Gutachten zum Datenschutz-Behördenaudit:

„Anonyme Nutzung des vom Landtag Schleswig-Holstein über das ParlaNet bereitgestellten Internet-Informationsangebots durch die Bürgerinnen und Bürger“

1. Grundlage und Gegenstand des Datenschutz-Behördenaudits

Mit Datum vom 03.06.2002 wurde die „Vereinbarung über die Zusammenarbeit bei der Durchführung des Datenschutz-Behördenaudits nach § 43 Abs. 2 LDSG“ vom Präsidenten des Schleswig-Holsteinischen Landtags und vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (im Folgenden auch ULD) unterzeichnet.

Gegenstand dieses Datenschutz-Behördenaudits ist demnach als abgegrenzter Teilbereich der Daten verarbeitenden Stelle die „anonyme Nutzung des vom Landtag Schleswig-Holstein über das ParlaNet bereit gestellten Internet-Informationsangebotes durch die Bürgerinnen und Bürger“ (im Folgenden auch ParlaNet-Audit). Dabei handelt es sich im Wesentlichen um das Web-Angebot, das durch den Chat-Server und die Möglichkeit der Anfrage per E-Mail, die zum inhaltlichen Angebot des Webservers gehört, ergänzt wird.

Andere Teilbereiche oder Einzelelemente des ParlaNets wurden nur insofern mit in das Auditierungsverfahren einbezogen, als sie entweder für die Bereitstellung des Internetangebotes insgesamt oder für Servicezwecke des Auditierungsgegenstandes von Bedeutung sind oder wenn von einer Verletzung ihrer Integrität ein Gefährdungspotenzial für den Auditierungsgegenstand im Sinne der im Folgenden definierten Risiken und Angriffsziele direkt ausgehen könnte.

Grundsätzlicher Ansatz der Bewertung sind neben den substanziellen Fragen des Datenschutzes Aspekte der allgemeinen Datensicherheit unter Berücksichtigung der potenziellen Gefährdungslage des Auditierungsgegenstandes. In diesem Fall besteht das Gefährdungspotenzial im Wesentlichen aus folgenden Risiken bzw. Angriffszielen:

- Durchbrechung der zugesicherten Anonymität
- Verletzung der Integrität der technischen Komponenten
- Verhinderung der Verfügbarkeit des Angebotes

Gelegentlich werden in den Bewertungen Anmerkungen in Bezug auf Fragen der Datensicherheit gemacht, die nicht direkt mit dem Auditierungsgegenstand zu tun haben. Dies wird jeweils herausgestellt; die Bemerkungen sollen jedoch auch nicht unerwähnt bleiben.

1.1 Technische Eingrenzung

Das Parlanet ist ein eigenständiges Netz im Schleswig-Holsteinischen Landtag, das an seinen Kommunikationspunkten bzw. Schnittstellen zu anderen Netzen sämtlich durch Firewalls abgeschlossen und abgesichert ist. Der innere Kern des ParlaNet kann als demilitarisierte Zone (DMZ) bezeichnet werden. Angeschlossen an das ParlaNet sind eigenständige SubLANs, z.B. der Fraktionen und der Landtagsverwaltung. Über das ParlaNet wird das Informationsangebot

des Schleswig-Holsteinischen Landtages zur Verfügung gestellt und abgesichert. Darüber hinaus werden diverse Services für die angeschlossenen Subnetze bereitgestellt.

Dies sind im Wesentlichen:

- Bereitstellung und Betrieb des Informationsangebotes des Schleswig-Holsteinischen Landtages
- Bereitstellung einer sicheren Betriebsumgebung für die Webangebote der Fraktionen und Funktionsträger des Schleswig-Holsteinischen Landtages (externe DMZ)
- Internetanschluss für Fraktionen, Mitglieder, Funktionsträger und Mitarbeiter des Schleswig-Holsteinischen Landtages
- Anschluss an das CampusNetzLand (CNL) und darüber erreichbare Dienste
- Dial-In-Service
- Bereitstellung zentraler Dienste (Druckservices etc.)

Insgesamt bestehen zurzeit Schnittstellen zu folgenden Netzen:

- Internetanbindung
- Gesicherter Zugriff auf die externe DMZ
- Anbindung an das CampusNetzLand (CNL) und an weitere auf diesem Weg mittelbar erreichbare Behördennetze
- Anbindung an Subnetze der Fraktionen und Funktionsträger im Schleswig-Holsteinischen Landtag
- Dial-In-Anschluss über das öffentliche Telefonnetz
- Subnetz zentrale Dienste (Druckservices etc.)
- SNA-Server
- Administrationsnetz

2. Gegenstand der Bestandsaufnahme

Die Bestandsaufnahme erfolgte durch das IT-Referat bzw. die Administration des ParlaNet des Landtags. Dabei wurde zunächst die vorhandene Dokumentation gesichtet und mit den Anforderungen der DSVO (Datenschutzverordnung vom 02.04.2001, GVBl SH 2001, 49) abgeglichen. In der Folge wurde die Dokumentation durch die Administration des ParlaNet entsprechend ergänzt. Es liegen abschließend die folgenden Dokumentationsobjekte für das Audit vor, die in die Audit-Akte eingehen:

- Vereinbarung über die Zusammenarbeit bei der Durchführung des Datenschutz-Behördenaudits nach § 43 Abs. 2 LDSG
- ParlaNet-Auditverfahren gem. § 43 Abs. 2 Landesdatenschutzgesetz (LDSG), Fassung vom 29.10.02
- Themenliste/Checkliste des ULD für das ParlaNet-Audit (mit Gesprächsergebnissen)
- Datenschutzmanagementsystem für das anonyme Surfen im Internetangebot des Schleswig-Holsteinischen Landtages, Stand 29.10.02
- Leistungsbeschreibung für das ParlaNet, Fassung vom 10.09.99
- Abschlussbericht, Fassung vom 06.09.99
- ParlaNet, Sicherheitskonzept gem. § 6 Abs.1 Datenschutzverordnung, Version 11.10.02
- ParlaNet-Datenschutzerklärung (www.ParlaNet.de/datenschutz.html)
- ParlaNet-Anleitung für Dial-In, kein Datum
- Das ParlaNet – eine kurze Einführung in Fuktionalität und Nutzen, kein Datum

- Ergebnisse der Sicherheitsüberprüfung des Netzes ParlaNet, Version 22.12.99, GE CompuNet
- Testprozeduren und Ergebnisse zur Abnahme des Systems „ParlaNet“ beim Landtag Schleswig-Holstein, Oktober 99, GE CompuNet
- Landtags-Infothek, kein Datum
- Weitere technische Angaben für SubLAN-Betreiber im ParlaNet, 25.08.99
- Weitere technische Angaben für SubLAN-Betreiber im ParlaNet, 02.03.01
- Konzeptänderungen des ParlaNet bezüglich Version 1.1, 26.11.99
- Konzeptänderungen des ParlaNet bezüglich Version 1.2, kein Datum, L155
- Konzeptänderungen des ParlaNet bezüglich Version 1.2, 14.12.99
- Konzeptänderungen ParlaNet Version 1.3, 04.02.02
- Freischaltung des Zeitprotokolls an den Firewalls A und C, 11.05.00
- Vereinheitlichung der Second Level Domain, 11.05.00
- Konzeptänderungen ParlaNet Version 1.3
- Verzeichnis der im Rahmen von „ParlaNet“ verwendeten Abkürzungen
- Online-Dokumentation „doku.pdf“ als Papier-Ausdruck und online-Dokument

Neben der Analyse der Dokumentation erfolgte durch das ULD eine Begehung der Serverräume und der Sicherheitsvorkehrungen. Fragen, die durch die Dokumentation aufgeworfen wurden bzw. die durch die Dokumentation nicht erschöpfend geklärt werden konnten, wurden mittels einer Checkliste zusammen mit der Administration des ParlaNet diskutiert. Die Checkliste mit den zugehörigen Gesprächsergebnissen ist Teil der Bestandsaufnahme (s.o.).

3. Bewertung der Bestandsaufnahme

3.1 Dokumentation

Eine Aufzählung der vorhandenen Dokumentation erfolgte bereits unter Punkt 2 „Gegenstand der Bestandsaufnahme“.

Bewertung:
Die vorliegende Dokumentation ist umfangreich, angemessen detailliert und von hoher Qualität. Es ist jedoch zu bemerken, dass nicht alle seitens der DSVO vorgesehenen Dokumentationsteile als Einzelobjekt vorhanden sind, z.B. gibt es kein abstraktes Soll-Konzept und kein Verfahrensverzeichnis. Die DSVO ist für die Landtagsverwaltung nicht direkt anwendbar (§ 1 Abs. 1 DSVO, § 1 Abs. 1 Datenschutzordnung des Schleswig-Holsteinischen Landtags, DSO-LT SH). Die Qualität der Dokumentation entspricht aber den Anforderungen der DSVO. Alle Informationen, die ihrem Inhalt nach erforderlich sind, sind auch vorhanden und strukturiert zugreifbar.

Wie anhand der Struktur der Dokumentation deutlich wird, ist die Dokumentation des ParlaNet offenbar zum einen Teil im Zusammenhang mit dem Beschluss- und Umsetzungsverfahren für das ParlaNet entstanden und zum anderen Teil aus den Anforderungen und Notwendigkeiten der täglichen Arbeit der Administratoren direkt hervorgegangen. Positiv hervorzuheben ist in diesem Zusammenhang die schlüssige und gut benutzbare Online-Dokumentation, die dem ULD als Dokument „doku.pdf“ übergeben wurde.

Im Dokument „Anleitung für Dial-In“ wird explizit auf die Möglichkeit hingewiesen, das Einwahlpasswort systemseitig unter Windows zu hinterlegen. Dies ist aus Sicherheitsgründen grundsätzlich nicht empfehlenswert, für den Auditgegenstand jedoch nicht von Bedeutung.

3.2 Anonymisierungsverfahren

Bei der Nutzung des Informationsangebotes des Schleswig-Holsteinischen Landtages fallen technisch notwendigerweise Verbindungsdaten über die oder den Nutzenden und das angefragte Informationsmaterial an. Je nach Einstellung des Clientprogramms (Browser) des Nutzers können darüber hinaus weitere Daten ohne Anforderung des Servers an diesen übermittelt werden.

