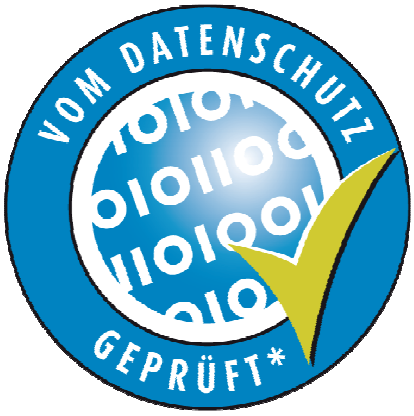

Gutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Kreisverwaltung Plön:

Internetdienste E-Mail und WWW

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Datum:	23.03.2010
Aktenzeichen:	16.01/05.007
Telefon:	0431/988-1200
Fax	0431/988-1223
E-Mail:	mail@datenschutzzentrum.de

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Audits

1.1 Vereinbarung

Gegenstand des Datenschutz-Audits sind die von der Kreisverwaltung Plön für die Kreisverwaltung und die über das Kreisnetz angeschlossenen Kommunen bereitgestellten Internetdienste E-Mail und WWW (World Wide Web).

Bestandteile des Audits sind:

- die internen und externen Firewallsysteme,
- die aktiven Netzkomponenten, die zur Verbindung der Firewallsysteme mit den Serversystemen genutzt werden,
- die WLAN-Access-Points der Kreisverwaltung Plön,
- die Web-, Mail-, Proxy- und Blackberry-Serversysteme und
- die Server für den Verzeichnisdienst.

Nicht Bestandteil des Audits sind die Endgeräte der Kreisverwaltung und die IT-Systeme der angeschlossenen Kommunen, mobile Endgeräte wie Laptops oder Blackberry-Smartphones.

Nicht Bestandteil des Audits ist das Kreisnetz, mit dem die angeschlossenen Kommunen auf die Dienste E-Mail und WWW zugreifen. Dieses wurde im Auditverfahren 21/2007 bereits durch das ULD begutachtet und zertifiziert.

1.2 Vorgehen bei der Auditierung

Die Auditierung erfolgte unter Berücksichtigung der „Hinweise des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Datenschutz-Behördenaudits nach § 43 Abs. 2 LDSG[1]“.

Die Auditierung wurde zur Ergebnissicherung durch ein Voraudit vorbereitet. Im Voraudit wurde überprüft, ob in der Kreisverwaltung die Voraussetzungen für das Datenschutz-Behördenaudit vorliegen. Das Voraudit wurde in den nachfolgend genannten Schritten durchgeführt:

- Abgrenzung des Auditgegenstands,
- Festlegung der Datenschutzziele,
- Sammlung der zum Auditgegenstand gehörenden Dokumentation,
- Bestandsaufnahme der technischen und organisatorischen Abläufe,

[1] Landesdatenschutzgesetz Schleswig-Holstein

- Erstellung eines Ergebnisberichts mit Projektplan,
- Mängelbeseitigung,
- Einrichtung eines Datenschutzmanagementsystems,
- Erstellung des Datenschutzkonzepts,
- Aufbereitung der für das Datenschutz-Behördenaudit erforderlichen Dokumentation sowie
- abschließende Überprüfung der Erfüllung aller im Voraudit festgelegten und durchzuführenden Aufgaben.

Das Voraudit wurde durch Herrn Heiko Behrendt, Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz, durchgeführt.

Das Datenschutz-Behördenaudits wurde auf Basis der Ergebnisse des Voraudits in den folgenden Schritten durchgeführt:

- Überprüfung der Abgrenzung des Auditgegenstands,
- Analyse der Dokumentation (Datenschutzkonzept),
- Begutachtung der Wirkungsweise des Datenschutzmanagementsystems und der Erreichung der festgelegten Datenschutzziele,
- Hervorhebung von anerkennenswerten und datenschutzfreundlichen Datenverarbeitungsprozessen,
- stichprobenartige Überprüfung der Umsetzung der im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen und
- Überprüfung der Einhaltung datenschutzrechtlicher und bereichsspezifischer Vorschriften in Bezug auf den Auditgegenstand.

