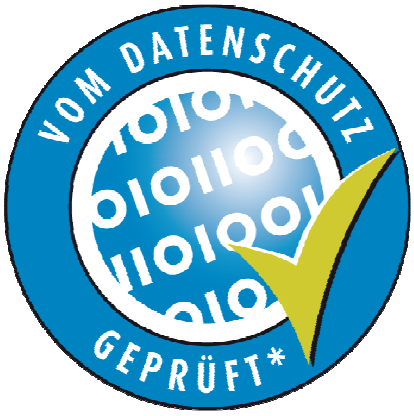

Kurzgutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Stadt Flensburg:

Anbindung des internen Netzwerks an andere Netzwerke

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Datum:	18.04.2008
Aktenzeichen:	16.01/05.010
Telefon:	0431/988-1211
Fax	0431/988-1223
E-Mail:	mail@datenschutzzentrum.de

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Audits

1.1 Vereinbarung

Grundlage dieses Datenschutz-Audits ist der Audit-Vertrag zwischen der Stadtverwaltung Flensburg und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein vom 23.03.2006.

Gegenstand des Datenschutz-Audits ist die Anbindung des verwaltungsinternen Netzes der Stadtverwaltung an andere Netzwerke.

1.2 Datenschutzziele

Die Stadtverwaltung Flensburg hat die folgenden Datenschutzziele festgelegt:

- Beachten der Rechtmäßigkeit und Ordnungsmäßigkeit der Datenverarbeitung
- Beachten der Grundsätze der Ordnungsmäßigkeit des Verwaltungshandelns
- Wahrung des Rechts der Bürgerinnen und Bürger auf informationelle Selbstbestimmung
- Datensparsame Durchführung der Datenverarbeitung
- Sicherstellen der Verfügbarkeit der verwendeten Systeme und Programme
- Aufrechterhalten der Integrität der Systeme und insbesondere der gespeicherten personenbezogenen Daten
- Gewährleisten der Vertraulichkeit der verarbeiteten Daten, insbesondere der Schutz des verwaltungsinternen Netzes gegen unbefugten Zugriff aus anderen, nicht-vertrauenswürdigen Netzen
- Beachten von wirtschaftlichen oder haushaltsrechtlichen Obliegenheiten
- Schutz vor ungewünschtem Datenabfluss

Diese Ziele sind durch die Daten verarbeitenden Stelle im Rahmen eines speziellen Sicherheitskonzepts festgelegt worden.

2 Feststellung zu den sicherheitstechnischen Elementen des Datenschutz-Managementsystems

2.1 Dokumentation

Die Stadtverwaltung Flensburg wählt für die Dokumentation der automatisierten Datenverarbeitung gemäß DSVO einen strukturierten Ansatz. Dieses Vorgehen wurde im Rahmen des Auditverfahrens entwickelt und erstmalig anhand des verwendeten Firewallsystems umgesetzt. Die Stadtverwaltung ist bestrebt, auch weitere Verfahren nach diesem einheitlichen Vorgehen zu dokumentieren.

In einem „Stammordner“ werden sämtliche allgemeinen, verfahrens- und systemübergreifenden Aspekte der Datenverarbeitung zusammengefasst.

Darüber hinaus werden im Stammordner große Teile der verfahrensübergreifenden Dokumentation und Protokolle gemäß § 8 DSVO geführt. Die system- oder verfahrensspezifischen Teile sind dann in einzelnen System- oder Verfahrensakten aufgeführt.

Grundsätzlich werden möglichst viele Aspekte der Verarbeitung personenbezogener Daten in allgemeinen Sicherheits- und IT-Konzepten zusammengefasst.

Für das Firewallsystem wurden im Rahmen eines speziellen IT-Konzepts gemäß § 4 DSVO die technischen und organisatorischen Vorgaben sowie die erzielbaren Ergebnisse dokumentiert.

Basierend auf dem speziellen IT-Konzept findet sich dann in einem speziellen Sicherheitskonzept eine Dokumentation der für das Firewallsystem getroffenen Sicherheitsmaßnahmen gemäß § 6 DSVO.

