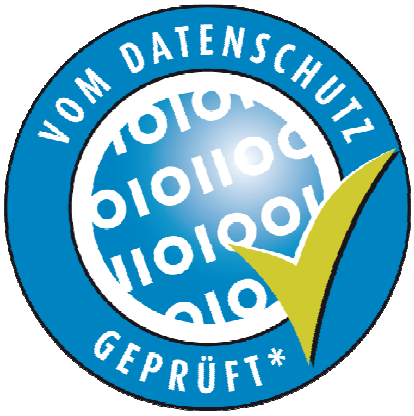


Kurzgutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Kommunales Kommunikationsnetz

der

Kreisverwaltung Plön

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Datum : 26.11.2007
Aktenz. : 16.01/05.007
Telefon : 0431 988 1200
Fax : 0431 988 1223
E-Mail : mail@datenschutzzentrum.de

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Audits

Das Unabhängige Landeszentrum für Datenschutz (ULD) und die Kreisverwaltung Plön haben vereinbart, das „**Kommunale Kommunikationsnetz der Kreisverwaltung Plön**“ (Kreisnetz Plön) zu auditieren. Bei dem Kreisnetz Plön handelt es sich um eine netztechnische Infrastruktur auf der Plattform des so genannten “Kommunikationsnetzes Schleswig-Holstein – KNSH“[1] der Telekommunikationsfirma T-Systems Enterprise Services GmbH[2] über das Daten direkt zwischen den Kommunen des Kreises Plön und der Kreisverwaltung ausgetauscht werden. Die Kreisverwaltung übernimmt für die organisatorische und technische Steuerung des Kreisnetzes die Verantwortung und tritt gegenüber den Kommunen als **Netzbetreiber** auf.

Die Kreisverwaltung hat für ihr Kreisnetz folgende **Datenschutzziele** festgelegt:

- Herstellung einer für das Kreisgebiet **flächendeckenden** Kommunikationsinfrastruktur für die Kommunen,
- Transport von Daten in einem **abgeschotteten** Kreisnetz,
- Schutz der im Kreisnetz übertragenen Daten vor Angriffen aus dem **Internet** und vor Angriffen aus angeschlossenen Nutzernetzen,
- einfache und **revisionssichere** Kontrolle der festgelegten Sicherheitsmaßnahmen durch den Nutzer,
- Einhaltung der in der **IT-Sicherheitsleitlinie** festgelegten Sicherheitsziele und die damit verbundene Gewährleistung der Umsetzung des festgelegten **Sicherheitsniveaus**,
- Einrichtung einer **IT-Sicherheitsorganisation** durch die Festlegung von Zuständigkeiten sowie die Abgrenzung der Verantwortung der beteiligten Personen,
- eine umfassende und nachvollziehbare **Dokumentation** über den Aufbau und den Betrieb des Kreisnetzes Plön.

[1] Das KNSH bildet auch die physikalische Netzinfrastruktur des Landesnetzes Schleswig-Holstein. Das ULD hat das Landesnetz am 28. August 2006 auditiert. Siehe https://www.datenschutzzentrum.de/landesnetz/.

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

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

1. Beachtung von **Rechtsvorschriften**, Richtlinien und sonstigen Arbeitsanweisungen zur Datensicherheit und zur Ordnungsmäßigkeit der Datenverarbeitung,
2. Festlegung von **Zuständigkeiten** sowie die Abgrenzung der Verantwortung der beteiligten Betreiber, Dienstleister und Nutzer,
3. Ausgestaltung der **technischen** und **organisatorischen** Maßnahmen zur Datensicherheit der für das Kreisnetz eingesetzten IT-Systeme und der über das Kreisnetz kommunizierten Daten,
4. Einführung von **IT-Sicherheitsprozessen** für die Aufrechterhaltung des festgelegten Sicherheitsniveaus, indem die aufbau- und ablauforganisatorischen Strukturen angepasst werden,
5. Schaffung geeigneter und einheitlicher **Schnittstellen** zum Sicherheitsmanagement des Kunden und des Dienstleisters T-Systems sowie
6. revisionssichere **Kontrolle** der festgelegten Sicherheitsmaßnahmen.

Zum Kreisnetz Plön gehören nachfolgend vorgelegte Unterlagen. Sie sind **Gegenstand des Audits** und wurden einer ausführlichen **Begutachtung** unterzogen (siehe Tz. 2):

- Konzept des Kreisnetzes in der Version 1.0 vom 15.11.2007
- Sicherheitskonzept Kreisnetz in der Version 1.0 vom 22.10.2007
- Sicherheitsleitlinie in der Version 1.0 vom 9.07.2007
- Sicherheitsmanagement in der Version 1.0 vom 9.07.2007
- Sicherheitsmaßnahmen und Restrisiken der Firma T-Systems in der Version 1.42 vom 2.11.2006
- Betreibervertrag für das Kreisnetz zwischen Kreis und Kommune aus dem Jahr 2005
- Übersicht, über die vom Kreis Plön mit den kreisangehörigen Nutzern zu schließenden Vereinbarungen als Anlage zum Betreibervertrag

- Benutzerhandbuch Auftragsverwaltungssystem in der Version 1.0 vom 5.11.2007
- Benutzerhandbuch Kreisnetz-Forum in der Version 1.0 vom 11.10.2007
- Benutzerhandbuch Nagios-System in der Version 1.0 vom 9.11.2007

2 Feststellung zu den sicherheitstechnischen Elementen des Kreisnetzes Plön

2.1 Zweck und Ausprägung

Aufgabe des Kreisnetzes Plön 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. Das Kreisnetz Plön dient dem Zweck,

- eine **flächendeckende** und **einheitliche** Kommunikationsinfrastruktur für die öffentlichen Verwaltungen im Kreis Plön herzustellen,
- Daten zwischen den angeschlossenen Verwaltungen elektronisch in einem einheitlichen Verfahren sicher und datenschutzkonform zu übermitteln,
- durch die einheitliche Anschlusstechnik und flächendeckende Verfügbarkeit übergreifende **Verwaltungsprozesse** im Kreis Plön sicherzustellen und
- eine Kommunikationslösung und die damit verbundenen Prozesse einfach, beherrschbar und **wirtschaftlich** anzubieten.