Die von der Kreisverwaltung vorgelegte Dokumentation für den Auditgegenstand bildet die Grundlage für die Begutachtung vor Ort.

Das Datenschutz-Behördenaudit wurde durch Herrn Sven Thomsen, Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz, durchgeführt.

1.3 Datenschutzziele

Als Datenschutzziele wurden von der Kreisverwaltung Plön festgelegt:

- Umsetzung einer ordnungsgemäßen Datenverarbeitung nach gesetzlichen und vertraglichen Vorgaben,
- Schutz der vertraulichen Daten aller Beteiligten,
- Gewährleistung der Integrität, der Vollständigkeit und Authentizität der Daten,
- Sicherstellung der Kontinuität der Arbeitsabläufe durch Verfügbarkeit der Daten und Informationssysteme im Rahmen tolerierbarer technisch bedingter Stillstandszeiten sowie
- transparente und nachvollziehbare Gestaltung der Datenverarbeitungsprozesse.

Die Kreisverwaltung Plön hat die folgenden strategischen Maßnahmen getroffen, um die Sicherheits- und Datenschutzziele zu erreichen:

- Einrichtung eines IT-Sicherheitsmanagements zur Gewährleistung und Kontrolle der im IT-Sicherheitskonzept festgelegten Maßnahmen,
- Festlegung eines Test- und Freigabeverfahrens für die in der Kreisverwaltung und für die im Rahmen der Auftragsdatenverarbeitung eingesetzten Informationssysteme,
- Festlegung eines revisionsfähigen Verfahrens zur Dokumentation der Berechtigungen der Mitarbeiterinnen und Mitarbeiter auf den in der Kreisverwaltung eingesetzten Informationssystemen,
- Schulung der für IT-Sicherheit zuständigen Mitarbeiterinnen und Mitarbeiter,
- Einrichtung von personalisierten Benutzerkennungen zur Gewährleistung geregelter Zugriffe auf Fachverfahren und andere Systeme,
- Beschränkung von Zugriffsrechten auf die für die Aufgabenerfüllung notwendigen Rechte sowie
- Speicherung der Daten auf zentralen IT-Systemen.

2 Feststellungen zu den sicherheitstechnischen Elementen des Datenschutzmanagementsystems

2.1 Dokumentation

Die Kreisverwaltung orientiert sich für die Dokumentation der automatisierten Verarbeitung personenbezogener Daten und zum Nachweis angemessener und wirksamer Sicherheitsmaßnahmen an der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten IT-Grundschutz-Vorgehensweise (im Folgenden „BSI-Grundschutz" genannt).

2.1.1 Leitlinien, Richtlinien und Dokumentation

Die Kreisverwaltung Plön folgt bei der Auswahl und Umsetzung von einzelnen Sicherheitsmaßnahmen den Vorgaben der ebenfalls vom BSI veröffentlichten Grundschutz-Kataloge. Konform mit den Vorgaben der Kataloge hat die Kreisverwaltung ein umfangreiches System von Leitlinien und Richtlinien erstellt, mit dem sicherheitstechnische Vorgaben für die IT-Systeme des Auditgegenstands gemacht werden und wesentliche Prozesse eines Systems zum Management von IT-Sicherheit (Informationssicherheitsmanagementsystem, ISMS) vordefiniert werden.

Die Umsetzung der technischen und organisatorischen Maßnahmen wurde durch die Kreisverwaltung überprüft. Die Ergebnisse der Überprüfung sind dokumentiert.

Der primär auf IT-Sicherheit liegende Fokus des BSI-Grundschutzes wurde durch eigene Dokumente und Vorgaben zum Thema Datenschutz und Datenschutzmanagement erweitert.