In einer Restrisikoanalyse wurden diejenigen Sicherheitsrisiken dokumentiert, die nicht oder nur zum Teil durch die im Sicherheitskonzept dokumentierten Maßnahmen ausgeschlossen werden können.

2.1.1 Systemakten

Für die Führung der Systemakten ist der Administrator des Firewallsystems verantwortlich.

Die Stadtverwaltung hat für jedes Serversystem und jede aktive Netzkomponenten des Firewallsystems eine Systemakte eingeführt. In den Systemakten werden neben der Bezeichnung des jeweiligen Systems, dem Standort des Systems und der Einbindung in das Netzwerk zusätzlich sämtliche auf dem System installierten Programme dokumentiert.

Zu Zwecken der Inventarisierung und fortlaufenden administrativen Protokollierung der administrativen Tätigkeiten wird ein kombiniertes Inventarisierungs- und Ticketsystem verwendet. In diesem System werden regelmäßige und anlassbezogene Tätigkeiten an den Systemen dokumentiert.

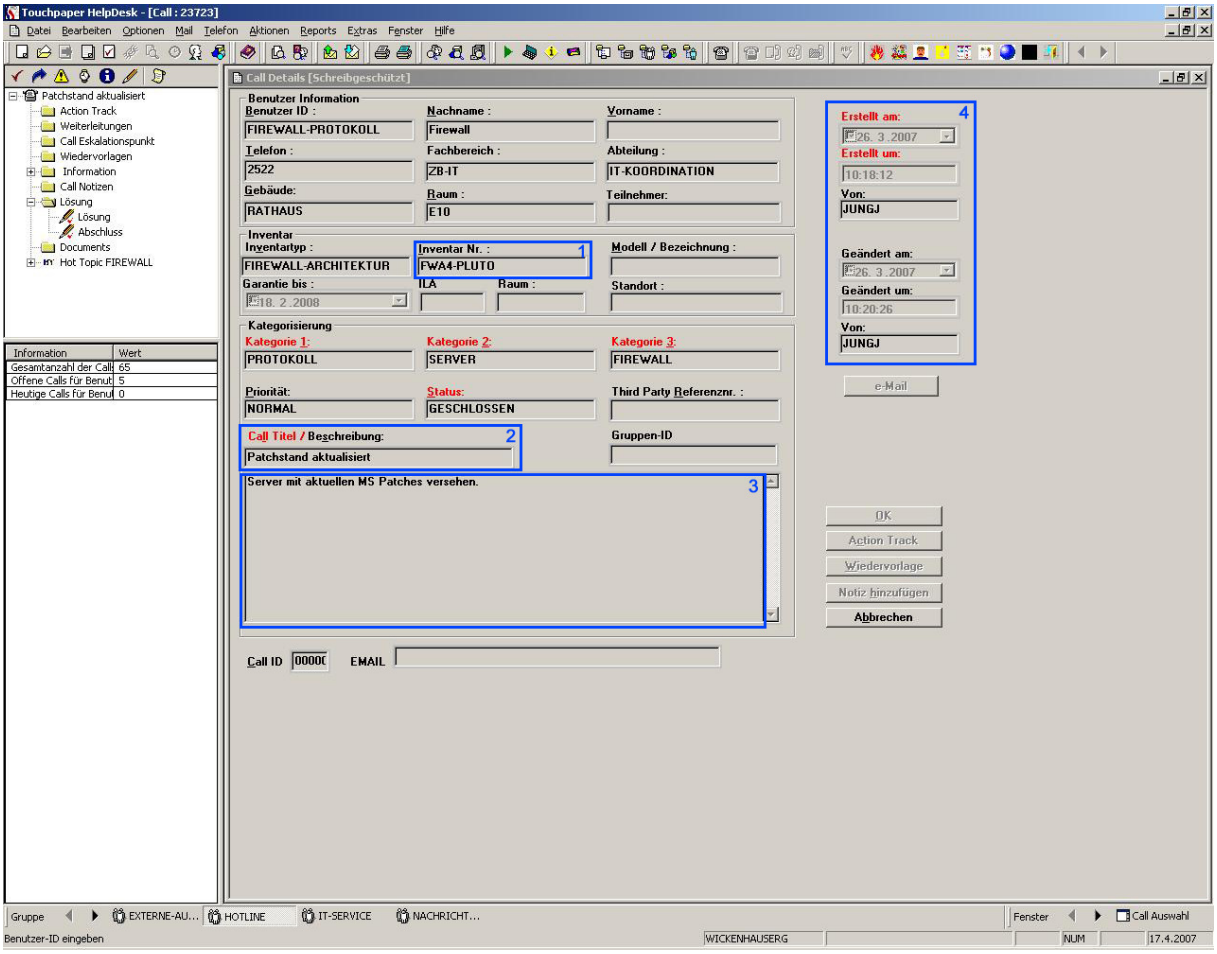

Abbildung 1: Beispieleintrag im Ticketsystem

Für jedes System wird zusätzlich regelmäßig eine Dokumentation der administrativen Tätigkeiten im Sinne des § 8 Abs. 5 DSVO in der jeweiligen Systemakte abgelegt.