Alle kreisangehörigen Kommunen (15 Verwaltungen) sind am Kreisnetz Plön angeschlossen. Zurzeit gibt es zwischen der Kreisverwaltung und den Kommunen 151 technische **Dienstleistungsvereinbarungen über die Nutzung von Services**, die das Kreisnetz Plön als **Netzinfrastruktur** voraussetzen. Dazu zählt z. B. der zentrale Zugriff auf Fachprogramme und Daten der Kommunen und des Kreises. Damit wird die Möglichkeit geschaffen, dass jede Kommune über das Kreisnetz Plön zentral installierte Anwenderprogramme des Kreises nutzen kann.

2.2 Betreiber

Das Kreisnetz wird von der Kreisverwaltung Plön betrieben. Die Kreisverwaltung besitzt jedoch keine eigenen Netzleitungen, sondern hat mit dem **Finanzministerium** des Landes Schleswig-Holsteins als **Betreiber des Landesnetzes**[3] eine vertragliche Vereinbarung über die **Mitnutzung** der technischen Netzinfrastruktur des Landesnetzes des von T-Systems bereitgestellten **Kommunikationsnetzes Schleswig-Holstein (KNSH)** geschlossen.

Das Landesnetz ist eine **zentrale Kommunikationsplattform** für die Dienststellen der Landesverwaltung und großer Teile der kommunalen Verwaltung in Schleswig-Holstein. Die physikalische **Netzinfrastruktur** wird von der T-Systems zur Verfügung gestellt.

Die **datenschutzrechtliche Verantwortung** für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung über das Kreisnetz liegt bei den Datenverarbeitenden Stellen der Kreisverwaltung sowie der jeweiligen kommunalen Nutzer, soweit sie das Kreisnetz zur Erfüllung ihrer Aufgaben nutzen. Dabei stützen sich die Verwaltungen auf die **Betriebsverantwortung** des Kreises Plön für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung des Kreisnetzes als Infrastruktur, die dieser als Betreiber im Wege der Auftragsdatenverarbeitung erbringt. In der Kreisverwaltung selbst liegt die Betriebsverantwortung einschließlich der Gewährleistung von Datenschutz und Datensicherheit bei der **IT-Abteilung der Kreisverwaltung**.

2.3 Dienstleister

Aufgabe von **T-Systems** ist die Bereitstellung und der Betrieb von Übertragungsleistungen und –schnittstellen zum Transport von Daten zwischen den der Kreisverwaltung Plön benannten Kommunikationspartnern. Hierzu richtet T-Systems so genannte virtuelle Gruppen ein, die mit Hilfe der **MPLS-Technologie** voneinander abgeschottet werden.

T-Systems übernimmt die Aufgabe der **Administration** der Übergaberouter des Kreisnetzes Plön nach den Vorgaben der jeweiligen Nutzer. Die Kommune beauftragt die Einstellungen ihrer **Kommunikationsparameter** über die Kreisverwaltung. Die Kreisverwaltung beauftragt anschließend T-Systems mit der Administration. Nach Abschluss der von T-Systems durchgeführten Arbeiten **kontrolliert** die Kreisverwaltung die Einstellungen auf dem Übergaberouter und erstellt anschließend für

[3] Das Landesnetz wurde vom ULD am 28. August 2006 auditiert.

die Kommune einen gesonderten **Bericht** der durchgeführten Änderungen, damit diese die ordnungsgemäße Erfüllung ihres Auftrages kontrollieren kann.

In seinem **Sicherheitskonzept** stellt T-Systems dar, durch welche Sicherheitsmaßnahmen der Datentransport auf dem KNSH gegenüber anderen Kunden von T-Systems abgeschottet wird. T-Systems übernimmt gegenüber dem Finanzministerium und übergeleitet durch die Vereinbarung zwischen dem Finanzministerium und dem Kreis Plön auch gegenüber diesem die Verantwortung für die **Verfügbarkeit** des Leitungsnetzes sowie für die **Umsetzung** der in ihrem Sicherheitskonzept festgelegten Sicherheitsmaßnahmen.

2.4 Kommune

Die angeschlossenen Kommunen nutzen das Kreisnetz für den **Datentransport** im Rahmen ihrer Fachanwendungen und für den Austausch von Verwaltungsinformationen. Anschlussberechtigt sind alle kreiszugehörigen Kommunen.

Bei einem Anschluss an das Kreisnetz hat die Kommune folgende **Sachverhalte und Anforderungen** zu berücksichtigen:

- Bei der Nutzung des Kreisnetzes werden die Daten der Kommune **unverschlüsselt** transportiert. Sollte die Sicherheitsbetrachtung der Kommune für die Verarbeitung ihrer personenbezogenen Daten einen **höheren Schutz** erfordern, hat sie weitergehende Sicherheitsmaßnahmen in eigener Zuständigkeit zu treffen.