Die Leitlinien und Richtlinien sind geeignet, einen sicheren und datenschutzkonformen Betrieb der IT-Systeme des Auditgegenstands vorzugeben. Sie werden ergänzt durch eine Installations- und Konfigurationsdokumentation, aus der die wesentlichen Schritte zur Inbetriebnahme der verwendeten Hard- und Softwarekomponenten nachvollzogen werden können.

Die Dokumentation wird bei administrativen Änderungen an den Systemen fortgeschrieben. Zusätzlich nutzt die Kreisverwaltung zur Steuerung und elektronischen Ablaufdokumentation administrativer Änderungen ein Ticketsystem.

2.1.2 Dienstanweisungen

Die in den Leitlinien und Richtlinien gemachten Vorgaben zur Datensicherheit und zum Datenschutz beim Betrieb der IT-Systeme sind zusätzlich organisatorisch in geltende Dienstanweisungen für die Beschäftigten der Kreisverwaltung umgesetzt.

In einer allgemeinen Dienstanweisung über die elektronische Datenverarbeitung und den Datenschutz in der Kreisverwaltung Plön sind die Grundsätze für eine ordnungsmäßige und wirtschaftliche Durchführung einer technikunterstützten Informationsverarbeitung festgelegt.

Die allgemeine Dienstanweisung legt fest, dass die Informationstechnik der Kreisverwaltung Plön nur für dienstliche Zwecke genutzt werden darf. Die Aufgaben der Fachämter und des Hauptamts sind klar abgegrenzt. Die Dienstanweisung legt den Umgang mit Zugangskennungen und das Verhalten bei Störungen und Fehlern fest. Speziell für den Bereich Datenschutz und Datensicherheit sind in der allgemeinen Dienstanweisung Vorgaben zur Umsetzung der Zweckbindung, der Datensparsamkeit und der Verantwortung bei der Verarbeitung personenbezogener Daten enthalten. Die Rolle der behördlichen Datenschutzbeauftragten ist definiert. Zuwiderhandlungen gegen die Dienstanweisung können disziplinarische, arbeitsrechtliche und ggfs. strafrechtliche Konsequenzen zur Folge haben.

In einer speziellen Dienstanweisung über die Nutzung elektronischer Kommunikationsmedien sind Vorgaben zur Nutzung der Internetdienste E-Mail und WWW definiert. Es wird nochmals darauf hingewiesen, dass die Nutzung von Internetdiensten rein zu dienstlichen Zwecken zu erfolgen hat.

2.1.3 Nutzungsvereinbarungen mit angeschlossenen Kommunen

Die über das Kreisnetz angeschlossenen Kommunen schließen mit der Kreisverwaltung Plön Nutzungsvereinbarungen für die Dienste E-Mail und WWW.

In den Nutzungsvereinbarungen zu E-Mail und WWW ist geregelt, dass die Nutzung ausschließlich zu dienstlichen Zwecken erfolgen darf. Die Kommunen müssen zusichern, dass sie durch eigene Dienstvereinbarungen oder –anweisungen die in der Nutzungsvereinbarung getroffenen Regeln organisationsintern umsetzen. Die Kommunen werden über die Aufbewahrungsfristen und Auswertungsmöglichkeiten der anfallenden Protokolldaten informiert. Ebenso wird dargestellt, dass Inhalte mit Schadfunktion an zentraler Stelle gefiltert werden.

2.2 Aufbau- und Ablauforganisation

2.2.1 Allgemeine Geschäftsverteilung

Die Kreisverwaltung Plön ist in drei Fachbereiche aufgeteilt. Die Fachbereiche sind in einzelne Fachämter, die Fachämter in einzelne Abteilungen gegliedert.

Die Abteilung Informationstechnik (AIT) ist dem Hauptamt und hierüber dem Fachbereich 1 zugeordnet.

2.2.2 Datenschutzbeauftragte

Als behördliche Datenschutzbeauftragte ist Frau Capell förmlich gemäß § 10 LDSG bestellt.