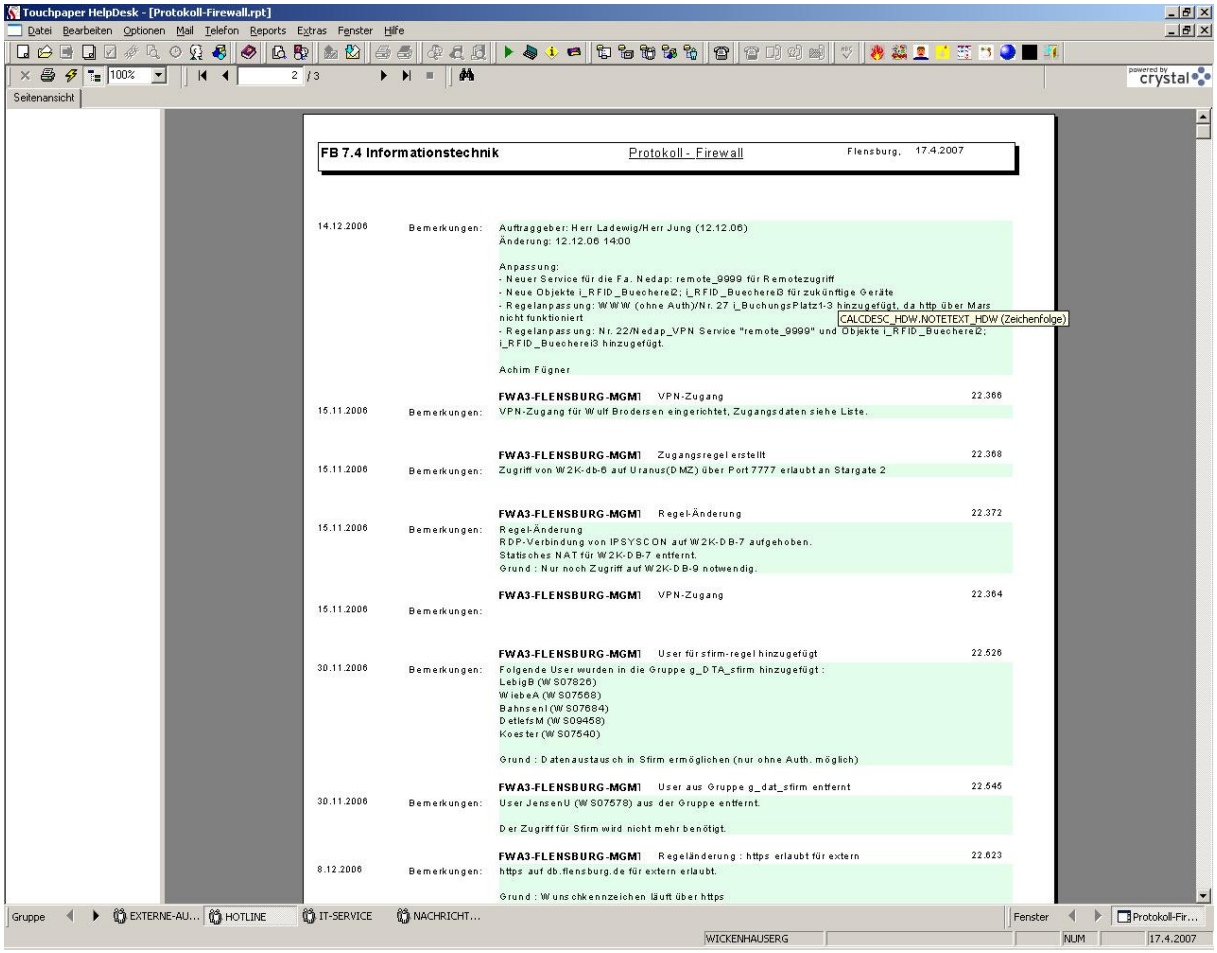

Abbildung 2: Auszug aus der administrativen Protokollierung

Für jedes Server-System werden die notwendigen Schritte für einen Wiederanlauf im Falle eines Komplettausfalls in der Serverakte vorgehalten. Die Notfalldokumentation ist so angelegt, dass ausgehend von der Wiederbeschaffung eines Ersatz-Systems alle notwendigen Installations- und Konfigurationsarbeiten enthalten sind.

2.1.2 Verfahrensakten

Die Pflege der Verfahrensakten für das Firewallsystem erfolgt durch den Administrator.

In der Verfahrensakte ist neben allgemeinen Informationen zum Firewallsystem ein Berechtigungskonzept im Sinne einer Dokumentation der vergebenen Rechte gemäß § 8 Abs. 4 DSVO enthalten.

Die Verfahrensakte dokumentiert darüber hinaus die gemäß § 7 DSVO durchgeführten Test- und Freigabeverfahren für das Firewallsystem.

2.1.3 Spezielles IT-Konzept

Die Stadtverwaltung hat die technischen und organisatorischen Vorgaben für die allgemeine Verarbeitung personenbezogener Daten in einem informationstechnischen Konzept gemäß § 4 DSVO zusammengefasst.

Neben Vorgaben für die Server-, Client- und Netzwerkinfrastruktur sind im IT-Konzept die Obliegenheiten der Systemadministration festgelegt.