- Die Kommune hat **eigenverantwortlich** in einem Sicherheitskonzept die technischen und organisatorischen Sicherheitsmaßnahmen für die automatisierte Datenverarbeitung in ihrem Verantwortungsbereich festzulegen, um den Schutz ihrer **internen Datenverarbeitung** und der von ihr über das Kreisnetz kommunizierten Daten zu gewährleisten.

- Die für den Datentransport eingesetzten **IT-Systeme** (Übergaberouter, Nagios-System) stehen in der Verantwortung der Kreisverwaltung. Eine Administration durch die Kommune ist ausgeschlossen.

- Die **Konfiguration** des Übergaberouters sowie die **Sicherheitseinstellungen** sind für die jeweils betroffene Kommune **transparent** und jederzeit **kontrollierbar**.

2.5 Aufbau des Kreisnetzes

Das Kreisnetz stellt eine **sternförmige Vernetzung** der Kommunen mit der Kreisverwaltung dar. Es werden für das Routing innerhalb des Netzes die landesweit für Kommunen festgelegten IP-Adressräume verwendet. Die Kommunikation findet über das Kreisnetz Plön **ausschließlich** zwischen der in der Kreisverwaltung befindlichen Service-Area und den im internen Netz der Kommune befindlichen IT-Systemen statt. Eine Datenkommunikation von **Teilnehmer zu Teilnehmer** auf **direktem Wege** ist nicht realisiert.

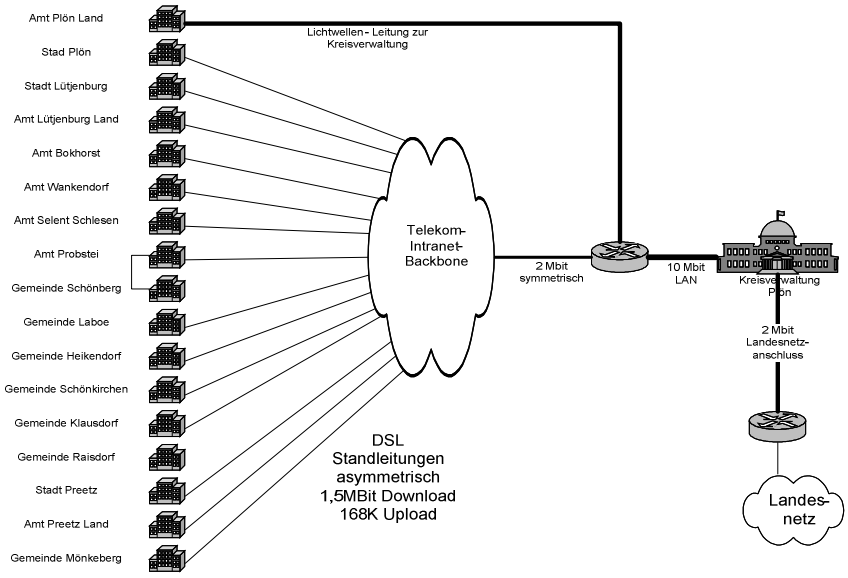


Abb.: Netzstruktur[4]

Die Kreisverwaltung hat als **Betreiber** des Kreisnetzes die technischen und organisatorischen Strukturen des Kreisnetzes bestimmt und gewährleistet die Umsetzung der für das Kreisnetz festgelegten IT-Sicherheitsmaßnahmen. Zu dem Kreisnetz gehören folgende Komponenten:

- **Übergaberouter**

Der Übergaberouter verbindet das interne Netz der Kommune bzw. das Netz der Kreisverwaltung mit einer Anschlussleitung zum so genannten KNSH-Backbone. Die Übergaberouter der Kommunen sind so konfiguriert, dass nur eine Kommunikation

[4] Die Gemeinde Schönberg und das Amt Probstei werden zum 01.01.2008 fusionieren. Aus der Fusion erklärt sich die indirekte Anbindung der Gemeinde Schönberg.

mit dem Übergaberouter der Kreisverwaltung möglich ist.

- **KoKoNet-Switch**

Der KoKoNet-Switch verbindet innerhalb der Kreisverwaltung den zentralen Übergaberouter mit der Firewall und der dahinter liegenden Service-Aera und dem Servernetz. Zusätzlich sind an dem KoKoNet-Switch weitere Netzanbindungen zu Kommunen über **Lichtwelle** angeschlossen. Die **Trennung** der Datenkommunikation der einzelnen Kommunen erfolgt über so genannte **virtuell private Networks** (VPN).

- **Anschluss- bzw. Zugangsleitungen**

Jede Kommune verfügt über eine dedizierte **Anschlussleitung** zum Kreisnetz. Sie verbindet den Übergaberouter der Kommune mit dem KNSH-Backbone.

- **Backbone**

Der von T-Systems gemanagte KNSH-Backbone besteht aus **Hochgeschwindigkeitsstandleitungen** und so genannten Backbone- und Konzentrationsroutern, die an mehreren **Standorten** in Schleswig-Holstein das Kommunikationsnetz verbinden.

Die Datenkommunikation auf dem Backbone erfolgt ebenfalls durch die Einrichtung von virtuellen Gruppen (VPN), die mit Hilfe der **MPLS-Technologie** voneinander abgeschottet werden.

2.6 Netzwerkmanagement

2.6.1 Nagios

Zur Nachverfolgung laufender Prozesse auf den Kreisnetzkomponenten (Übergaberouter, KoKoNet-Switch) wird die Managementsoftware **„Nagios“** eingesetzt. Mit Nagios ist es möglich, die **Einstellungen** der Kreisnetzkomponenten zu überwachen. Sie verfügt über eine Sammlung von Modulen zur Netzwerk-, Host- und Serviceüberwachung sowie einem Webinterface zum Abfragen der gesammelten Daten.

