Kurzgutachten

über das Auditverfahren gemäß § 43 Abs. 2 LDSG

„Anschluss des internen Netzes der Stadtverwaltung Neumünster an das Internet“

Kiel, 27. Oktober 2004

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Behördenaudits

Das Unabhängige Landeszentrum für Datenschutz (ULD) und die Stadtverwaltung Neumünster haben am 12.12.2003 eine Vereinbarung getroffen, nach der ein **Behördenaudit** bezogen auf das Projekt „**Anschluss des internen Verwaltungsnetzes an das Internet“** durchgeführt werden sollte.

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

- der ausreichende Schutz der automatisiert verarbeiteten Daten vor Angriffen aus dem Internet,
- ein hinreichend sicherer Transport der über die Internetdienste „E-Mail“ und „WWW“ versendeten bzw. empfangenen Daten sowie
- die Einhaltung der getroffenen Sicherheitsmaßnahmen

festgelegt.

Die Realisierung des Anschlusses des internen Netzes der Stadtverwaltung an das Internet 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.

Mit der Umsetzung der festgelegten Ziele wurde der Fachdienst EDV-Dienste betraut. Er legte die für die Erreichung der Datenschutzziele notwendigen Aufgaben in einem **Arbeits- und Zeitplan** fest.

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 Oberbürgermeister als Leiter der Daten verarbeitenden Stelle. Für die Einhaltung der jeweils anzuwendenden **Vorschriften** zum Datenschutz und zur Datensicherheit in den **Fachdiensten** sind die Fachdienstleiter zuständig und verantwortlich.

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

Die Schaffung der Voraussetzungen für den Einsatz und die Überwachung des laufenden Betriebs der IT-Systeme obliegt dem Fachdienst EDV-Dienste. Die durchzuführenden Arbeiten werden prinzipiell als **Dienstleistungen** für die **Fachdienste** angesehen.

2.2 Internetkommunikation

Die Einführung neuer Informations- und Kommunikationstechnologien zielt auf eine Verbesserung des **Bürgerservices** und auf **Effizienzsteigerungen** durch verbesserte Informationsflüsse ab. Vor diesem Hintergrund kommt zunächst die Nutzung nachstehender Internetdienste in Betracht:

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

- Homepage (Selbstdarstellung)

Für die Nutzung der neuen Informations- und Kommunikationstechnologien wurden ein **„Internet-Realisierungskonzept“** und ein **„Internet-Sicherheitskonzept“** erarbeitet.

2.3 Internetrisiken

Es wurden in Bezug auf die ausgewählten Internet-Dienste folgende **Risiken** für den Datenschutz und die Datensicherheit herausgearbeitet:

- **Netzspezifische Sicherheitsrisiken**

  Mit dem Anschluss an das Internet werden das **interne Verwaltungsnetz** und die daran angeschlossenen IT-Systeme von außen zugänglich.

- **WWW (Informationsabfrage)**

  ActiveX, JAVA und JavaScript als aktive Inhalte einer Web-Seite können zur Ausforschung von IT-Systemen und zum Installieren und Ausführen von Viren und „Trojanischen Pferden“ führen.

  Bei einem **Transfer** (Download) von angebotenen Programmen auf die dienstlichen IT-Systeme besteht die Gefahr der Vireninfizierung und der Nutzung von dienstlich nicht gestatteten Anwendungen.

- **E-Mail (Nachrichtenaustausch)**

  Dienstliche Nachrichten, die per E-Mail versandt werden, können **mitgelesen, verändert oder verfälscht** werden. Über E-Mails können **virenifizierte Programme oder Textdokumente** auf dienstliche IT-Systeme gelangen.

- **Homepage (Selbstdarstellung)**

  Die auf der Homepage veröffentlichen Informationen können durch unzureichende Absicherung des „Web-Servers“ von **„Hackern“** manipuliert werden.

2.4 Technisches Realisierungskonzept

Das „Technische Realisierungskonzept“ beschreibt den **Einsatz** der technischen Komponenten für den Internet-Anschluss unter Berücksichtigung folgender Anforderungen:

- Umsetzung einer Internetpräsentation bzw. Selbstdarstellung
- Einrichtung von Mail-Accounts für die Mitarbeiter der Verwaltung
- Informationsrecherche im Internet über Web-Surfen
- Blocken von nicht erwünschten Inhalten (Contentfilterung)
- Virenschutz
- Berücksichtigung von Datenschutz und Datensicherheit
- Schnittstelle für den Zugang zu externen Verwaltungsnetzen
- Unterstützung von Fernwartungszugängen

Zum Schutz vor Übergriffen aus dem Internet werden Firewall-Systeme eingesetzt. Sie verfügen über mehrere **demilitarisierte Zonen (DMZ)**. Diese sind in vordefinierte Sicherheitsebenen („Securitylevel“) unterteilt.