2.1.4 Spezielles Sicherheitskonzept

Im speziellen Sicherheitskonzept für das Firewallystem der Stadtverwaltung Flensburg werden die technischen und organisatorischen Maßnahmen dargestellt, die seitens der Stadtverwaltung getroffen worden sind.

Das Sicherheitskonzept enthält Maßnahmen zu:

- den Räumen und den Gebäuden,
- den verwendeten IT-Systemen,
- einer nachvollziehbaren Administration der Systeme,
- den Übergängen in andere Netzwerke,
- den verwendeten Paketfiltern,
- den verwendeten Application-Level-Gateways,
- den Webservern und zu
- der vorliegenden Datenverarbeitung im Auftrag.

Zusätzlich sind die sicherheitsrelevanten Regelungen bezüglich der Administration der Systeme, Maßnahmen zur Notfallvorsorge und dem Verhalten bei Sicherheitsvorfällen enthalten.

Das Sicherheitskonzept beschreibt darüber hinaus die regelmäßigen und anlassbezogenen Kontrolltätigkeiten des behördlichen Datenschutzbeauftragten und des Leiters der Abteilung Informationstechnik.

2.1.5 Dienstanweisungen

Die im speziellen IT-Konzept und Sicherheitskonzept festgelegten technischen und organisatorischen Vorgaben sowie die Sicherheitsmaßnahmen werden durch mehrere Dienstanweisungen in geltende Anweisungen an die Beschäftigten der Stadtverwaltung umgesetzt.