Das Netzwerkmanagement der Kreisverwaltung ist durch den Einsatz von Nagios in der Lage, den **Betriebszustand aller Übergaberouter** der am Kreisnetz angeschlossenen Kommunen zu kontrollieren. Folgende Daten können auf dem eigenen Kreisnetzübergaberouter, auf dem KoKoNet-Switch und auf den Übergaberoutern der Kommunen eingesehen werden:

- Routing-Tabelle,

- IP-Adressen,
- VLANs und
- Protokolle der Konfigurationsänderungen auf dem Übergaberouter.

2.6.2 Auftragsverwaltungssystem

Die Kreisverwaltung setzt für die Bearbeitung der von den Kommunen gemeldeten Aufträge die Software **„Quadriga“** ein. Mit der Software werden Aufträge bearbeitet sowie Störungen dokumentiert und nachvollzogen. Die **Aufträge** und **Störungen** können verschiedenen Mitarbeitern der IT-Abteilung zugeordnet und nach Priorität bearbeitet werden. Es lassen sich darüber hinaus **Standardvorfälle** festlegen, die eine standardisierte Vorgehensweise bei der Bearbeitung Aufträge oder Störungen ermöglichen. Die Kreisverwaltung sorgt mit diesem System für eine nachvollziehbare Dokumentation der Auftragsbearbeitung.

2.6.3 Kreisnetz-Forum

Die Kreisverwaltung hat zur Unterstützung der Administratoren in den Kommunen eine **Kommunikationsplattform** zur Beseitigung eigener technischer Probleme eingerichtet. Sie besteht aus einem **Forum**, in dem die Kreisverwaltung technische Informationen für die Kommunen bereitstellt. Des Weiteren können sich die Administratoren der Kommunen in dem Forum zu technischen Themen äußern und es als **Fehlerinformationsquelle** sowie als **Diskussionsplattform** nutzen. Das Forum enthält außerdem eine Sammlung häufig gestellter Fragen und die dazugehörigen Antworten.

2.7 Kreisnetzdokumentation

Die Kreisnetzdokumentation beschreibt den **Aufbau**, die **Funktionsweise** und das erreichte **Sicherheitsniveau** des Kreisnetzes Plön. Sie besteht aus folgenden Dokumenten:

- Konzept des Kreisnetzes
- Sicherheitskonzept Kreisnetz

- Sicherheitsleitlinie
- Sicherheitsmanagement
- Sicherheitsmaßnahmenkatalog der Firma T-Systems
- Betreibervertrag für das Kreisnetz zwischen Kreis und Kommune
- Nutzungsvereinbarungsübersicht
- Benutzerhandbuch Auftragsverwaltungssystem
- Benutzerhandbuch Kreisnetz-Forum
- Benutzerhandbuch Nagios-System

Die Dokumentation entspricht den **Anforderungen** der Datenschutzverordnung. Eine Anpassung des Anschlussvertrages zwischen Kreis und Kommune an die veränderten **technischen Rahmenbedingungen** und die **neu strukturierte Dokumentation** steht jedoch noch aus und ist zeitnah mit der weiteren **Fortschreibung** und **Optimierung** der einzelnen Dokumente anzupassen.

2.8 Datenschutz- und Sicherheitsmanagement

2.8.1 Sicherheitsmanagement

Das Sicherheitsmanagement der Kreisverwaltung Plön besteht aus

- dem Leiter der Abteilung für Informationstechnik (AIT),
- der behördlichen Datenschutzbeauftragten,
- eines für die IT-Sicherheit zuständigen Mitarbeiters aus der AIT und
- einem kommunalen EDV-Verantwortlichen für die Sicherheitsaspekte des Kreisnetzes.

Die Mitarbeiter des Sicherheitsmanagement sind für alle **IT-Sicherheitsfragen** zuständig. Sie sind Ansprechpartner für die **IT-Verfahrensanwender** der Kreisverwaltung und der am Kreisnetz Plön angeschlossenen Kommunen. Sie prüfen und bewerten die für die IT-Verfahren getroffenen Sicherheitsmaßnahmen auf ihren **Umsetzungsstand** und auf ihre **Wirksamkeit**.

Über **Schulungsmaßnahmen** soll sichergestellt werden, dass **Sicherheitsvorfälle** auch in den Kommunen erkannt und durch eine **zuständige Person** bei der Kommune dem Sicherheitsmanagement zur weiteren Bearbeitung gemeldet werden.

2.8.2 IT-Sicherheitsleitlinie

Die **IT-Sicherheitsleitlinie** der Kreisverwaltung Plön beinhaltet die **angestrebten IT-Sicherheitsziele**, die verfolgten **IT-Sicherheitsstrategien** sowie grundlegende Verfahren und Regeln zur dauerhaften Steuerung und Kontrolle der Informationssicherheit. Sie gilt für alle Fachbereiche der Kreisverwaltung. Darüber hinaus kommt Sie zur Anwendung bei der Erbringung informationstechnischer **Dienstleistungen** für Dritte, wie z.B. die am Kreisnetz Plön angeschlossenen Kommunen.