Relevante personenbeziehbare Daten fallen durch die übermittelte IP-Adresse des Nutzers an, da diese zur Rückübermittlung der Antwort in jedem Fall vom Server gespeichert werden muss. Da die IP-Adresse einem Nutzer in der Regel mindestens für eine Internetsitzung zugeteilt wird und der Nutzer über diese Adresse als Person ermittelbar ist, wird die IP-Adresse als personenbezogenes Datum gewertet. Dies ist auch dann der Fall, wenn die Adresse nicht allein durch die Informationsanbieter ermittelt werden kann, sondern weitere Dienstleister bzw. Stellen zwischengeschaltet sind.

Die für die Anfrage notwendigen Verbindungsdaten werden im vorliegenden Verfahren nur auf der ersten Firewall, die auf dem Weg zum Webangebot passiert wird, temporär im Arbeitsspeicher vorgehalten. Die Firewall fungiert in diesem Fall als Application Proxy. Dem Web- bzw. Chatserver selbst wird bereits nur noch die IP-Adresse der Firewall zusammen mit den solchermaßen anonymisierten Restdaten übermittelt. Somit ist eine Zuordnung von einer Anfrage zu einer IP-Adresse bzw. einem Nutzer durch den Webserver bereits nicht mehr möglich. Die vom Webserver an die Firewall rückübermittelte Antwort wird durch die Firewall an die temporär gespeicherte IP-Adresse des Nutzers weiter übermittelt.

Das Verfahren ist in der dem ULD vorliegenden Dokumentation detailliert beschrieben. Es kommt bei den drei Firewalls A, B und C des ParlaNet in dieser Form zum Einsatz. Somit werden sowohl Anfragen der Bürgerinnen und Bürger, als auch der angeschlossenen Fraktionsnetze und Funktionsträger anonymisiert.

Die Verbindungen, die über das Internet von Bürgerinnen und Bürgern zum Informationsangebot des Schleswig-Holsteinischen Landtages aufgebaut werden, laufen über die Firewall A des ParlaNet. Neben dem Webangebot gilt dies auch für das Chat-Forum, bei dem eine Anonymisierung in derselben oben beschriebenen Form stattfindet. Mails, die über eine Funktion des Webangebotes an die Adresse info@parlanet.de gehen, können nicht vollständig anonymisiert werden, da zumindestens die E-Mail-Adresse des Absenders für eine Antwort zwingend notwendig ist. Hier wird jedoch der Mailheader von überflüssigen Zusatzinformationen bereinigt, die für die Zustellung einer Antwortmail nicht erforderlich sind (siehe auch Abschnitt 3.5.1).

Bewertung:
Durch das hier gewählte Anfrageverfahren wird die IP-Adresse eines Nutzers nur für die Dauer der Anfrage auf der Firewall bzw. dem Application Proxy vorgehalten. Sie wird nicht an die angefragten Web- oder Chatserver übermittelt und kann von diesen nicht weiter verwertet werden. Die Anonymität des Nutzers ist somit gewährleistet, solange die Integrität des ParlaNet bzw. des bei der Anfrage genutzten Application Proxy gewährleistet ist und die Firewall korrekt konfiguriert ist. Das Verfahren ist insgesamt geeignet, die Anonymität der Nutzenden angemessen sicherzustellen. Das Restrisiko kann als sehr gering bewertet werden.

3.3 Physikalische Sicherheit der Komponenten

Sämtliche Systemkomponenten des ParlaNet befinden sich in den Technikräumen des Landeshauses und des Gebäudes Karolinenweg in geschlossenen, besonders gesicherten Räumen. Zutritt für Dritte wird nur in Begleitung gewährt.

Im Serverraum des Landeshauses ist die Hauptzahl der Komponenten untergebracht. Der Serverraum befindet sich im Kellergeschoss unter dem IT-Referat mit direktem Zugang von diesen Räumen. Die entscheidende Sicherheitszone für den Serverraum im Landeshaus wird durch die Räume des IT-Referates gebildet, die durch eine Tür mit Kartenschloss abgesichert sind. Zutritt zu diesen Räumen haben nur die Mitarbeiter des IT-Referates (zu denen die ParlaNet-Administratoren gehören), sowie Pförtner und der Hauselektriker. Die Verwaltung und technische Kodierung der Smartcards erfolgt durch das IT-Referat. Eine Protokollierung der Türbenutzung erfolgt momentan hauptsächlich innerhalb der Kartenleser, die Umstellung auf einen Server ist jedoch geplant. Eine Umstellung der Zutrittsüberwachung ist im Rahmen des Umbaus des Landeshauses als Teil des baulichen Sicherheitskonzeptes geplant.