In einer speziellen Dienstanweisung zur Nutzung der Internet-Dienste ist zunächst geregelt, dass die Internet-Dienste ausschließlich für die dienstliche Nutzung zur Verfügung gestellt werden, eine private Nutzung ist ausdrücklich verboten. Es ist geregelt, wie die Kontrolle dieses Verbots unter Beteiligung des Datenschutzbeauftragten und unter Wahrung der Rechte der Personalvertretung durchgeführt wird. Zusätzlich ist eine enge Zweckbindung für die Protokolldaten der Internetnutzung festgelegt, die eine Auswertung zu Zwecken der automatisierten Verhaltens- und Leistungskontrolle ausdrücklich untersagt.

Für die E-Mail-Nutzung in der Stadtverwaltung ist eine spezielle Dienstanweisung eingeführt worden. Genau wie die allgemeine Internetnutzung ist die Nutzung von E-Mail nur zu dienstlichen Zwecken erlaubt. Die bei der E-Mail-Nutzung anfallenden Protokolldaten sind detailliert beschrieben. Eine Missbrauchskontrolle findet nur unter Beteiligung des Datenschutzbeauftragten und unter Einschaltung des Personalrats statt. Die Protokolldaten unterliegen einer engen Zweckbindung und dürfen nur zur Analyse und Korrektur technischer Fehler und zur Gewährleistung der Systemsicherheit verwendet werden.

2.2 Aufbau und Ablauforganisation

2.2.1 Allgemeine Geschäftsverteilung

Die Stadtverwaltung Flensburg gliedert sich in sieben Fachbereiche:

- Fachbereich 1: Bürgerservice, Schutz und Ordnung
- Fachbereich 2: Jugend, Soziales, Gesundheit
- Fachbereich 3: Bildung, Kindertagesbetreuung, Kultur, Sport
- Fachbereich 4: Umwelt und Planen
- Fachbereich 5: Infrastruktur
- Fachbereich 6 Kommunale Immobilien
- Fachbereich 7: Zentrale Dienstleistungen

Die Abteilung Informationstechnik ist dem 1. Bürgermeister direkt unterstellt.

2.2.2 Abteilung Informationstechnik

Die Abteilung Informationstechnik wird durch Herrn Dr. Marcus Ott geleitet.

Die Administration der für die Anbindung des verwaltungsinternen Netzwerks an andere Netze genutzten Systeme wird von Herrn Jan Jung durchgeführt. Perspektivisch wird Herr Lennart Bobrowski diese Aufgabe ab Juli 2007 wahrnehmen.

Herr Jung und Herr Bobrowski werden in Fragen des Datenschutzes, der Datensicherheit und Einzelfragen der ordnungsgemäßen Datenverarbeitung durch den behördlichen Datenschutzbeauftragten beraten.

2.2.3 Datenschutzbeauftragter

Als behördlicher Datenschutzbeauftragter ist Herr Hesebeck benannt.

Herr Hesebeck arbeitet in seiner Funktion als Datenschutzbeauftragter weisungsfrei und ist dem Oberbürgermeister direkt unterstellt.

2.2.4 Regelmäßige Kontrollen

Die Abteilung Informationstechnik setzt für die Anbindung des verwaltungsinternen Netzwerks an andere Netze ein Firewallsystem ein, welches aus mehreren Systemen besteht.

Im speziellen Sicherheitskonzept für das verwendete Firewallsystem ist festgelegt, dass der Leiter der Abteilung Informationstechnik in Zusammenarbeit mit dem behördlichen Datenschutzbeauftragten die Angemessenheit und Wirksamkeit der getroffenen Sicherheitsmaß-

nahmen zumindest einmal jährlich überprüft.

Die Stadtverwaltung gliedert die Dokumentation gemäß DSVO in Verfahrens- und Systemakten. Im Rahmen einer jährlichen Fortschreibung werden die Systemakten und Verfahrensakten durch den Leiter der Abteilung Informationstechnik in Zusammenarbeit mit dem behördlichen Datenschutzbeauftragten auf Vollständigkeit und Aktualität geprüft.