2.8.3 Sicherheitskonzept Kreisnetz

Das Sicherheitskonzept für das Kreisnetz Plön beinhaltet technische und organisatorische Maßnahmen, die von der Kreisverwaltung Plön und dem Dienstleister T-Systems umgesetzt werden. Die **Verantwortung** für die sichere Datenkommunikation im Kreisnetz liegt jedoch vollständig bei der Kreisverwaltung Plön. Die von ihr für das Kreisnetz Plön zu gewährleistenden **Sicherheitsanforderungen** ergeben sich aus dem zwischen Kreisverwaltung und Kommune abgeschlossenen Betreiber- bzw. Anschlussvertrag.

Folgende **Sicherheitsmaßnahmen** sind für den Betrieb des Kreisnetzes Plön von besonderer Bedeutung:

- Zwischen der Kreisverwaltung Plön und der Kommune wird ein Betreiber- bzw. Anschlussvertrag unter Einbeziehung **sicherheitstechnischer und datenschutzrechtlicher** Regelungen abgeschlossen.
- Es ist ein Sicherheitsmanagement für die **Aufrechterhaltung und Fortentwicklung** des für das Kreisnetz Plön festgelegten Sicherheitsniveaus eingerichtet.
- Es werden **Sicherheitschecks** durchgeführt und die Ergebnisse dokumentiert.
- Sicherheitsvorfälle werden nach einem **geregelten Verfahren** bearbeitet.
- Der Übergaberouter ist nur von T-Systems administrierbar. Die Kreisverwaltung Plön hat für **Kontrollzwecke** auf allen dem Kreisnetz Plön zugehörigen Übergabe-

routern lesende Berechtigungen, während eine einzelne Kommune nur auf ihren eigenen Übergaberouter über lesende Berechtigungen verfügt.

- Der ordnungsgemäße Betrieb wird über das **Netzwerkmanagement** der Kreisverwaltung Plön überwacht.
- Die Administration der Netzkomponenten wird von T-Systems **revisionssicher** in einem Servicecenter durchgeführt.
- Alle administrativen Zugriffe von T-Systems auf den Kreisnetz-Komponenten werden auf einem **Authentisierungsserver** erfasst.

2.8.4 Behördliche Datenschutzbeauftragte

Die Kreisverwaltung Plön hat eine **behördliche Datenschutzbeauftragte** gemäß § 10 Landesdatenschutzgesetz (LDSG) bestellt. Sie überwacht und prüft als Mitglied des Sicherheitsmanagements für das Kreisnetz Plön

- die **Umsetzung und Einhaltung** festgelegter Sicherheitsziele und Sicherheitsmaßnahmen,
- die Abarbeitung **sicherheitsrelevanter Vorfälle** sowie
- die Sicherheitsvorgaben der **beauftragten Dienstleister**.

Sie ist in der Bewertung der IT-Sicherheit fachlich weisungsfrei und hat direkten Zugang zum Landrat.

2.8.5 Überwachung der Kreisnetz-Schnittstellen

Die Übergaberouter der Kommunen verbinden das **interne Netz** mit dem Kreisnetz Plön. Die auf ihnen durchgeführten **Konfigurationsänderungen** sind für die Kommunen ohne den Einsatz von Revisionstools nur schwer erkennbar, so dass ungewollte Veränderungen durch eine **Fehlkonfiguration** oder durch eine bewusste Manipulation nicht festgestellt werden können. Um dieses Risiko zu vermeiden und um eine sichere Datenkommunikation zwischen Kommune und Kreisverwaltung zu gewährleisten, richtet die Kreisverwaltung Plön im Bereich ihres Netzwerkmanagements und in dem Technikraum der Kommune jeweils einen **Nagios-Überwachungsserver** ein.