Der Serverraum ist durch ein weiteres Kartenschloss gesichert. Er ist durch Gitter und verschlossene Türen in unterschiedliche gesicherte Abschnitte („Käfige“) unterteilt, da sich neben den Komponenten des ParlaNet auch die Telefontechnik (Zuständigkeitsbereich des Anlagenverantwortlichen und des Finanzministeriums) in diesem Raum befindet. Innerhalb des ParlaNet-Käfigs befinden sich die Komponenten in Technikschränken, die bei der Begehung durch das ULD verschlossen vorgefunden wurden. Eine Protokollierung des Zutritts zum Serverraum erfolgt analog zum IT-Referat durch den Kartenleser.

Die Fenster des Serverraums sind durch Luftschutzpanzertüren innen vor jedem Fenster gesichert, die durchgängig verschlossen gehalten werden.

Die Verkabelung des ParlaNets verläuft innerhalb des abgesicherten ParlaNet-Käfigbereiches und ist außerhalb dieses Käfigs nicht erreichbar.

Der Technikraum im Gebäude Karolinenweg ist mit einem hochwertigen Schloss versehen und wird durchgängig verschlossen gehalten. Da dieser Raum eine Vielzahl unterschiedlicher technischer Komponenten beinhaltet, besteht Zutrittsberechtigung für mehrere Personengruppen. Die Netzwerkkomponenten des ParlaNet befinden sich daher in einem Netzwerkschrank mit hochwertiger Schliessanlage, der durchgängig verschlossen gehalten wird. Der zugehörige Schlüssel wird in den Räumen des IT-Referates in einem verschlossenen Kasten aufbewahrt.

Der Themenbereich Brandschutz wird zurzeit im Rahmen des baulichen Sicherheitskonzeptes erörtert. Momentan ist ein Brandschutz nur durch computergeeignete Feuerlöscher gegeben. Für den Katastrophenfall ist der Serverraum mit einem Notlicht und Leuchtstreifen versehen.

Bewertung:
Insgesamt wird die Sicherheit der Technikräume als gut beurteilt.

Bei der Protokollierung des Zutritts fallen durch die Kartenleser personenbezogene Daten der Mitarbeiter an. Gesetzliche Vorschriften zum Datenschutz und zur Mitbestimmung sind zu beachten.

3.4 Netzwerksicherheit

Das ParlaNet ist topologisch als „screened subnet“ angelegt. Direkte Kontakte zwischen internen und externen IP-Adress-Objekten sind also unzulässig und werden auf technischer Ebene vollständig unterbunden. Verbindungen erfolgen ausschließlich über Stellvertreterobjekte. Dies wird ebenfalls durch die Firewall-Policies (alle Dienste, die nicht explizit erlaubt sind, sind verboten) unterstützt.

Das aus technischer Sicht mehrstufige Sicherheitskonzept (Sandwichkonzept) des ParlaNet sieht auf Layer-3-Netzwerkebene (OSI-Schichtenmodell) durchgängig geswitchte Netzwerkstrukturen vor (strukturierte Verkabelung). Dabei weisen bereits die Switche unzulässige Kommunikationsversuche oder Kommunikationsversuche mit unsicheren Protokollen (z.B. Telnet) ab.

Innerhalb des Landeshauses ist der Übergabepunkt einzelner SubLANs zum ParlaNet durch Einbauswitche (Installationsswitche) realisiert, die darüber hinaus die Wandlung von LWL (Lichtwellenleiter) auf CU (Kupferkabel, Kategorie 5) vornehmen. Die an das ParlaNet angeschlossenen selbstverwalteten SubLANs, z.B. der Fraktionen, sind auf Layer-3-Ebene innerhalb der Switche als VLANs (virtuelle LANs) realisiert. Einzelne Raumanschlüsse sind diesen VLANs zugeordnet. Die Raumanschlüsse sind grundsätzlich nicht belegt und werden nur auf Anforderung für das jeweilige SubLAN geschaltet.

Die zentralen aktiven und passiven Netzwerkkomponenten wie auch die Patchfelder befinden sich in gesonderten verschlossenen Räumen der jeweiligen Liegenschaften. Die in Augenschein genommenen Netzwerkkomponenten im Landeshaus befanden sich bei der Begehung innerhalb des verschlossenen Serverraumes in einem der abgetrennten Bereiche (Käfig) in gesonderten abgeschlossenen Technikschränken. Im gesamten Landeshaus sind LWL-Kabel mit definierten Übergabepunkten für SubLANs verlegt.

Im Gebäude Karolinenweg befinden sich die Netzwerkkomponenten in einem ebenfalls verschlossenen Technikraum, zu dem neben dem Technikpersonal auch andere Berechtigte Zugang haben. Die Komponenten sind in einem verschlossenen Technikschrank mit einer hochwertigen Schließanlage gesichert. Im Gebäude Karolinenweg sind Kategorie-6-Kabel verlegt.

Die Administration sämtlicher Netzwerkkomponenten erfolgt durch drei Personen des Serviceteams „ParlaNet“ ausschließlich durch verschlüsselte Netzwerkverbindungen (ssh oder Webbrowser-basiert) und passwortgeschützt. Die Administratoren haben individuelle Zugänge.

Zur Administration der Server innerhalb der DMZ gibt es ein physikalisch vom Restnetz getrenntes Administrationsnetz, zu dem nur die Administratoren Netzzugang haben. Die Komponenten des ParlaNets, die DMZ und das Administrationsnetz sind nicht über den zentralen Switch angeschlossen, sondern verfügen über einen gesonderten Layer-2-Switch.