Die Ergebnisse der regelmäßigen Kontrollen werden in den jeweiligen System- und Verfahrensakten dokumentiert.

Zusätzlich zu den eigenen, internen Kontrollen gibt die Stadtverwaltung externe Sicherheitsaudits in Auftrag. Im Zeitraum der Auditierung wurde eine externe Untersuchung durchgeführt.

2.2.5 Anlassbezogene Kontrollen

Ergeben sich durch Berichterstattung in der Fachpresse, aufgrund von Meldungen der Softwarehersteller oder aus anderen Publikationen Hinweise, dass die Stadtverwaltung Flensburg ihre Sicherheitskonzeption neu prüfen muss, so führt der Datenschutzbeauftragte in Zusammenarbeit mit dem Leiter der Abteilung Informationstechnik eine entsprechende Prüfung durch.

Die Ergebnisse dieser Kontrollen werden dokumentiert.

2.2.6 Verhalten bei Sicherheitsvorfällen

Die Stadtverwaltung hat im Sicherheitskonzept festgelegt, welche Kriterien auf einen Sicherheitsvorfall schließen lassen und wie ein möglicher Sicherheitsvorfall zu bearbeiten ist.

Die Bearbeitung erfolgt in zwei Schritten. Im ersten Schritt wird die Behebung des Sicherheitsvorfalls durch Sofortmaßnahmen durchgeführt. Sämtliche getroffenen Maßnahmen werden dokumentiert. Im zweiten Schritt wird der Sicherheitsvorfall nachbereitet und eine abschließende Dokumentation des Vorfalls erstellt.

2.2.7 Integration von Datenschutz und Datensicherheit in das Verwaltungshandeln

Der Datenschutzbeauftragte wird bei jeder Beschaffung von Informations- und Kommunikationstechnologie beteiligt. Es ist festgelegt, dass bei der Planung und Änderung von Verfahren zur Verarbeitung personenbezogener Daten der behördliche Datenschutzbeauftragte zu beteiligen ist.

2.2.8 Administration

Die Arbeit der Systemadministration ist durch eine spezielle Dienstanweisung geregelt.

Jegliche administrativen Berechtigungen bzw. Zugänge sind in einem administrativen Be-

rechtigungskonzept festgelegt.

Administratives Personal wird vor Aufnahme administrativer Tätigkeiten gesondert geschult.

Die auf dem Firewallsystem anfallenden Protokolle werden wöchentlich durch die Systemadministration kontrolliert. Die Auswertung muss im Ticketsystem der Abteilung Informationstechnik dokumentiert werden.

Jede sicherheitskritische Konfigurationsänderung wird zwischen dem Leiter der Abteilung und dem zuständigen Administrator vorher besprochen und die Umsetzung sowie abschließende Tests im Ticketsystem dokumentiert.

Fernwartung bzw. Fernadministration durch externe Dienstleister ist erst nach Freischaltung durch die Administration möglich. Durch einen geregelten Beauftragungsprozess wird Art und Umfang der Fernwartungstätigkeiten vor Durchführung definiert, während der Durchführung vom Dienstleister dokumentiert und nach der Durchführung geprüft und freigegeben.

2.3 Firewallsystem

Das Firewallsystem ist als zentraler Übergabepunkt in andere Netze eingerichtet, die nicht unter Kontrolle der Stadtverwaltung Flensburg stehen. Jegliche Verbindungen in andere Netzwerke werden über dieses System geführt. Andere, parallele Netzverbindungen dürfen nicht hergestellt werden.

Das System wird mehrstufig aufgebaut und stellt eine sogenannte „demilitarisierte“ Zone bereit, in der diejenigen Systeme aufgenommen werden, die Informationen für den Zugriff aus verwaltungsexternen Netzen bereitstellen.