Sie überwacht und prüft als Mitglied des IT-Sicherheitsmanagements

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

Frau Capell arbeitet in ihrer Funktion als Datenschutzbeauftragter weisungsfrei und ist dem Landrat direkt unterstellt.

2.2.3 IT-Sicherheitsmanagement

Das IT-Sicherheitsmanagement besteht aus Mitarbeitern oder deren Vertretern folgender Bereiche der Kreisverwaltung

- dem Leiter der Abteilung für Informationstechnik (AIT),
- der behördlichen Datenschutzbeauftragten (bDSB) des Kreises Plön,
- einem für die IT-Sicherheit zuständigen Mitarbeiters aus der AIT (IT-Sicherheitsbeauftragter) und
- sofern Sicherheitsaspekte des Kreisnetzes berührt werden: einem kommunalen EDV-Verantwortlichen.

Das IT-Sicherheitsmanagement führt regelmäßige, zumindest jedoch quartalsweise Sitzungen durch, in denen aktuelle Sicherheitsthemen behandelt werden.

Sofern erforderlich, werden anlassbezogen außerordentliche Sitzungen einberufen.

Die Sitzungen des IT-Sicherheitsmanagement werden in Form eines Ergebnisprotokolls dokumentiert.

2.2.4 Regelmäßige Kontrollen

Wesentliche Betriebsparameter und sicherheitskritische Einstellungen der verwendeten IT-Systeme werden automatisiert überwacht. Die Protokolle ausgewählter, sicherheitskritischer Komponenten werden auf einem zentralen Protokollserver abgelegt und ausgewertet.

Die auf dem Firewallsystem anfallenden Protokolle werden wöchentlich durch die Systemadministration kontrolliert.

Die Umsetzung, Einhaltung und Aktualität der IT-Sicherheitsleitlinie wird in regelmäßigen Abständen, zumindest jedoch jährlich, durch das IT-Sicherheitsmanagement überprüft.

Das IT-Sicherheitsmanagement prüft und bewertet die Umsetzung, Wirksamkeit und Angemessenheit der im Sicherheitskonzept getroffenen Sicherheitsmaßnahmen. Interne Audits sollen mindestens jährlich erfolgen, die Ergebnisse werden dokumentiert.

2.2.5 Anlassbezogene Kontrollen

Das IT-Sicherheitsmanagement kann anlassbezogen die Wirksamkeit und Angemessenheit einzelner Sicherheitsmaßnahmen prüfen. Die Ergebnisse der Prüfungen werden schriftlich festgehalten.

2.2.6 Verhalten bei Sicherheitsvorfällen

Die Kreisverwaltung Plön hat Sicherheitsvorfälle als Schadensereignisse unter Verstoß gegen die Sicherheits- und Datenschutzziele oder die im Sicherheitskonzept festgelegten Sicherheitsmaßnahmen definiert.

Sicherheitsvorfälle sind dem IT-Sicherheitsmanagement unverzüglich zu melden. Die Meldung hat durch die für den Betrieb und die Nutzung der IT-Verfahren verantwortlichen Personen zu erfolgen.

Das IT-Sicherheitsmanagement

- überprüft die mitgeteilte Bewertung des Sicherheitsvorfalls und der getroffenen Maßnahmen zur Schadensbeseitigung,
- veranlasst präventive Maßnahmen zur Risikominimierung (z. B. Überarbeitung des Sicherheitskonzeptes) und
- berichtet über Sicherheitsvorfälle dem Hauptamt.

Die Kreisverwaltung Plön hat die Vorgehensweisen zum Erkennen, Melden, Bearbeiten und Dokumentieren von Sicherheitsvorfällen und zur Schulung und Sensibilisierung der Beschäftigten in einer speziellen Richtlinie festgelegt.

2.2.7 Integration von Datenschutz und Datensicherheit

Es ist festgelegt, dass bei der Planung und Änderung von Verfahren zur Verarbeitung personenbezogener Daten die behördliche Datenschutzbeauftragte zu beteiligen ist. Die behördliche Datenschutzbeauftragte wirkt als Mitglied des IT-Sicherheitsmanagements an der Kontrolle und Weiterentwicklung der technischen und organisatorischen Sicherheitsmaßnahmen mit.