Für die Einwahl in die dedizierten SubLANs steht innerhalb des ParlaNet ein Einwahlrouter zur Verfügung. Nach der Passwortabfrage auf dem Router erfolgt eine weitere Authentifikation über eine dedizierte Firewall mit Hilfe eines Radius-Servers.

Bewertung:
Die Netzwerksicherheit entspricht dem gegenwärtigen Stand der Technik und kann somit als hoch angesehen werden.

Für den Dial-In-Service ist eine Absicherung primär durch zweimalige Passworteingabe vorgesehen. Da jedoch jeder Nutzer eine IP-Adresse aus seinem SubLAN erhält und nach erfolgreichem Dial-In direkt in dieses SubLAN weitergeleitet wird, ergibt sich insgesamt nur ein mäßiges Gefahrenpotential für die Integrität des ParlaNet. Darüber hinaus muss jeder Dial-In-Berechtigte neben der generellen Dial-In-Berechtigung eines gesamten SubLANs auf Antrag der Netzverantwortlichen auch von seinem zuständigen SubLAN-Administrator freigeschaltet werden, bevor der Service überhaupt genutzt werden kann.

Weiterhin ist zu bedenken, dass eine Administration des ParlaNet nur über verschlüsselte Verbindungen erfolgen kann. Dennoch wäre es denkbar, dass ein potenzieller Angreifer sich Informationen z. B. über die IP-Adressaufteilung verschafft, um auf diese Weise einen Angriff auf das ParlaNet selbst zu versuchen. Es sollte daher durch das IT-Referat geprüft werden, ob eine Erhöhung der Netzwerksicherheit im Bereich des Dial-In-Services z.B. durch Benutzung von VPN-Clients erreicht werden kann. Da die Firewall C ohnehin in den Dial-In-Vorgang einbezogen ist, könnte sie auch als VPN-Gateway fungieren.

Es ist noch zu bemerken, dass der LWL-Verkabelung allgemein eine bessere Abhörsicherheit zugesprochen wird als der Kupferverkabelung. Die Benutzung allgemein zugänglicher Infrastruktur (in diesem Fall die LWL-Verbindung zwischen den Liegenschaften) ist grundsätzlich ein weitgehend unbeachtetes Problem der Netzwerksicherheit, das durch zusätzliche Verschlüsselung auf Netzwerkebene entschärft werden könnte. In diesem Fall würde jedoch Verschlüsselung keinen signifikanten Zuwachs an Sicherheit bedeuten; die Gebäudeverbindung ist für den Auditierungsgegenstand nicht von Bedeutung.

3.5 Administrative Verfahren

3.5.1 Konzept und Serversicherheit

Sämtliche Systemkomponenten des ParlaNet sind in der vorgelegten Dokumentation mit Informationen zu Aufbau, Stand der Softwareversionen, laufenden Diensten, eingetragenen Benutzern usw. erfasst.

Die Server des ParlaNet sind auf Betriebssystemebene als so genannte „gehärtete Systeme“ aufgesetzt. Die dazu notwendigen Änderungen sind schriftlich protokolliert. Es laufen nur die zur Funktionserfüllung notwendigen Dienste. Es werden weitgehend aktuelle Betriebssystemversionen mit aktuellen Patches verwendet. Die Applikationssoftware wird auf aktuellem Stand gehalten. Eine Absicherung der Systemintegrität erfolgt durch Einsatz der Software „Tripwire“. Ein Einsatz zusätzlicher Auditsoftware ist nicht vorgesehen.

Im Rahmen des Audits sind vorrangig die eingesetzten Webserver und Firewalls von Bedeutung. Die Firewallpolicies sind streng nach dem Prinzip „alles was nicht erlaubt ist, ist verboten“ ausgerichtet. Kommunikationsbeziehungen erfolgen ausschließlich über Stellvertreterobjekte (Application Level Gateways/Proxies). Auf den Firewalls ist Network Adress Translation (NAT) eingerichtet, unerlaubte Zugriffsversuche werden protokolliert.

Auf den Firewalls sind des weiteren aktiviert:
- Relay-Schutz (E-Mails werden nur für Adressen des ParlaNet angenommen)
- Absenderadressen werden nur aus dem Bereich des ParlaNet akzeptiert
- Adress-Hiding (keine Weitergabe von externen Nutzeradressen an weitere Server, Entfernung von zusätzlichen Adressinformationen aus E-Mails, z.B. „received-by“)
- Antispoofing (Blockierung von eingehenden IP-Paketen mit unlogischer Adressherkunft)

- Syn-Defending auf der Firewall A (Schutz gegen Syn-Flooding als DOS-Attacke)

Eine schriftliche Security-Policy mit detaillierter Analyse des verbleibenden Restrisikos ist Teil der Dokumentation. Das Konzept des ParlaNet sowie die Security-Policy lagen dem ULD vor. Virenscanner, Appletscanner oder ein Intrusion Detection System sind konzeptionell nicht vorgesehen und werden nicht eingesetzt.