2.3.1 Serverräume

Die Komponenten des Firewallsystems sind in Serverräumen im Erdgeschoss und Keller des Rathauses untergebracht.

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

2.3.2 IT-Systeme allgemein

Sämtliche aktiven Komponenten werden ausschließlich über verschlüsselte Protokolle administriert.

Jedes System ist mit einem Virenscanner ausgestattet. Der Virenscanner wird zumindest täglich aktualisiert. Die korrekte Funktion des Virenscanner 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. Novellsysteme werden regelmäßig manuell mit Patches und Updates versehen. Die Paketfilter werden über das zentrale Managementsystem mit Aktualisierungen versehen.

Jedes Serversystem ist mit einem RAID-System und redundanten Netzteilen ausgestattet.

Die Daten jedes Servers werden auf Bandlaufwerke in mehreren Generationen gesichert. Die verwendeten Sicherungsbänder werden in einem feuersicheren Tresor aufbewahrt. Für jedes System sind ein Sicherungsplan und eine Anleitung zur Wiederherstellung in der jeweiligen Systemakte hinterlegt. Jedes IT-System hängt an einer unterbrechungsfreien Stromversorgung, die im Falle eines Stromausfalls für ein geordnetes Herunterfahren der Server sorgt.

2.3.3 Netzwerkübergänge

Die Stadtverwaltung Flensburg ist an das Landesnetz Schleswig-Holstein angeschlossen. Sämtliche verfügbaren Sicherheitsmaßnahmen werden umgesetzt. Hierzu zählen die Prüfung des Berichtswesens, der Zugang zum webbasierten Auskunftssystem LNWebView und die Nutzung des Überwachungsprogramms „LNRC – Landesnetz Router Control".

Die Stadtverwaltung ist über den Internetprovider Versatel an das Internet angeschlossen. Versatel trifft für die Stadtverwaltung keine eigenen Sicherheitsmaßnahmen.

Jeglicher Datenverkehr des verwaltungsinternen Netzes mit externen Netzwerken 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 Stadtverwaltung setzt hierfür eine Kombination aus Paketfiltern, die einzelne Verbindungen zwischen anderen Netzen und Systemen der Stadtverwaltung freischaltet, und mehreren Proxyservern ein, die die übertragenen Daten auf schadhafte Inhalte kontrollieren.

Das Design des Firewallsystems folgt aktuellen Empfehlungen z.B. des Bundesamts für Sicherheit in der Informationstechnik.

2.3.4 Paketfilter

Die Konfiguration der Paketfilter wird an zentraler Stelle über ein Managementsystem durchgeführt.

Auf dem Managementsystem findet eine Protokollierung der durchgeführten Änderungen statt. Es bietet die Möglichkeit den aktuellen Status der Systeme vor einer Änderung zu sichern.

Die Paketfilter filtern den Netzwerkverkehr auf Transportebene. Sie arbeiten als sogenannte „stateful packetfilter".

Darüber hinaus bieten die Systeme Funktionen zur Erkennung von netzbasierten Angriffen und die Möglichkeit, Sicherheitsprobleme nachgelagerter Systeme an zentraler Stelle durch Filtern problematischen Netzwerkverkehrs temporär zu beheben.

Die Paketfilterregeln sind durch detaillierte Kommentare in der Systemakte dokumentiert.

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

Die Paketfilter werden vom zentralen Managementsystem mit Patches und Updates versorgt und sind durch dieses zentrale Management im Falle eines Systemausfalls wiederherstellbar.

2.3.5 Proxyserver 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 Stadtverwaltung 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 Stadtverwaltung erhalten täglich mehrere „Spamberichte“. Sie können die Zustellung von falsch positiv als Spam erkannten E-Mails veranlassen. Nicht angeforderte Mails werden nach 30 Tagen gelöscht.