2.2.8 Administration

Alle administrativen Berechtigungen bzw. Zugänge sind in einem administrativen Berechtigungskonzept festgelegt.

Administratives Personal wird vor Aufnahme administrativer Tätigkeiten gesondert geschult.

Jede sicherheitskritische Konfigurationsänderung wird vorab durch den Leiter der Abteilung und dem zuständigen Administrator vorab evaluiert; die Umsetzung sowie abschließende Tests werden im Ticketsystem dokumentiert.

2.3 Informations- und Kommunikationstechnik

Die Nutzung der Dienste E-Mail und WWW erfolgt ausschließlich über einen zentralen Übergabepunkt in der Kreisverwaltung. Ausschließlich hier werden Verbindungen in andere Netze eingerichtet, die nicht unter Kontrolle der Kreisverwaltung Plön oder einer der angeschlossenen Kommunen stehen. Jegliche Verbindungen in andere Netze werden über diese Systeme geführt. Andere, parallele Netzverbindungen dürfen nicht hergestellt werden.

Das Netz der Kreisverwaltung Plön ist in unterschiedliche Netzzonen aufgeteilt, in denen einzelne Netze der Kreisverwaltung logisch zusammengefasst sind. Ziel ist die Berücksichtigung verschiedener Schutzbedarfe der einzelnen IT-Systeme (Server, Netzkomponenten, Clients etc.).

Durch diese Trennung werden zielgerichtet Dienste mit verschiedenen Sicherheitsanforderungen für die Kreisverwaltung und die angeschlossenen Kommunen umgesetzt und angeboten.

Das Netz und die zur Filterung und Weiterleitung des Datenverkehrs genutzten Systeme sind mehrstufig aufgebaut und stellen unter anderem eine sogenannte „demilitarisierte" Zone bereit, in der diejenigen Systeme aufgenommen werden, die Informationen für den Zugriff aus verwaltungsexternen Netzen bereitstellen.

Zwei Paketfilter bilden eine demilitarisierte Zone (DMZ), in die zum einen Application-Level-Gateways und zum anderen Mail- und Webserver eingebunden wurden.

Die Zugriffe auf die Application-Level-Gateways, die Mail- und Webserver werden durch die Paketfilter gesteuert.

2.3.1 Serverräume

Die IT-Systeme des Auditgegenstands sind in Serverräumen im Erdgeschoss und Keller der Kreisverwaltung untergebracht.

Die Serverräume sind mit einer Klimaanlage, Brandmeldeanlage und für den IT-Bereich zugelassenen Feuerlöschern ausgestattet.

Zutritt zum Serverraum haben die Administratoren der Abteilung Informationstechnik sowie die Leitung der Daten verarbeitenden Stelle. Außerhalb der normalen Geschäftszeiten sind die Serverräume sowie die angrenzenden Büros alarmgesichert.

2.3.2 IT-Systeme allgemein

Sämtliche aktive Komponenten werden ausschließlich über verschlüsselnde Protokolle oder aus eigens dafür eingerichteten administrativen Netzen verwaltet. Die Administrationszugänge sind nur von explizit freigeschalteten Arbeitsplätzen aus einem ausschließlich für administrative Zwecke genutzten Netzes zugänglich.

Jedes administrative System und die Application-Level-Gateways sind mit einem Virenscanner ausgestattet. Der Virenscanner wird zumindest täglich aktualisiert. Die korrekte Funktion des Virenscanners sowie seine Aktualität werden zentral überwacht.

Jedes System wird regelmäßig mit Patches, Bugfixes und ServicePacks versehen. Windows-Server nutzen hierzu die integrierten Funktionen für das automatische Systemupdate. Die Patches werden wöchentlich geprüft und nach erfolgreichem Test freigegeben. Linuxsysteme werden regelmäßig manuell mit Patches und Updates versehen. Die Paketfilter werden manuell aktualisiert.