Bewertung:
Das technische Konzept des als DMZ bezeichneten ParlaNet ist als sehr gut zu bewerten und frei von Beanstandungen. Der Einsatz eines UNIX-Betriebssystems für die sicherheitsrelevanten Systeme ist aus Gründen der Systemsicherheit ebenfalls positiv hervorzuheben.

Bei den Webservern und Firewalls handelt es sich ebenfalls um ausgereifte Systeme, die eine gute Produktkontinuität haben dürften. Die eingesetzte Firewallsoftware wird bei korrekter Installation und Einstellung allgemein als hoch sicher angesehen. Sicherheitstechnisch befinden sich die Server (unter Berücksichtigung des geplanten Betriebssystem-Updates) auf dem Stand der Technik.

Eventuell könnte die Sicherheit des ParlaNet durch Einsatz eines Intrusion Detection Systems noch weiter erhöht werden. Der Einsatz eines solchen Systems wird zurzeit durch das IT-Referat geprüft. Sollte ein Intrusion Detection System zum Einsatz kommen, muss auch die Überarbeitung der Datenschutzerklärung zeitnah erfolgen.

Der Einsatz von Viren- oder Appletscannern ist konzeptbedingt nicht erforderlich.

3.5.2 Administration der Komponenten

Zuständigkeiten und Verantwortlichkeiten sind für jede einzelne Systemkomponente des ParlaNet schriftlich festgelegt. Vertretungen sind geregelt. Test und Freigabe sind ebenfalls für jede Komponente erfolgt und schriftlich dokumentiert.

Die Root-Zugänge auf den Servern sind deaktiviert und durch individuelle Administrationszugänge der zuständigen Mitarbeiter ersetzt. Eine Administration der Komponenten ist nur aus dem physikalisch getrennten Administrationsnetz möglich. Die Firewalls werden über verschlüsselte Verbindungen oder über die ebenfalls verschlüsselte Managementkonsole administriert.

Fernwartung durch Dritte oder eine externe Vergabe von Serviceaufgaben erfolgt nicht.

Bewertung:
Die Dokumentation für die tägliche Arbeit der Administratoren ist vorbildlich durch die Online-Dokumentation umgesetzt, so dass auch im Vertretungsfall alle notwendigen Informationen vorliegen dürften. Ein zusätzlicher Schutz gegen Logfile-Manipulationsmöglichkeiten durch Administratoren in Form eines Audit-Systems wäre wünschenswert.

Ein abgestuftes Zugriffskonzept für Administratoren ist aufgrund der Gruppengröße nicht erforderlich.

3.5.3 Notfallvorsorge, Backup und Recovery

Alle Systemkomponenten können angabegemäß hardwaremäßig durch andere Komponenten ersetzt werden, nötigenfalls könnten Arbeitsplatzrechner eingesetzt werden. Dedizierte Ersatzhardware ist weder für Server noch für Netzwerkkomponenten vorhanden. Die zentralen Server sind mit redundanten Netzteilen ausgestattet. Festplattenarrays o.ä. werden nicht eingesetzt.

Die Switche und sonstigen Netzwerkkomponenten sind ebenfalls untereinander austauschbar, wobei weniger wichtige Netzsegmente dann ausfallen würden. Managementkonsole und Netzteile der Netzwerkkomponenten sind ebenfalls redundant ausgelegt. Für die eingesetzten Netzwerkkomponenten besteht angabegemäß ein Wartungsvertrag.

Die USV wurde während eines Stromausfalles bereits erfolgreich benutzt.

Die Server werden gemäß der Leistungsbeschreibung zyklisch durch Backup verschlüsselt gesichert und die Bänder in einem dedizierten Tresor gelagert. Das Einspielen eines Backups wurde bereits getestet.

Bewertung:
Für den Ausfall von Hardware-Komponenten (Server wie Netzwerkkomponenten) sollte ein gewisser Grundstock an Hardware vorgesehen werden, damit im Notfall nicht der Ausfall von Services vorbestimmt ist.

Der Ausfall einzelner Serverklassen sollte turnusmäßig (z.B. jährlich) getestet werden. Es sollte seitens der ParlaNet-Administration geprüft werden, ob Hinweise zum Recovery in die Serverdokumentation aufgenommen werden.

3.6 Datenschutzkontrolle

Die Datenschutzkontrolle erfolgt durch das Datenschutzgremium des Landtags gemäß § 13 Abs. 1 Datenschutzordnung des Schleswig-Holsteinischen Landtages vom 03.09.1998, geändert am 23.01.2002 (DSO-LT SH). Technische Unterstützung erhält das Datenschutzgremium durch die im Bereich der Administration des Landtagsverwaltungsnetzes eingesetzten und damit mit dem ParlaNet nicht betrauten Mitarbeiter des IT-Referates des Landtages. Zur Beratung des Datenschutzgremiums stehen außerdem die IuK-Kommission des Landtages und die Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz zur Verfügung.

