LD31 –16.01/02.008 Kiel, 16. Juni 2004

Kurzgutachten

über das Auditverfahren gemäß § 43 Abs. 2 LDSG

Verarbeitung personenbezogener Daten mit IT-Systemen in der Stadtverwaltung Bad Schwartau

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Behördenaudits

Das Unabhängige Landeszentrum für Datenschutz (ULD) und die Stadtverwaltung Bad Schwartau haben am 28.10.2002 eine Vereinbarung getroffen, aufgrund der ein **Behördenaudit** bezogen auf das Projekt

- „**Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung der Stadt Bad Schwartau ohne Berücksichtigung der Rechtmäßigkeit der Datenverarbeitung in den einzelnen Fachverfahren der Fachämter“** und

- **„Anschluss des internen Netzes der Stadtverwaltung an das Internet“**

durchgeführt werden soll.

Als **Datenschutzziele** wurden von der Leitungsebene der Stadtverwaltung

- die technische und organisatorische Umsetzung von Sicherheitsmaßnahmen für die interne automatisierte Datenverarbeitung und für den Anschluss des internen Netzes an das Internet,

- der ausreichende Schutz der automatisiert verarbeiteten Daten vor Angriffen aus dem Internet sowie

- ein hinreichend sicherer Transport der über die Internetdienste „E-Mail“ und „WWW“ versendeten bzw. empfangenen Daten

festgelegt.

Die **Realisierung** der Sicherheitsmaßnahmen umfasste daher folgende Teilaspekte:

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

b) Festlegung der entsprechenden Zuständigkeiten und Verantwortungsabgrenzungen,

c) Ausgestaltung der technischen und organisatorischen Maßnahmen zur Datensicherheit der IT-Systeme,

d) Festlegung der technischen und organisatorischen Maßnahmen bei der Nutzung der Internetdienste,

e) Definition der Maßnahmen zur Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme,

f) Gewährleistung der Vollständigkeit der Dokumentation der Programme und Verfahren.

2 Feststellungen zu den sicherheitstechnischen Elementen des Datenschutz-Managementsystems

2.1 Zuständigkeiten und Verantwortlichkeiten

Die **Gesamtverantwortung** für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung trägt der Bürgermeister als Leiter der Daten verarbeitenden Stelle. Für die Einhaltung der **Vorschriften** zum Datenschutz und zur Datensicherheit in den **Fachämtern** sind die Amtsleiter zuständig und verantwortlich.

Die **Überwachung** und **Prüfung** der in den Sicherheitskonzepten festgelegten Sicherheitsmaßnahmen obliegt dem Datenschutzbeauftragten.

Die Schaffung der Voraussetzungen für den Einsatz und die Überwachung des laufenden Betriebs der IT-Systeme obliegt den IT-Koordinatoren. Die durchzuführenden Arbeiten dieser Mitarbeiter werden prinzipiell als **Dienstleistungen** für die **Fachämter** angesehen.

2.2 Datenschutzkonzept

Als Grundlage für die Festlegung der Sicherheitsmaßnahmen wurde zunächst ein **IT-Konzept** erstellt. Es wurde am 22.12.2003 vom Bürgermeister in Kraft gesetzt. Zusätzlich wurden in einzelnen Fachbereichen weitere Erhebungen über **Arbeitsabläufe** sowie über **den Hard- und Softwarebe-**

stand vorgenommen.
Auf dieser Basis wurden die erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen in einem umfassenden **Sicherheitskonzept** festgelegt. Es gliedert sich in die Bereiche

- Grundlagen und Aufbau,
- allgemeine Datenverarbeitung,
- automatisierte Datenverarbeitung,
- Internetdienste und
- Telekommunikationsdienste.

Die festgelegten Sicherheitsmaßnahmen gelten als **Mindestanforderungen** für alle Fachämter. Das Sicherheitskonzept wurde der Leitungsebene (Bürgermeister, Amtsleiter) vorgelegt und mit ihr im Rahmen einer Präsentation erörtert. Es wurde vom Bürgermeister mit Wirkung vom 23.12.2003 in Kraft gesetzt.

2.3 Automatisierte Datenverarbeitung

Die automatisierte Datenverarbeitung wird im Bereich der Stadtverwaltung auf der Basis eines **Terminalserver-Konzeptes** abgewickelt. Dieses Konzept beruht darauf, dass Rechenvorgänge und Softwareanwendungen sowie die mit ihnen verarbeiteten Daten zentral auf einem Rechner abgearbeitet werden. Der Arbeitsplatz-PC des Benutzers dient für Ein- und Ausgabevorgänge nur noch als Verbindungssystem. Für diesen Zweck benötigt der PC selbst keine leistungsstarke Hardware und keine spezielle Softwareintelligenz. Beim Client kann es sich um einen normalen PC mit einer speziellen Client-Software (Terminalserver-Client) oder um ein dediziertes Windows-Terminal (Thin Client) handeln. Derzeit werden bei der Stadtverwaltung sowohl abgerüstete PC als auch Thin Clients eingesetzt.