Administrative Berechtigungen sind nach dem Minimalprinzip vergeben. Die Systeme sind gemäß den Sicherheitsvorgaben der Hersteller konfiguriert.

Die Daten jedes Servers werden auf Bandlaufwerke in mehreren Generationen gesichert. Die verwendeten Sicherungsbänder werden in einem feuersicheren Tresor aufbewahrt. Lediglich die Administration hat Zugriff auf die Datensicherungsbänder. Für jedes System sind ein Sicherungsplan und eine Anleitung zur Wiederherstellung hinterlegt.

Jedes IT-System hängt an einer unterbrechungsfreien Stromversorgung, die im Falle eines Stromausfalls für ein geordnetes Herunterfahren der Server sorgt.

Für die Systeme des Auditgegenstands hat die Kreisverwaltung auf Basis der BSI-Grundschutz-Kataloge angemessene und wirksame Sicherheitsmaßnahmen umgesetzt.

2.3.3 Netzübergänge

Die Kreisverwaltung Plön ist an das Kreisnetz, das Internet und an das Landesnetz Schleswig-Holstein angeschlossen.

Jeglicher Datenverkehr des internen Netzes der Kreisverwaltung sowie der über das Kreisnetz angeschlossenen Kommunen mit externen Netzen wird explizit an den Netzübergängen freigeschaltet. Es gilt das Prinzip: „Es ist alles verboten, was nicht ausdrücklich erlaubt ist."

Jeglicher Datenverkehr wird nicht nur auf seine Zulässigkeit, sondern auch auf schadhafte Inhalte wie Viren, Würmer und Trojaner geprüft.

Die Kreisverwaltung setzt hierfür eine Kombination aus Paketfiltern und mehreren Proxyservern ein. Die Paketfilter schalten dabei die einzelne Verbindungen zwischen dem Kreisnetz, dem Landesnetz oder dem Internet und Systemen der Kreisverwaltung sowie der über das Kreisnetz angebundenen Kommunen frei, während die Proxyserver die übertragenen Daten auf schadhafte Inhalte kontrollieren.

Das Design des Firewallsystems folgt aktuellen Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik („P-A-P-Architektur").

2.3.4 Paketfilter

Es werden zwei Paketfilter eingesetzt.

Die Paketfilter filtern den Netzverkehr auf Transportebene. Sie arbeiten als sogenannte „Stateful Packetfilter".

Die Paketfilterregeln sind durch detaillierte Kommentare in der Installations- und Konfigurationsdokumentation nachvollziehbar beschrieben. Die Dokumentation teilt sich in allgemeine Regeln für Datenverkehr für die Kreisverwaltung und die angeschlossenen Kommunen und spezielle Regeln für einzelne Kommunen. Die Dokumentation ist aussagekräftig und für sachkundige Personen in angemessener Zeit nachvollziehbar.

Die Konfiguration neuer Kommunikationsmöglichkeiten erfolgt grundsätzlich in Abstimmung mit dem Fachverfahrensverantwortlichen und dem zuständigen Systemadministrator der Abteilung Informationstechnik.

2.3.5 Aktive Netzkomponenten

Die Konfiguration der verwendeten aktiven Netzkomponenten wie Router und Switches ist minimalisiert und gesondert gehärtet. Für jede Netzkomponente sind die angeschlossenen IT-Systeme dokumentiert.

2.3.6 WLAN

Die Kreisverwaltung Plön betreibt ein WLAN (Wireless Local Area Network), das einen uneingeschränkten Webzugriff von externen, nicht im Verantwortungsbereich der Kreisverwaltung Plön liegenden mobilen Arbeitsgeräten (mobilen Clients) insbesondere in Besprechungsräumen ermöglichen soll.