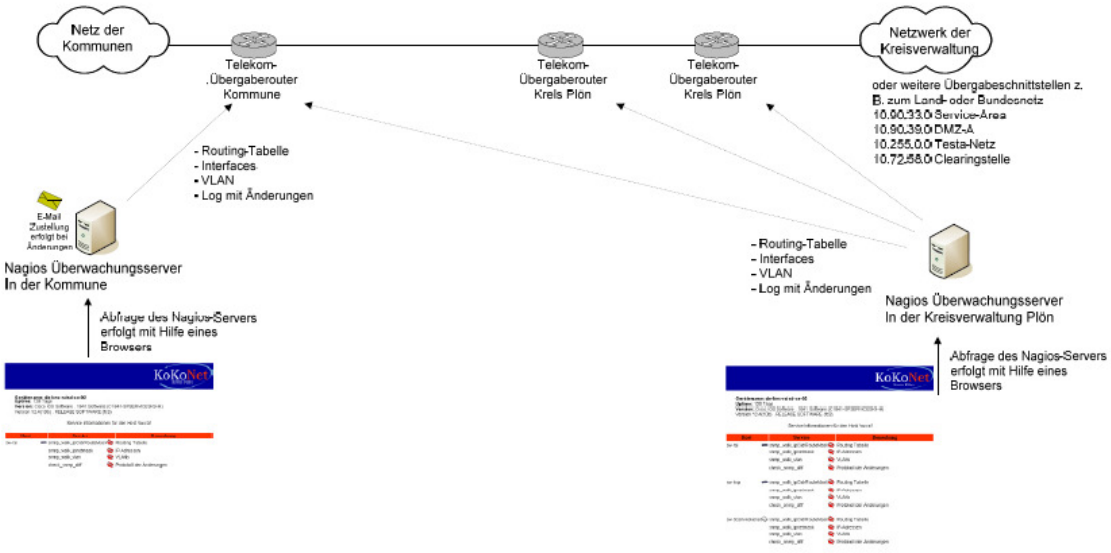


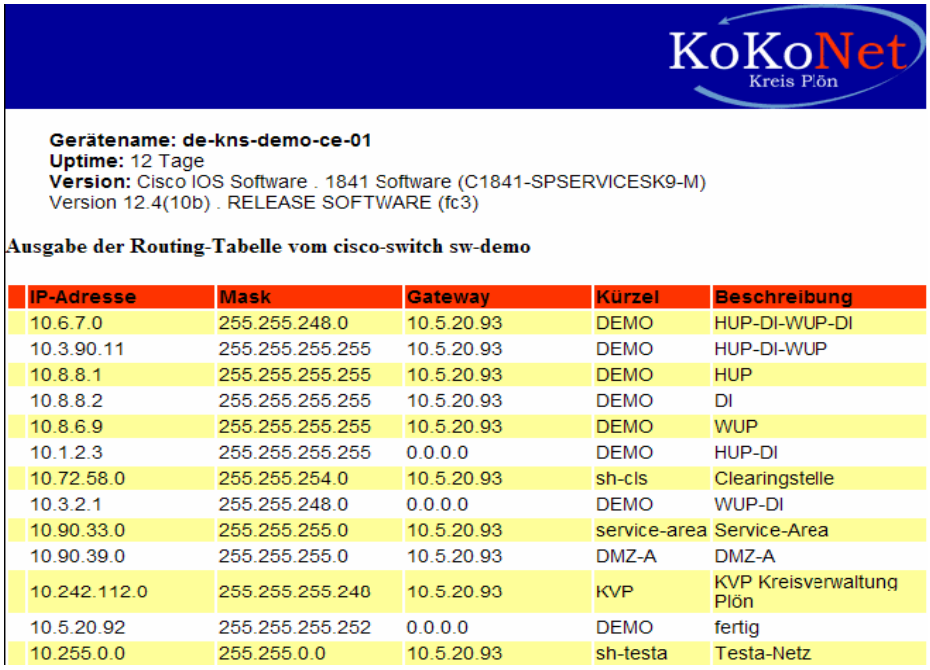
Abb.: Nagios Überwachungsserver

Über den Nagios-Überwachungsserver **in der Kreisverwaltung Plön** können interne Daten aus dem Übergaberouter ausgelesen werden. Hierzu gehören Informationen über die Routing-Tabelle, eingerichtete VLANs und die Protokolldatei mit den Konfigurationsänderungen. Der Nagios-Überwachungsserver bemerkt durch einen **Abgleich der Konfigurationsdaten** der Übergaberouter jede auf ihnen durchgeführte administrative Änderung. Sobald eine Veränderung der Konfigurationsdaten am Übergaberouter durchgeführt wird, zeigt Nagios diese an. Zusätzlich wird eine **Benachrichtigung** an eine voreingestellte E-Mail-Adresse geschickt. Die Kreisverwaltung Plön kann mit diesem Verfahren alle durch ihren Dienstleister T-Systems auf Übergaberoutern des Kreisnetzes Plön durchgeführten Veränderungen lückenlos nachvollziehen.

Die **Kommune** ist mit dem Anschluss ihres internen Netzes an das Kreisnetz ebenfalls in der Lage, die auf ihrem Übergaberouter durchgeführten Aktivitäten zu kontrollieren. Sie bekommt von der Kreisverwaltung Plön einen vorinstallierten Nagios-Überwachungsserver zur Verfügung gestellt, mit dem sie **selbständig alle Aktivitäten** auf dem Übergaberouter **revisionssicher** nachvollziehen kann. Der Nagios-Überwachungsserver stellt hierfür nur genau die Funktionen zur Verfügung, die er für eine **vollständige** und nachvollziehbare Überwachung benötigt.

Die Kommune kann insbesondere die **Routing-Tabellen** und die **Log-Dateien** einsehen. Sobald eine Veränderung auf dem Übergaberouter stattgefunden hat, erhält eine in der Kommune definierte Person eine Benachrichtigung per E-Mail. So lässt sich sofort nachvollziehen, ob die Veränderung auf einen **Auftrag durch die Kom-**

mune zurückzuführen ist. Ist dies nicht der Fall, wurde auf den Übergaberouter **unerlaubt** zugriffen und es liegt ein **Sicherheitsvorfall** vor.



KoKoNet Kreis Plön

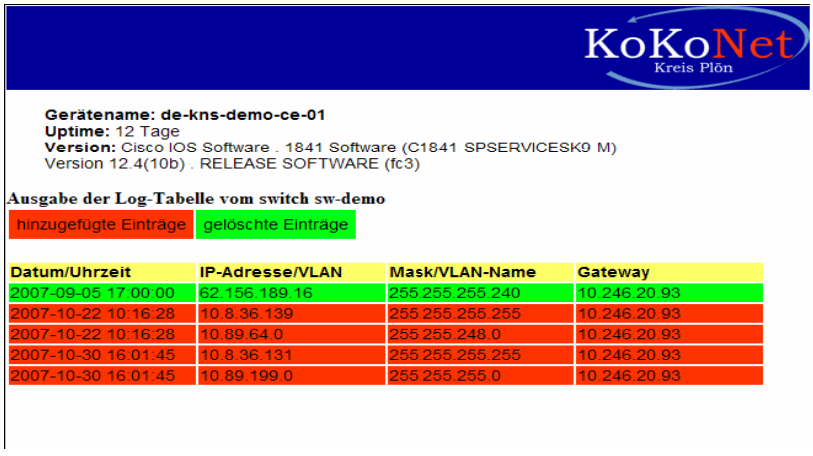
Gerätename: de-kns-demo-ce-01
Uptime: 12 Tage
Version: Cisco IOS Software . 1841 Software (C1841-SPSERVICESK9-M) Version 12.4(10b) . RELEASE SOFTWARE (fc3)