Pakete von einer Schnittstelle mit einem geringeren Security-Level werden nur dann an eine DMZ mit höherem Security-Level weitergeleitet, wenn dafür eine explizite Firewall-Regel eingetragen ist. Alle anderen Pakete werden gefiltert. Der Security-Level stellt also einen Wert für das an der DMZ vorgesehene Schutzbedürfnis dar.

Die Firewall-Systeme beinhalten in Bezug auf das **Verwaltungsnetz** u.a. folgende Sicherheitsregeln:

- Es werden keine Datenpakete, welche als Anfragen aus dem Internet kommen, in das Verwaltungsnetz durchgeleitet.

- Nicht benötigte Dienste sind **deaktiviert**.

- Das **Intrusion Detection System** (IDS) zeigt alle aktiven Verbindungen an und warnt den Administrator bei sicherheitsrelevanten Ereignissen.

Bei dem Internetdienst „WWW“ werden „Cookies“ und „Java-Script“ zugelassen, während Active X, Java und VBScript geblockt werden.

E-Mails, die nicht die **Sicherheitsregeln** erfüllen, werden für einen kurzen Zeitraum in einem gesonderten Bereich auf dem internen Server zwischengespeichert. Nur der interne Absender/Empfänger erhält über diesen Vorgang eine Benachrichtigung.

Alle Internet-Komponenten werden von den Mitarbeitern des Fachdienstes EDV-Dienste administriert. Der **fernadministrative** Zugriff auf die Firewallkomponenten ist deaktiviert.

2.5 Sicherheitsmaßnahmen

Auf der Grundlage des „Internet-Realisierungskonzeptes“ und unter Berücksichtigung der Internetrisiken wurden Sicherheitsmaßnahmen für die Internetanbindung in einem **gesonderten Sicherheitskonzept** festgelegt.

Das **Sicherheitskonzept** gibt die im Rahmen des Behördenaudits definierten Datenschutzziele in detaillierter Form wieder. Von besonderer Bedeutung sind folgende Regelungen:

- Vor dem **Echteinsatz** und im Bedarfsfall während des Echteinsatzes werden die ergriffenen Sicherheitsmaßnahmen von einem qualifizierten externen Dienstleister auf ihre Wirksamkeit durch Penetrationstests überprüft.

- **Veränderungen** der Sicherheitseinstellungen bedürfen nach Abstimmung mit dem behördlichen Datenschutzbeauftragten der Zustimmung des Fachdienstleiters EDV-Dienste.

- Zum **Schutz vor Angriffen** von außen sind die Übergänge vom internen

Verwaltungsnetz zum Internet durch eine Firewall zu schützen.

- Die **Verfügungsgewalt** (Überwachung und Administration) über die eingesetzten Firewall-Komponenten liegt ausschließlich bei der Stadtverwaltung.

- **Unerlaubte Zugriffe auf der physikalischen** Ebene werden protokolliert und abgewehrt. Bei Ereignissen von sicherheitsrelevanter Bedeutung werden gesonderte Warnmeldungen ausgegeben.

- Eine **Fernadministration** der Firewall-Komponenten ist nicht gestattet.

- Es werden nur die E-Mails an den Arbeitsplatz geleitet, die **virenüberprüft** sind und zugelassene **Attachements** (z.B. TXT, RTF) enthalten.

- Der Zugriff auf die Web-Seiten wird in Bezug auf die sicherheitskritischen Komponenten **Aktive-X, Java und VBScript** gefiltert.

- Web-Seiten werden nach **Text-Zensur-Skripten** geprüft und ggf. für den Aufruf nicht zugelassen.

- Das **„Herunterladen“** ausführbarer Programme und Dateien auf die Arbeitsplatzrechner ist nicht zugelassen.

- Vor der Darstellung personenbezogener Daten auf der Homepage ist die **Einwilligung der Betroffenen** einzuholen.

- Alle Einstellungen auf den Internet-Komponenten werden **nachvollziehbar** dokumentiert.

2.6 Dienstvereinbarung für die Nutzung der Internetdienste

Für die Nutzung der Internetdienste **„WWW“** und **„E-Mail“** wurden Dienstvereinbarungen zwischen der Stadt Neumünster und dem Personalrat geschlossen. In ihnen werden insbesondere

- die **Zuständigkeiten** für die Einrichtung und den Betrieb der Internetkomponenten,

- die **Nutzungsbedingungen** für die Internetdienste,
- der **Protokollierungsumfang** bei der Nutzung der Internetdienste sowie
- die **disziplinarischen Maßnahmen** bei Nichteinhaltung der Anweisungen

beschrieben.