Das WLAN ist vom internen Netz der Kreisverwaltung Plön abgeschottet und nur einem definierten Personenkreis zugänglich (z. B. Kreistagsabgeordnete, Presse). Personalisierte Nutzungsberechtigungen werden nur nach einmaliger Registrierung der jeweiligen Person in der Abteilung für Informationstechnik vergeben. Die personalisierte Nutzungsberechtigung wird entzogen, sobald die Person den Zugang nicht mehr benötigt.

Die verwendeten Access-Points sind minimalisiert konfiguriert und zusätzlich gehärtet. Die Installations- und Konfigurationsdokumentation ist angemessen und nachvollziehbar.

2.3.7 Application-Level-Gateways für E-Mail und WWW

Die Application-Level-Gateways werden grundsätzlich auf minimalisierten Serverinstallationen betrieben und unterliegen den in den vorherigen Abschnitten dargestellten allgemeinen Sicherheitsmaßnahmen.

FTP- und HTTP-Daten werden auf Viren, Würmer und Trojaner gescannt. Schadhafte Inhalte werden automatisch entfernt.

Schadhafte Daten oder Daten mit potentiellen Sicherheitsproblemen (im Allgemeinen ausführbare Dateien) im SMTP-Datenverkehr werden in ein Quarantäne-Postfach verschoben. Die Empfängerin oder der Empfänger in der Kreisverwaltung werden per E-Mail benachrichtigt und können durch die Systemadministration eine Zustellung der dann gesäuberten E-Mail veranlassen.

Unerwünschte E-Mailinhalte (Spam) werden zurückgehalten. Die Beschäftigten der Kreisverwaltung und der angeschlossenen Kommunen können auf Basis eines täglichen Berichts, der die zurückgehaltenen E-Mails auflistet, die Zustellung von falsch positiv als Spam eingestuften E-Mails veranlassen.

Die Konfiguration der Proxyserver erfolgt regelbasiert. Die auf den Systemen eingestellten Regeln sind nachvollziehbar dokumentiert. Angeschlossene Kommunen können grundsätzlich eigene Regelsätze vorhalten.

2.3.8 Mailserver

Die Kreisverwaltung Plön betreibt einen Mailserver, der für die Ablage und Weiterleitung von E-Mails sowohl von der Kreisverwaltung als auch von den angeschlossenen Kommunen genutzt wird.

Die Löschfristen der auf dem Mailserver anfallenden Protokolldaten entsprechen den Vorgaben der Konzepte und der mit den Kommunen geschlossenen Nutzungsvereinbarungen.

Das Mailsystem ist gemäß Herstellervorgaben installiert und konfiguriert. Zusätzlich hat die Kreisverwaltung eigene Sicherheitsmaßnahmen getroffen, um einen unautorisierten Zugriff auf Postfächer einzelner Benutzer zu verhindern. Die vergebenen Berechtigungen sind minimalisiert und gemäß den konzeptionellen Vorgaben umgesetzt.

2.3.9 Blackberry-Serversystem

Die Kreisverwaltung bietet eigenen Mitarbeitern und Beschäftigten der angeschlossenen Kommunen die Nutzung eines Dienstes zur mobilen Verarbeitung von E-Mails, Kontaktdaten und Terminen der Firma Blackberry an. Die Installation und Konfiguration des Blackberry-Dienstes folgt den Sicherheitsvorgaben des Herstellers. Die direkt mit externen Netzen kommunizierenden Komponenten der Lösung sind von den datenhaltenden Bestandteilen netztechnisch getrennt worden. Der Datenverkehr ist auf die zwingend notwendigen Verbindungen eingeschränkt. Die für den

Dienst notwendigen Berechtigungen sind minimal vergeben.

2.3.10 Verzeichnisdienst

Die Kreisverwaltung verwendet zur Administration der Betriebssysteme und Anwendungen der Firma Microsoft den Verzeichnisdienst „Active Directory“. Die Berechtigungen im Active Directory sind gemäß Herstellervorgaben und den Vorgaben der BSI-Grundschutz-Kataloge minimalisiert vergeben. Die Protokolle des Active Directories werden regelmäßig ausgewertet. Wesentliche Sicherheitseinstellungen werden automatisiert überwacht.