3 Datenschutzrechtliche Bewertung

3.1 Rechtsvorschriften

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 Datenschutz-Management 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

Datenschutzverordnung (DSVO)

- § 3 Verfahrensdokumentation
- § 4 Verfahrenszweck
- § 5 Verfahrensbeschreibung
- § 6 Sicherheitskonzept
- § 7 Test und Freigabe
- § 8 Verfahrensübergreifende Dokumentation und Protokolle

Die folgenden Bedingungen müssen somit den Datenschutzzielen der Stadtverwaltung folgend eingehalten werden:

- Es sind die Vorschriften über Berufs- und besondere Amtsgeheimnisse unter Berücksichtigung der bereichsspezifischen Gesetze zu beachten (z.B. § 30 AO, § 35 SGB I, § 38 LMG, § 203 StGB).
- Die Daten verarbeitende Stelle hat den Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten (§ 4 Abs. 1 LDSG).
- Unbefugten ist der Zugang zu Datenträgern, auf denen personenbezogene Daten gespeichert sind, zu verwehren (§ 5 Abs. 1 Nr. 1 LDSG).

- Es ist zu verhindern, dass personenbezogene Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können (§ 5 Abs. 1 Nr. 2 LDSG).
- Die sicherheitstechnischen Anforderungen an die automatisierte Datenverarbeitung sind in einem Sicherheitskonzept festzulegen und umzusetzen (§ 5 Abs. 3 LDSG i.V.m. § 6 DSVO).
- Die Verarbeitung personenbezogener Daten wird erst ermöglicht, nachdem systemseitig die Berechtigung der Benutzer festgestellt worden ist (§ 6 Abs. 1 LDSG).
- Die Befugnisse zur Systemadministration sind eindeutig festgelegt (§ 6 Abs. 2 LDSG i.V.m. § 8 Abs. 4 u. 5 DSVO).
- Die Arbeiten der Systemadministratoren werden protokolliert und kontrolliert (§ 6 Abs. 2 LDSG).
- Die Hardware und die Software sind in einem Geräte- bzw. Softwareverzeichnis erfasst (§ 8 Abs. 1 u. 2 DSVO).
- Es ist zu dokumentieren, welchen Personen welche Zugriffsbefugnisse auf Datenbestände gewährt wurden (§ 8 Abs. 4 DSVO).
- Automatisierte Verfahren sind vor ihrem erstmaligen Einsatz und nach Änderungen zu testen und durch die Bürgermeisterin oder dem Bürgermeister als Daten verarbeitenden Stelle oder von ihr / ihm befugte(n) Person(en) freizugeben (§ 5 Abs. 2 LDSG i.V.m. § 7 DSVO).
- Die automatisierten Verfahren sind so zu dokumentieren, dass sie für sachkundige Personen in angemessener Zeit nachvollziehbar sind und als Grundlage für die Überwachung der automatisierten Datenverarbeitung herangezogen werden können (§ 6 Abs. 5 i.V.m. § 3 DSVO).
- Die ordnungsgemäße Anwendung der Datenverarbeitung ist zu überwachen (§ 6 Abs. 5 LDSG).

3.2 Zusammenfassende Bewertung

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

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

- Die Stadtverwaltung Flensburg hat eine gut strukturierte, systematische und übersichtliche Dokumentation gemäß DSVO erstellt. Diese bietet eine effektive Arbeitsgrundlage für das behördliche Datenschutzmanagementsystem.
- Der Umgang mit schadhaften Inhalten sowie die Bearbeitung unerwünschter E-Mails ist korrekt, datensparsam und für die Mitarbeiterinnen und Mitarbeiter der Stadtverwaltung transparent und nachvollziehbar geplant und umgesetzt.
- Sämtlicher Datenverkehr mit dem Internet wird sowohl auf Inhalts- als auch auf Netzwerkebene kontrolliert. Die dabei anfallenden Protokolldaten werden nach einem geregelten Verfahren unter Beteiligung des behördlichen Datenschutzbeauftragten ausgewertet.

Die Prüfung hat ergeben, dass Konzepte und Anwendung des Datenschutz-Managementsystems keinen Anlass zu datenschutzrechtlichen Beanstandungen geben.

Kiel, 18.04.2008 (Dr. Martin Meints)