2.7 Test des Internetanschlusses

2.7.1 Anforderungen für den Test

In dem Sicherheitskonzept für den Internetanschluss wurde festgelegt, dass die für die Internetkommunikation ergriffenen **Sicherheitsmaßnahmen** von einem **externen Dienstleister** auf ihre Wirksamkeit hin zu überprüfen sind. Hierfür wurde der vom ULD erstellte **Anforderungskatalog** für den Test des Internetanschlusses herangezogen. Er hat folgende Struktur:

- **Einleitung**
  Grundsätzliche Aspekte, z.B. die Bedeutung der Risiken und das erforderliche Sicherheitsniveau
- **Leistungsbeschreibung**
  Vorgaben für die Durchführung und den Umfang der Tests
- **Ablauf der Sicherheitsüberprüfung**
  Phase 1: Durchführung der Penetrationstests
  Phase 2: Technische Mängelbeseitigung
  Phase 3: Organisatorische Mängelbeseitigung
  Phase 4: Durchführung eines Auditverfahrens

2.7.2 Penetrationstest

Die Überprüfung des Internetanschlusses der Stadtverwaltung wurde vom ULD in Zusammenarbeit mit einem von ihm beauftragten Dienstleister

durchgeführt. Ziel des Penetrationstests war, als Außenstehender (Hacker) das interne **Verwaltungsnetz** zu kompromittieren bzw. Sicherheitsdefizite aufzudecken. Der Penetrationstests beinhaltete umfangreiche System-Analyseverfahren sowie den Einsatz zahlreicher Security- und „Hacker-tools“. Im **Ergebnis** wurde festgestellt, dass ein Angriff von außen auf das Verwaltungsnetz zu keinem Erfolg führte.

2.8 Dokumentation über die Internetnutzung

Es lagen als **Dokumentation** folgende Unterlagen vor:

- TuI-Konzept der Stadtverwaltung,
- Internet-Realisierungskonzept,
- Internet-Sicherheitskonzept,
- Dokumentation über den Penetrationstest,
- Dienstvereinbarung für die technikunterstützte Informationsverarbeitung,
- Dienstvereinbarung zur Internetnutzung „WWW“,
- Dienstvereinbarung zur E-Mailnutzung,
- Konfigurationsakten der einzelnen Internetkomponenten,

Die Dokumentation entspricht den Anforderungen der **Datenschutzverordnung**.

2.9 Internetdienste-Nutzung

2.9.1 Benutzer-Arbeitsplatz-PC

Die im internen Verwaltungsnetz installierten Benutzer-Arbeitsplatz-PC sind noch nicht für die Nutzung der Internetdienste freigeschaltet. „E-Mail“ und

„WWW“ werden bisher über Standalone-PC bereitgestellt.

Erst nach der Zertifizierung werden die in das Verwaltungsnetz integrierten Arbeitsplatz-PC schrittweise für die Nutzung der Internetdienste „E-Mail“ und „WWW“ freigeschaltet. Die Zugriffe und Funktionen werden den **Anforderungen** des Sicherheitskonzeptes entsprechend eingeschränkt.

Während dieser Maßnahme wird auch der auf den Arbeitsplatz-PC zur Verfügung gestellte **Funktionsumfang** überprüft und auf die **dienstlichen Erfordernisse** beschränkt. Im Rahmen der Migration von Windows NT nach Windows 2003 werden darüber hinaus die Sicherheitsmaßnahmen auf der Arbeitsplatzebene durch den Einsatz der **Gruppenrichtlinien** optimiert.

2.9.2 WWW

Das „Web-Seiten-Angebot“ wird über **Filtermechanismen** überprüft und eingeschränkt. Es können nur die Web-Seiten aufgerufen werden, die einer Überprüfung in Bezug auf **schädigende** Inhalte unterzogen wurden. Die Funktionen „Aktive Inhalte“ und „Download“ werden am Mitarbeiter-Arbeitsplatz nicht zugelassen. Darüber hinaus werden die Web-Seiten über eine **Schlagwortreferenzliste** gefiltert, so dass z.B. rassistische Web-Seiten geblockt werden.

2.9.3 E-Mail

Personenbezogene Daten der Fachdienste dürfen nicht per E-Mail versandt werden. E-Mails mit unerlaubten Dateianhängen (z.B. exe, com, etc.) werden herausgefiltert, ohne weitere Bearbeitung in einen gesonderten Bereich verlagert und nach kurzer Zeit automatisch gelöscht. Die E-Mails, die die **Sicherheitsvorgaben** erfüllen, werden in das Postfach des Adressaten auf dem E-Mail-Verwaltungsserver übertragen.