Die für den Verzeichnisdienst genutzten Serversysteme sind speziell für diesen Einsatzzweck gehärtet worden. Für den Verzeichnisdienst sind spezielle Maßnahmen zur Datensicherung und -wiederherstellung getroffen worden.

3 Datenschutzrechtliche Bewertung

Die automatisierte Verarbeitung personenbezogener Daten erfordert technische und organisatorische Maßnahmen, die die Datensicherheit bzw. die Ordnungsmäßigkeit der Datenverarbeitung gewährleisten. Des Weiteren sind interne Regelungen zu treffen, die insbesondere personelle und organisatorische Aspekte mit einbeziehen. Es muss zudem gewährleistet sein, dass die datenschutzrechtlichen Anweisungen auch tatsächlich in konkrete Datensicherungsmaßnahmen umgesetzt werden und ihre Einhaltung durch das IT-Sicherheitsmanagement kontrolliert wird. 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
- § 9 Vorabkontrolle
- § 10 Behördliche Datenschutzbeauftragte

Datenschutzverordnung (DSVO)

- § 3 Verfahrensdokumentation
- § 4 Dokumentation der Sicherheitsmaßnahmen
- § 5 Dokumentation des Tests und der Freigabe

Zusätzlich sind bereichsspezifische rechtliche Regelungen regelmäßig daraufhin zu prüfen, ob detaillierte Vorgaben zu Aufbewahrungsfristen, Dokumentationsvorgaben oder Löschfristen bestehen oder sich geändert haben.

Die behördliche Datenschutzbeauftragte verfügt über die erforderliche Sachkunde und Zuverlässigkeit. Ihre Bestellung steht in keinem Konflikt mit anderen dienstlichen Aufgaben.

Die Überprüfung hat ergeben, dass die im Sicherheitskonzept festgeschriebenen Maßnahmen angemessen sind und vollständig umgesetzt werden.

Die durch dieses Audit erfassten Verarbeitungsprozesse zeichnen sich insbesondere durch folgende „datenschutzfreundliche" Aspekte aus:

- Zum Schutz vor Angriffen von außen wurden die Übergänge vom internen Verwaltungsnetz zum Internet mit abgestuften Firewallsystemen ausgestattet.
- Überwachung und Administration der eingesetzten Firewallkomponenten werden ausschließlich von der Kreisverwaltung durchgeführt.
- Die ergriffenen Sicherheitsmaßnahmen werden regelmäßig von qualifizierten Mitarbeitern auf ihre Wirksamkeit hin überprüft.
- Veränderungen der Sicherheitseinstellungen bedürfen nach Abstimmung mit dem IT-Sicherheitsmanagement und der behördlichen Datenschutzbeauftragten der Zustimmung des Leiters der IT-Abteilung.
- Alle Einstellungen auf den Paketfiltern und Application-Level-Gateways werden nachvollziehbar dokumentiert.
- Nicht zugelassene Zugriffe werden protokolliert und abgewehrt. Bei Ereignissen von sicherheitsrelevanter Bedeutung werden gesonderte Warnmeldungen ausgegeben.
- Eine Fernadministration der Firewallkomponenten ist nicht gestattet.
- Es werden nur solche E-Mails an den Arbeitsplatz geleitet, die virenüberprüft sind und zugelassene Anhänge enthalten.
- Der Zugriff auf die Webseiten wird in Bezug auf die sicherheitskritischen Komponenten ActiveX, Java und VBScript gefiltert.
- Schadhafte Inhalte in Webseiten oder E-Mails werden gefiltert und gegebenenfalls für den Aufruf oder die Weiterleitung nicht zugelassen.

Die Prüfung hat ergeben, dass das Konzept und die Anwendung des Datenschutzmanagementsystems keinen Anlass zu datenschutzrechtlichen Beanstandungen geben.

Kiel, 23.03.2010 (Sven Thomsen)