Ausgabe der Routing-Tabelle vom cisco-switch sw-demo

IP-Adresse	Mask	Gateway	Kürzel	Beschreibung
10.6.7.0	255.255.248.0	10.5.20.93	DEMO	HUP-DI-WUP-DI
10.3.90.11	255.255.255.255	10.5.20.93	DEMO	HUP-DI-WUP
10.8.8.1	255.255.255.255	10.5.20.93	DEMO	HUP
10.8.8.2	255.255.255.255	10.5.20.93	DEMO	DI
10.8.6.9	255.255.255.255	10.5.20.93	DEMO	WUP
10.1.2.3	255.255.255.255	0.0.0.0	DEMO	HUP-DI
10.72.58.0	255.255.254.0	10.5.20.93	sh-cls	Clearingstelle
10.3.2.1	255.255.248.0	0.0.0.0	DEMO	WUP-DI
10.90.33.0	255.255.255.0	10.5.20.93	service-area	Service-Area
10.90.39.0	255.255.255.0	10.5.20.93	DMZ-A	DMZ-A
10.242.112.0	255.255.255.240	10.5.20.93	KVP	KVP Kreisverwaltung Plön
10.5.20.92	255.255.255.252	0.0.0.0	DEMO	fertig
10.255.0.0	255.255.0.0	10.5.20.93	sh-testa	Testa-Netz

Abb.: Ausgabe der Routing-Tabelle

Darüber hinaus kann die Kommune auch auf den bei der Kreisverwaltung installierten Nagios-Überwachungsserver zugreifen. Sie kann von diesem Nagios-Überwachungsserver ihren eigenen Übergaberouter sowie zusätzlich den bei der Kreisverwaltung Plön aufgestellten **Kreisnetz-Übergaberouter** und den **KoKoNet-Switch** kontrollieren. So besteht für die Kommune sogar noch bei **Ausfall** ihres eigenen Nagios-Übergabeservers die Möglichkeit, die Kontrolle über ihren Übergaberouter aufrechtzuerhalten.



KoKoNet Kreis Plön

Gerätename: de-kns-demo-ce-01
Uptime: 12 Tage
Version: Cisco IOS Software . 1841 Software (C1841 SPSERVICESK9 M) Version 12.4(10b) . RELEASE SOFTWARE (fc3)

Ausgabe der Log-Tabelle vom switch sw-demo

hinzugefügte Einträge | gelöschte Einträge

Datum/Uhrzeit	IP-Adresse/VLAN	Mask/VLAN-Name	Gateway
2007-09-05 17:00:00	62.156.189.16	255.255.255.240	10.246.20.93
2007-10-22 10:16:28	10.8.36.139	255.255.255.255	10.246.20.93
2007-10-22 10:16:28	10.89.64.0	255.255.248.0	10.246.20.93
2007-10-30 16:01:45	10.8.36.131	255.255.255.255	10.246.20.93
2007-10-30 16:01:45	10.89.199.0	255.255.255.0	10.246.20.93

Abb.: Ausgabe der Log-Tabelle

2.8.6 Sicherheitsvorfälle

Für das Kreisnetz Plön wurde eine Reihe von **Ereignissen** als Standard-Sicherheitsvorfall festgelegt. Über das IT-Sicherheitsmanagement werden die am Kreisnetz Plön angeschlossenen Kommunen über das **Erkennen** und **Melden** von Sicherheitsvorfällen geschult. Tritt ein **Sicherheitsvorfall** ein, wird das IT-Sicherheitsmanagement benachrichtigt. Zuständige Mitarbeiter der IT-Abteilung nehmen den Sicherheitsvorfall im Auftragsverwaltungssystem auf und beginnen entsprechende **Gegenmaßnahmen** einzuleiten.

3 Datenschutzrechtliche Bewertung

3.1 Prüfungsverlauf

Das Audit **„Kommunales Kommunikationsnetz der Kreisverwaltung Plön“** (Kreisnetz Plön) wurde vom Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) über mehrere Phasen begleitet.

Zunächst wurde in Zusammenarbeit mit der Kreisverwaltung Plön eine **Bestandsaufnahme** über die organisatorischen und technischen Strukturen des Kreisnetzes Plön durchgeführt. Die Ergebnisse der Erhebung sowie Handlungsempfehlungen wurden von der Kreisverwaltung aufgenommen und stufenweise bearbeitet.

Es erfolgte eine Anpassung der **Dokumentation** an die derzeitigen Gegebenheiten unter Berücksichtigung aller organisatorischen, technischen und datenschutzrechtlichen Belange. Weiterhin wurden die **Sicherheits- und Revisionsfunktionen** des Netzwerkmanagements bei der Kreisverwaltung und bei der Kommune optimiert.

Nach Abschluss aller Arbeiten und nach Erreichung der von der Kreisverwaltung festgelegten **Ziele** wurde vom ULD im November 2007 die **Begutachtungsphase** eingeleitet. Analysiert wurden insbesondere die zur **Konzeption** gehörigen Dokumente (siehe Anlagenverzeichnis) sowie ihre Umsetzung. Die für das Kreisnetz Plön festgelegten **Sicherheitsmaßnahmen** wurden darüber hinaus vor Ort mit den bereits umgesetzten aufbau- und ablauforganisatorischen Gegebenheiten stichprobenartig geprüft und abgeglichen. Dazu gehörten insbesondere folgende Punkte:

- Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit,
- Integration der Mitarbeiter in den Sicherheitsprozess,
- Beachtung rechtlicher Rahmenbedingungen,

- Dokumentation des IT-Sicherheitsprozesses,
- systemtechnische Konfiguration einzelner Kreisnetz-Komponenten,
- Netzwerkmanagementdienste (Log-Server und Nagios),
- Umsetzung des Berichtswesens,
- Revisionsfunktionen bei der Kommune,
- Verhaltensregeln und Meldewege bei Sicherheitsvorfällen sowie
- Sensibilisierung der Mitarbeiter für IT-Sicherheit.