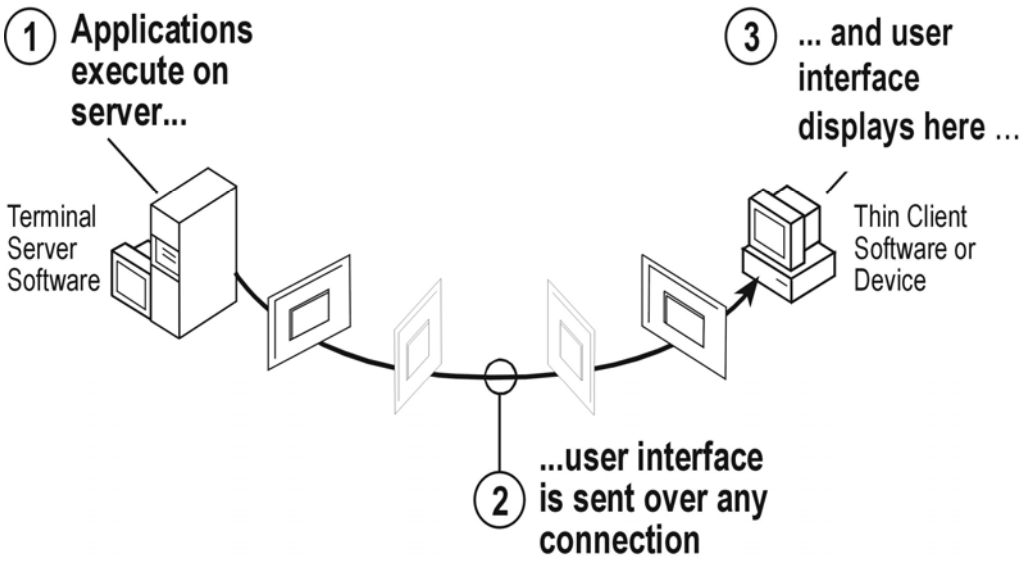

Abb.: Windows Terminal-Server-Konzept

Aus **sicherheitstechnischer Sicht** hat das Konzept den Vorteil, dass der Benutzer nur die Ressourcen auf seinem Arbeitsplatz-PC nutzen kann, die ihm zur Verfügung gestellt wurden. Die Nutzung und das Installieren von nicht erwünschten Anwendungen sowie das lokale Abspeichern von Daten werden damit ausgeschlossen, weil derartige Zugriffe unter der Voraussetzung einer ordnungsgemäßen Konfiguration nicht unterstützt werden.

Der Zugang zu den auf den Terminalservern installierten Fachanwendungen erfolgt über einen am Arbeitsplatzrechner installierten Client (ICA Client). Dort sind nur die Fachanwendungen aufrufbar, für die der Benutzer Berechtigungen erhalten hat.

Die Fachanwendungen der Stadtverwaltung befinden sich auf mehreren Terminal-Servern (Serverfarm), um eine Lastenverteilung zu gewährleisten.

Für eine sichere und ordnungsgemäße Datenverarbeitung wurden u.a. folgende **Anforderungen** an das Sicherheitsniveau gestellt:

- Gewährleistung einer Datenabschottung durch eine nachvollziehbare Benutzer- und Rechteverwaltung,

- Bereitstellung der Fachanwendungen auf dem Arbeitsplatz-PC auf das erforderliche Maß,

- strukturierte zentrale Datenverwaltung,
- sachgerechte Dokumentation aller Einstellungen an Hard- und Software,
- Aufbau einer qualifizierten IT-Koordination,
- Kontrolle und Überwachung durch die Bestellung eines Behördlichen Datenschutzbeauftragten.

Die **Konkretisierung** des Sicherheitsniveaus wurde in Form der Festlegung einzelner Sicherheitsmaßnahmen im Datenschutzkonzept berücksichtigt. So wurden Sicherheitsmaßnahmen z.B. für

- die Arbeitsplatzebene,
- die zentralen Komponenten bzw. der Server,
- das Netzwerk bzw. die Verkabelung,
- die externen Dienstleister,
- die Datenverwaltung,
- die Datensicherung,
- die Fachverfahren sowie
- für die Benutzer- und Rechteverwaltung

festgelegt.

2.4 Internetkommunikation

Die Einführung neuer Informations- und Kommunikationstechnologien in der Stadtverwaltung zielt neben einer Verbesserung des **Bürgerservices** auch auf **Effizienzsteigerungen** durch verbesserte Informationsflüsse ab. Vor

diesem Hintergrund kommt zunächst die Nutzung nachstehender Internetdienste in Betracht:

- WWW (Informationsabfrage)
- E-Mail (Nachrichtenaustausch)

2.4.1 Sicherheitskonzept für den Internetanschluss

Von besonderer Bedeutung sind folgende Sicherheitsmaßnahmen:

- Die **Verfügungsgewalt** (Überwachung und Administration) über die eingesetzten Firewall-Komponenten liegt bei der Stadtverwaltung.
- Es soll sichergestellt werden, dass **Angriffe auf der physikalischen** Ebene erkannt und abgewehrt werden.
- Eine **Fernadministration** der Firewall-Komponenten ist nicht gestattet.
- Ausgehende E-Mails dürfen **keine** personenbezogenen Daten enthalten.
- **Kopien** ein- und ausgehender E-Mails werden für **Kontrollzwecke** in einem gesonderten Archiv gespeichert.
- Es werden nur die E-Mails an den Arbeitsplatz geleitet, die **virenüberprüft** sind.
- E-Mails mit **Anhängen** werden in einem nur für den Administrator zugänglichen Fach gespeichert, während eine Kopie der E-Mail **ohne** Anhang an den Empfänger geleitet wird. Der Empfänger erhält einen entsprechenden Hinweis darüber, dass der Anhang nur vom Administrator nach vorheriger Überprüfung zugestellt werden kann.
- WWW-Seiten ohne **dienstlichen Bezug** werden deaktiviert.
- Es sind nur Web-Seiten **vertrauenswürdiger** Organisationen freigeschaltet.

- Das **„Herunterladen“** ausführbarer Programme und Dateien ist auf den Arbeitsplätzen nicht zugelassen.

2.4.2 Überwachung des Internetanschlusses

Für die dauerhafte Gewährleistung der **Einhaltung des Sicherheitsniveaus** sollen die **Internetaktivitäten** in Bezug auf **unerlaubte Aktionen** überwacht werden. Es soll insbesondere sichergestellt werden, dass Angriffe auf das interne Netz der Stadtverwaltung **erkannt** und **abgewehrt** werden können. Folgende Sicherheitsmaßnahmen wurden ergriffen:

- Das **Systemprotokoll der Firewall** protokolliert alle nicht erlaubten Aktivitäten. Es wird täglich von der IT-Koordination ausgewertet.

- Die **ordnungsgemäße Nutzung der Internetdienste** wird in regelmäßigen Abständen von dem behördlichen Datenschutzbeauftragten überwacht.

2.4.3 Dienstanweisung zur Nutzung der Internet-Dienste

In der Dienstanweisung zur Nutzung der Internet-Dienste werden die im Sicherheitskonzept festgelegten Sicherheitsmaßnahmen in konkrete **Handlungsanweisungen** für die Mitarbeiter der Stadtverwaltung umgesetzt. In ihr werden insbesondere

- die Verantwortlichkeiten für den Betrieb der Internetkomponenten und die Umsetzung der Dienstanweisung,

- die Nutzungsbedingungen für die Internetdienste,

- Regelungen über den Datenschutz und die Datensicherheit,

- der Protokollierungsumfang bei der Nutzung der Internetdienste sowie

- disziplinarische Maßnahmen bei Nichteinhaltung der Anweisungen

beschrieben.

2.5 Datenschutz-Management im laufenden Betrieb

Mit Abschluss des Behördenaudits geht das Datenschutz-Management auf den **behördlichen Datenschutzbeauftragten** über. In Zusammenarbeit mit der IT-Koordination **überwacht** er in regelmäßigen Abständen die Verfahrensabläufe in Bezug auf die Einhaltung gesetzlicher Vorschriften. Änderungen an Verfahren werden ihm von der IT-Koordination unverzüglich mitgeteilt, so dass er ggf. rechtzeitig das Unabhängige Landeszentrum für Datenschutz zum Zweck der Durchführung einer Nachprüfung informieren kann.

3 Datenschutzrechtliche Bewertung

Das Audit hat aufgezeigt, dass die von der Stadtverwaltung getroffenen technischen und aufbau- und ablauforganisatorischen Sicherheitsmaßnahmen die Anforderungen aus dem Datenschutzrecht (LDSG und DSVO) entsprechen. Hervorzuheben ist der Einsatz von **Thin Clients** im Rahmen des **Terminal-Server-Konzeptes** sowie die **spezielle Filterung der E-Mails und der Web-Seiten.**

In sicherheitstechnischer Hinsicht sind nach Abschluss des Audits also **keine Schwachstellen** erkennbar, die die Rechte der betroffenen Bürger und der Mitarbeiter der Stadtverwaltung beeinträchtigen könnten.

Die modular aufgebauten Sicherheitskonzepte repräsentieren ein **qualitativ hohes Niveau**. Sie bilden die Grundlage für ein wirksames Datenschutzmanagement im laufenden Betrieb der automatisierten Verfahren. Die mit dieser Aufgabe betraute behördliche Datenschutzbeauftragte wird in die Lage versetzt, durch einen effektiven **Soll-Ist-Vergleich** auf Veränderungen in den tatsächlichen Abläufen zu reagieren und Fehlentwicklungen offen zu legen. Es ist zu erwarten, dass durch diese Rahmenbedingungen eine Steigerung der **Effizienz** und der **Sicherheit** der automatisierten Prozesse eintreten wird.

Die Verleihung des Auditzeichens nach § 43 Abs. 2 LDSG ist damit gerechtfertigt.