4. Rechtliche Bewertung

Daten verarbeitende Stelle ist der Landtag Schleswig-Holstein. Auf diesen ist nicht das Landesdatenschutzgesetz Schleswig-Holstein (LDSG SH) anwendbar, sondern die Datenschutzordnung des Landtages (§ 1 Abs. 1 DSO-LT SH). Bei dem Informationsangebot des Landtages handelt es sich um einen Abrufdienst als Mediendienst i.S.d. § 2 Abs. 2 Nr. 4 Mediendienste-Staatsvertrag (MDStV) und, soweit es sich um die Vermittlung von Informationsangeboten handelt, um einen Teledienst i.S.d. § 2 Abs. 2 Nr. 3 Teledienstegesetz (TDG).

Gemäß § 18 Abs. 6 MDStV bzw. § 4 Abs. 6 Teledienstedatenschutzgesetz (TDDSG) hat der Anbieter dem Nutzenden die Inanspruchnahme von Medien- bzw. Telediensten anonym oder pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Die Nutzenden sind über diese Möglichkeit zu informieren. Gem. § 18 Abs. 4 MDStV bzw. § 4 Abs. 4 TDDSG ist der Anbieter weiter verpflichtet, durch technische und organisatorische Vorkehrungen die Möglichkeit des jederzeitigen Abbruchs der Verbindung, die umgehende Datenlöschung und den Schutz gegen Kenntnisnahme Dritter vorzusehen.

Diesen Anforderungen genügt das Landtagsangebot in vorbildlicher Weise. Die IP-Nummer eingehender Informationsanfragen gelangt über die Firewall des ParlaNet zum informationsanbietenden Webserver (Applikationsproxy), wo eine Umcodierung stattfindet. Die Informationsabrufe werden nicht mit der von außen anfragenden IP-Nummer, sondern mit einer ParlaNet-internen Adresse an die eigentlichen Informationsanbieter weitergeleitet. Eine Kenntnisnahme der von außen anfragenden IP-Nummer ist nicht möglich. Die eingehende IP-Nummer wird am Applikationsproxy nur so lange verarbeitet, wie dies erforderlich ist, um die Antwort auf die jeweilige Anfrage an die anfragende IP-Nummer zurückzusenden. Für diesen Zeitraum ist die kurzfristige Speicherung der eingehenden IP-Nummer und der innerhalb des ParlaNet genutzten Nummer erforderlich. Nach Abwicklung der Anfrage findet keine darüber hinausgehende Speicherung von eingehenden IP-Nummern bzw. internen Zuordnungsnummern statt. Dadurch erfolgt über den Zeitraum des eigentlichen Abrufvorganges hinaus keine Verarbeitung personenbezogener Daten.

In der Datenschutzerklärung unter www.ParlaNet.de/inhalt_datenschutz.html wird den Nutzenden die Anonymisierung der Nutzungsdaten erläutert. Nutzungsprofile werden weder in personenbezogener noch in pseudonymer Form erstellt (vgl. § 13 Abs. 4 MDStV, § 6 Abs. 3 TDDSG). Da weder personenbezogene noch pseudonyme Daten gespeichert werden, erfolgt keine Auskunftserteilung (vgl. § 20 MDStV, § 4 Abs. 7 TDDSG).

Vorschlag für eine Verbesserung der Datenschutzerklärung:

„Jeder Zugriff auf das Angebot des Schleswig-Holsteinischen Landtags führt zu einer Speicherung in einer Protokolldatei. Dabei erfolgt nach Beendigung der Nutzung keine Speicherung der IP-Nummer. Durch eine sofortige Anonymisierung der Abrufe kann von niemandem nachvollzogen werden, wer welche Daten abgerufen hat. Personenbezogene oder pseudonyme Nutzungsprofile können nicht erstellt werden.
Im Regelfall (Ausnahme: Chat, Presseticker, E-Mail) wird über jeden Abruf folgender Datensatz gespeichert:

- Host – durch NAT ausgetauschte IP-Adresse
- HostID – Kennzeichen der authentifizierten Maschinen bei Zugang in den nicht öffentlichen Bereichen

- UserID – Kennzeichen der authentifizierten User bei Zugang in den nicht-öffentlichen Bereichen
- Date – Datum des Zugriffs (Tag/Monat/Jahr:Stunde:Minute:Sekunde Zeitzone)
- Request – Angabe, welche Seite/Datei abgefragt wurde
- Status – nummerische Angabe des Rückgabe-/Statuswertes
- Bytes – übertragene Datenmenge
- Referer – Referenzdatei
- Userclient – Angabe des verwendeten Browsers

(u.U. ist auch eine populäre Zusammenfassung der Datenfelderbeschreibung möglich).

Die gespeicherten Daten werden nur zu statistischen Zwecken oder zur Klärung technischer Probleme von der Landtagsverwaltung ausgewertet. Eine Weitergabe an Dritte findet nicht statt.
Die Site verwendet keine Cookies. Auch andere Techniken, die dazu geeignet sind, das Zugriffsverhalten der Nutzenden nachzuvollziehen, werden nicht verwendet. JavaScript o.Ä. wird nicht eingesetzt.“

5. Datenschutzziele

Ausgehend von den Ergebnissen der Bestandsaufnahme hat die Landtagsverwaltung Datenschutzziele festgelegt, die für das Verfahren der Nutzung der über das ParlaNet bereit gestellten Informationen erreicht und dauerhaft eingehalten werden sollen. Diese Ziele sind im „Datenschutzmangementsystem für das anonyme Surfen im Internetangebot des Schleswig-Holsteinischen Landtages“ dokumentiert und beinhalten im Einzelnen

1. die Gewährleistung der anonymen Nutzung des vom Schleswig-Holsteinischen Landtag über das ParlaNet bereit gestellten Internet-Informationsangebots für die Bürgerinnen und Bürger,

2. die ständige Fortbildung der Administratoren,

3. die ständige Fortschreibung der Dokumentation.