3.2 Rechtliche Anforderungen

Das Kreisnetz Plön ist ein **geschlossenes Netz** für die kreisangehörigen Kommunen. Es ermöglicht den Transport personenbezogener Daten zwischen definierten Anschlüssen und ausschließlich zugelassenen Kommunen nach den von ihnen definierten Kommunikationsparametern. Das Kreisnetz Plön bietet den Kommunen ein einheitliches Sicherheitsniveau. Um dies zu erreichen, stellt die Kreisverwaltung Plön als Betreiber **Sicherheitsdienstleistungen** bereit, die anteilig auch vom Dienstleister T-Systems erbracht werden.

Das **Landesdatenschutzgesetz** sowie die **Datenschutzverordnung** finden infolgedessen neben den bereichsspezifischen Vorschriften Anwendung. Die gesetzlichen Regelungen zur Datensicherheit verweisen auf den **allgemeinen anerkannten Standard der IT-Sicherheit** und auf die **Anforderungen an ihre Dokumentation**.

Die automatisierte Verarbeitung personenbezogener Daten im Rahmen der Datenkommunikation über das Kreisnetz Plön erfordert technische und organisatorische Maßnahmen, die die Datensicherheit bzw. die Ordnungsmäßigkeit der Datenverarbeitung gewährleisten. Dabei sind insbesondere folgende Rechtsvorschriften zu beachten:

- **Landesdatenschutzgesetz (LDSG)**

§ 4 Datenvermeidung und Datensparsamkeit

§ 5 Allgemeine Maßnahmen zur Datensicherheit

§ 6 Besondere Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren

§ 7 Verfahrensverzeichnis, Meldung

§ 8 Gemeinsame Verfahren und Abrufverfahren

§ 17 Verarbeitung personenbezogener Daten im Auftrag, Wartung

- **Datenschutzverordnung (DSVO)**

§ 3 Verfahrensdokumentation

§ 4 Verfahrenszweck

§ 5 Verfahrensbeschreibung

§ 6 Sicherheitskonzept

§ 7 Test und Freigabe

§ 8 Verfahrensübergreifende Dokumentation und Protokolle

Darüber hinaus sind **interne Regelungen** über die personelle und organisatorische Gestaltung der Datensicherheit zu treffen. Es muss gewährleistet sein, dass die datenschutzrechtlichen Anweisungen auch tatsächlich in konkrete Datensicherungsmaßnahmen umgesetzt werden und ihre Einhaltung durch das **Sicherheitsmanagement** der Kreisverwaltung Plön kontrolliert wird.

3.3 Zusammenfassende Bewertung

Im Auditverfahren **„Kommunales Kommunikationsnetz der Kreisverwaltung Plön“** (Kreisnetz Plön) wurde festgestellt, dass die Kreisverwaltung Plön die im Sicherheitskonzept festgelegten Sicherheitsmaßnahmen weitgehend umgesetzt hat.

Die Praxistauglichkeit der für das Kreisnetz Plön erstellten Dokumentation wird durch den ordnungsgemäßen Betrieb des Kreisnetzes bestätigt. Die **Leitungsebene** ist sensibilisiert und übernimmt Aufgaben und Pflichten für die Informationssicherheit im Rahmen des von ihr eingerichteten Sicherheitsmanagement.

Darüber hinaus wurden bei der Durchführung des Audits folgende „**datenschutzfreundliche**“ Aspekte als besonders erwähnenswert festgestellt:

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

2. Die Kreisverwaltung stellt sicher, dass die im Kreisnetz Plön eingesetzten Übergaberouter nach den **Kommunikationsparametern** der Kommunen ordnungsgemäß administriert werden.

3. Sicherheitsrelevante Ereignisse können über den Einsatz der **Nagios-Überwachungsserver** von den Administratoren der IT-Abteilung der Kreisverwaltung Plön und von den Administratoren der Kommunen rechtzeitig erkannt und ausgewertet werden.

4. Die technischen und organisatorischen Abläufe im Kreisnetz werden in der **Kreisnetzdokumentation** vollständig beschrieben.

5. Das Kreisnetz ist für die Kommune als **abgeschlossenes Netzwerk** einzustufen, in dem ihre Daten unverschlüsselt, aber isoliert von anderen Kommunen transportiert werden. Die angeschlossenen Kommunen haben einen erhöhten Schutzbedarf festzulegen, wenn die die in der Sicherheitsanalyse beschriebenen Restrisiken als nicht ausreichend bewertet werden.

Die Prüfung hat ergeben, dass die Kreisverwaltung Plön als Betreiber ihres Kreisnetzes Plön Sicherheitsmaßnahmen umgesetzt hat, die eine sicherheitstechnische und datenschutzgerechte Datenkommunikation über das Kreisnetz Plön gewährleisten. Die Verleihung des Auditzeichen an die Kreisverwaltung Plön kann deshalb erfolgen.

Kiel, 26. November 2007

gez.: Sven Thomsen