmaßnahmen in Hinblick auf ihre Angemessenheit.

Der Sicherheitsmanager ist zuständig

- für die Einhaltung der für das Landesnetz getroffenen Sicherheitsmaßnahmen,

- für die Kontrolle und Aufsicht der im Betrieb des LN eingebundenen Auftragnehmer,

- für die Organisation der Sicherheitsmanagementprozesse,

- für die Bearbeitung von Sicherheitsvorfällen,

- für das Führen und Fortschreiben der Generaldokumentation,

- für das Durchführen bzw. Veranlassen von Kontrollen bzw. Audits gegenüber den Dienstleistern.

Der Sicherheitsmanager führt in einem regelmäßigen Turnus präventive Prüfungen und Audits durch, um die Umsetzung, Wirksamkeit und Praktikabilität der im Sicherheitskonzept getroffenen Sicherheitsmaßnahmen für das

Landesnetz oder einzelner Komponenten zu überprüfen. Der Sicherheitsmanager kann sich für Prüfungen und Audits unabhängiger Dritter bedienen.

Der Sicherheitsmanager des Finanzministeriums arbeitet mit den Sicherheitsbevollmächtigten der Dienstleister Dataport und T-Systems ES zusammen.

4 Datenschutzrechtliche Bewertung

4.1 Daten verarbeitende Stelle

Das Land Schleswig-Holstein betreibt durch das Finanzministerium ein Datennetz als Kommunikationsinfrastruktur (Landesnetz) für die öffentliche Verwaltung in Schleswig-Holstein. Die Zuständigkeit ergibt sich aus dem Organisationserlass der Ministerpräsidentin über die Geschäftsverteilung der Landesregierung vom 8. Juli 2003. Darin wird dem Finanzministerium die Zuständigkeit für das Ressort übergreifende strategische und operative IT-Management sowie für die zentralen Komponenten und Services der IT-Infrastruktur der Landesverwaltung übertragen. Aus der Vereinbarung zur gemeinsamen Entwicklung von E-Government-Strukturen und –Prozessen zwischen dem Finanzministerium und den Kommunalen Landesverbänden ergibt sich für das Finanzministerium ebenfalls die Zuständigkeit für den Aufbau einer landesweit standardisierten Plattform für Datenkommunikation.

Das Finanzministerium ist deshalb als Betreiber befugt, die von den angeschlossenen Nutzern (siehe Tz. 2.4) über das Landesnetz kommunizierten Daten zu übertragen und damit auch für diesen Zweck zu verarbeiten.

Das Finanzministerium ist als Betreiber des Landesnetzes Daten verarbeitende Stelle i.S.d. Landesdatenschutzgesetzes und insoweit datenschutzrechtlich für die Ordnungsmäßigkeit der Datenübertragung und der hierzu erforderlichen Administration des Landesnetzes verantwortlich. Hingegen sind die am Landesnetz angeschlossenen Nutzer für die Recht- und Ordnungsmäßigkeit der von ihnen übermittelten personenbezogenen Daten verantwortlich. Die Betreiberverantwortung für das Landesnetz liegt demnach beim Finanzministerium, während die Datenverantwortung bei den Nutzern anzusiedeln ist.

4.2 Auftragsdatenverarbeitung

Das Finanzministerium ist als Auftraggeber mit der Vergabe der Datenverarbeitung an seine Dienstleister für die Einhaltung der bereichsspezifischen Gesetze und der Datenschutzvorschriften verantwortlich. Es hat vertraglich sichergestellt, dass auch seine Dienstleister als Auftragnehmer diese Anforderungen erfüllen. Im Rahmen der Auftragsdatenverarbeitung hat das Finanzministerium dafür Sorge getragen, dass der Betrieb des Landesnetzes nur im Rahmen seiner Weisungen ausgeführt wird. Das Finanzministerium hat seine Auftragnehmer verpflichtet, jederzeit von ihr veranlasste Kontrollen zur Einhaltung der gebotenen technischen und organisatorischen Maßnahmen zu ermöglichen.

Mit der Einrichtung eines Datenschutz- bzw. Sicherheitsmanagements hat das Finanzministerium Strukturen geschaffen, die eine sachkundige Kontrolle seiner Dienstleister ermöglichen (vgl. Tz. 3). Das für das Landesnetz festgelegte Sicherheitsniveau kann auf diese Weise dauerhaft aufrechterhalten werden.

4.3 Zusammenfassende Bewertung

Die Überprüfungen vor Ort haben ergeben, dass die in dem Sicherheitskonzept festgelegten Sicherheitsmaßnahmen umgesetzt wurden.

Die mit dem Audit „Landesnetz“ erfassten Verarbeitungsprozesse zeichnen sich insbesondere durch folgende „datenschutzfreundliche“ Aspekte aus:

1. Mit dem Einsatz der MPLS-Technologie und der Einrichtung redundanter Netzkomponenten wird durch den Netzbetreiber T-Systems ES hinreichend sichergestellt, dass während des Transports der Daten über das Landesnetz die Verfügbarkeit, Vertraulichkeit und die Integrität sowie der Ordnungsmäßigkeit der Datenverarbeitung gewährleistet werden.

2. Dataport stellt sicher, dass die im Landesnetz eingesetzten Übergaberouter und die Verbindungsfirewall nach den Kommunikationsparametern der Nutzer ordnungsgemäß administriert werden.

3. Sicherheitsrelevante Ereignisse können über das automatisierte Berichtswesen sowie den Einsatz eines Revisionstools (LNRC) von den

Administratoren der Landesnetznutzer rechtzeitig erkannt und ausgewertet werden.

4. Die technischen und organisatorischen Abläufe im Landesnetz werden in der Generaldokumentation vollständig beschrieben.

5. Das Finanzministerium hat für die Aufrechterhaltung eines dauerhaft hohen Gesamtsicherheitsniveaus ein Datenschutz- bzw. Sicherheitsmanagement integriert, das eine umfassende Qualitätssicherung der sicherheitsrelevanten Landesnetzeigenschaften betreibt und auf eventuell auftretende Sicherheitsvorfälle zeitnah reagiert.

Alle von Dataport und T-Systems ES getroffenen Sicherheitsmaßnahmen sind in dem „Katalog der Sicherheitsmaßnahmen im Landesnetz“ (KdS) festgelegt und damit Bestandteil des Sicherheitskonzepts Landesnetz. Das Landesnetz ist für den Nutzer als abgeschlossenes Netzwerk einzustufen, in dem seine Daten unverschlüsselt, aber isoliert von anderen Nutzern transportiert werden. Ein erhöhter Schutzbedarf ist in der Verantwortung des Nutzers dann festzulegen, wenn von ihm die in der Sicherheitsanalyse beschriebenen Restrisiken als nicht ausreichend bewertet werden.

Aufgrund der Prüfung des Datenschutz-Management kann die Verleihung des Auditzeichens an das Finanzministerium als Betreiber des Landesnetzes erfolgen.