Als Virenschutz wird ein zweistufiges **Antivirensoftwareverfahren** eingesetzt. Die Software wird in regelmäßigen Abständen automatisiert aktualisiert.
Die E-Mail-Kommunikation ist in einer gesonderten **Dienstvereinbarung** geregelt.

2.9.4 Administration und Überwachung der Internetaktivitäten

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.

Zu diesem Zweck werden über das **Intrusion Detection System** IDS bei potentiellen Angriffen auf die Firewalls aber auch schon bei versuchten Spionage-Attacken **Protokolleinträge** generiert, die in regelmäßigen Abständen vom Fachdienst EDV-Dienste ausgewertet werden.
Die zu ergreifenden Maßnahmen werden vom Fachdient EDV-Dienste im Einzelfall festgelegt. Bei Verdacht eines **„Einbruches“** kann das Netz der Stadtverwaltung durch die Deaktivierung des entsprechenden Netzwerkinterfaces sofort vom Internet getrennt werden.

2.10 Datenschutz-Management im laufenden Betrieb

Zum Zeitpunkt der Begutachtung lag das Datenschutz-Management in der Zuständigkeit der Mitarbeiter des Fachdienstes **EDV-Dienste** und dem **behördlichen Datenschutzbeauftragten**.

Von ihnen wurden u.a. folgende Aufgaben erledigt:

- Umsetzung der Datenschutzziele und Dokumentation der Ergebnisse,
- Überwachung der Einhaltung der im Internet-Sicherheitskonzept festgelegten Sicherheitsmaßnahmen,
- Dokumentation des Verfahrens „Internetanbindung“ gemäß der DSVO (vgl. Tz. 2.8).

Mit Abschluss des Behördenaudits wird das Datenschutz-Management vom **behördlichen Datenschutzbeauftragten** und vom **Leiter des Fachdienstes EDV-Dienste** ausgeführt. Sie überwachen in regelmäßigen Abständen

die Einhaltung der gesetzlichen und verwaltungsinternen Vorschriften. Sofern sich Änderungen am Verfahren ergeben, wird das Unabhängige Landeszentrum für Datenschutz wegen der Durchführung einer Nachzertifizierung rechtzeitig informiert.

3 Datenschutzrechtliche Bewertung

Folgende Rechtsvorschriften wurden für die datenschutzrechtliche Bewertung herangezogen:

- **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 u. Protokolle

Die Überprüfung hat ergeben, dass die während der Bestandsaufnahme festgestellten Defizite im Rahmen des Audits systematisch beseitigt wurden. In Bezug auf die Erstellung konzeptioneller Unterlagen ist **positiv** hervorzuheben, dass die in dem Sicherheitskonzept festgelegten Sicherheitsmaßnahmen weitestgehend umgesetzt wurden.

Die durch das Audit „**Anschluss des internen Verwaltungsnetzes an das Internet“** erfassten Verarbeitungsprozesse zeichnen sich insbesondere

durch folgende „datenschutzfreundliche“ Aspekte aus:

1. Der Internet-Anschluss erfolgt über zwei hintereinander geschaltete Firewallsysteme mit abgestuften Securitylevel.

2. Der Fachdienst EDV-Dienste verfügt über umfangreiches und überdurchschnittliches „Know-how“ im Bereich Netzwerk- und Firewalltechnik.

3. Sicherheitsrelevante Ereignisse werden über das Intrusion Detection System (IDS) frühzeitig von den Administratoren erkannt und ausgewertet.

4. Die Nutzung der Internetdienste „E-Mail“ und „WWW“ ist bezüglich schädigender Inhalte bzw. bösartiger Angriffe reglementiert.

5. Die Wirksamkeit der Sicherheitseinstellungen ist durch einen umfassenden Penetrationstest überprüft worden.

Die **zügige und planmäßige** Durchführung des Audits ist insbesondere darauf zurückzuführen, das die Mitarbeiter des Fachdienstes EDV-Dienste den Internetanschluss auf **technisch hohem Niveau** realisiert haben. Der **Penetrationstest** hat gezeigt, dass ein **Angriff** auf das interne Netz der Stadtverwaltung über Internetschnittstellen bei **Aufrechterhaltung** der derzeitigen Sicherheitsmaßnahmen auch künftig zu **keinem** Erfolg führen dürfte.

Die Verleihung des Auditzeichens nach § 42 Abs. 3 LDSG ist damit gerechtfertigt.