Diese Ziele stellen allesamt Dauerziele dar, die kontinuierlich zu erfüllen sind und somit ihre Wirkung erst im Laufe des Gültigkeitszeitraums des Audits entfalten. Zum gegenwärtigen Zeitpunkt der Auditverleihung sind diese Ziele in vorbildlicher Weise in die Praxis umgesetzt. Hinsichtlich des Datenschutzziels Nr. 1, der Gewährleistung der anonymen Nutzung, ist die praktische Umsetzung bereits mit der Inbetriebnahme des Parlamentsnetzes am 30. August 1999 erfolgt. Die Zielsetzung im Rahmen des Audits bezieht sich aus diesem Grund nur noch auf die dauerhafte Gewährleistung der anonymen Nutzungsmöglichkeit in der Zukunft. Gleiches gilt für die Datenschutzziele Nr. 2 und 3, die zum gegenwärtigen Zeitpunkt zum einen durch ein hohes Fachwissen der Administratoren und zum anderen durch eine umfängliche, den Anforderungen entsprechende Dokumentation erfüllt werden.

6. Wesentlicher Inhalt des Datenschutzmanagementsystems

Zur Umsetzung dieser Ziele hat die Landtagsverwaltung ein Datenschutzmangementsystem eingerichtet. Dieses beinhaltet im Wesentlichen Maßnahmen zur Einhaltung der festgelegten Datenschutzziele sowie darüber hinaus allgemeine Maßnahmen zur dauerhaften Sicherung des erreichten Datenschutzniveaus. In diesem Rahmen liegt die Gesamtverantwortlichkeit für die Erreichung der Datenschutzziele und die Einhaltung der datenschutzrechtlichen Vorgaben bei

der Leitung der Abteilung 1 der Landtagsverwaltung sowie dem von dieser geführten Referat für Informations- und Kommunikationstechnik der Landtagsverwaltung.

Das Datenschutzmanagementsystem beschreibt für jedes der Datenschutzziele die zur Umsetzung bzw. Erhaltung erforderlichen Maßnahmen und benennt die Zuständigkeiten für deren Durchführung. In zeitlicher Hinsicht sind diese Maßnahmen als regelmäßig wiederkehrende Daueraufgaben ausgestaltet. Zu den hierfür erforderlichen Aufgaben gehört insbesondere die regelmäßige Durchführung von Schulungen für die Administratoren.

Ebenfalls Daueraufgaben sind die im Datenschutzmanagementsystem beschriebenen allgemeinen Aufgaben. Durch diese wird ein dauerhafter Prozess in Gang gesetzt, der eine ständige Überarbeitung und Anpassung des Verfahrens der anonymen Nutzung des ParlaNets an Veränderungen der technischen bzw. rechtlichen Rahmenbedingungen ermöglicht.

So soll beispielsweise die Bestandsaufnahme auch nach Erteilung des Auditzeichens weiterhin fortgeschrieben werden. Das Managementsystem der Landtagsverwaltung benennt Zuständigkeiten für eine fortlaufende Erfasssung und Analyse des Ist-Zustands der Datenverarbeitung im auditierten Verfahren. Wird hierbei die Nichteinhaltung datenschutzrechtlicher Vorgaben sichtbar, so können entsprechende Maßnahmen als weitere Datenschutzziele aufgenommen werden.

Es soll sichergestellt werden, dass nur geeignete Technik zum Einsatz kommt, um ausreichende Verfügbarkeit, Zugriffsgeschwindigkeit, Aktualität und Sicherheit zu gewährleisten. Weiterhin sieht das Datenschutzmanagementsystem vor, dass Änderungen der einschlägigen rechtlichen Vorschriften verfolgt und auf ihre Auswirkungen auf das auditierte Verfahren geprüft werden.

Zur Steigerung und dauerhaften Festigung des Bewusstseins und der Kenntnisse der Mitarbeiter über Fragen des Datenschutzes und der Datensicherheit finden diese Themen in Gesprächsrunden umfangreich Berücksichtigung. Außerdem soll die Formulierung eindeutiger Arbeitsziele durch Zielvereinbarungen erfolgen.

Zur Überwachung der Einhaltung der im Rahmen des Auditverfahrens festgelegten Ziele und Maßnahmen soll das Datenschutzgremium des Landtages bei Bedarf über den Stand der Umsetzung der Datenschutzziele in Kenntnis gesetzt sowie das Unabhängige Landeszentrum für Datenschutz über wesentliche Änderungen des audititerten Verfahrens informiert werden.

Bewertung:

Die Gesamtheit dieser Maßnahmen ist geeignet, einen ständigen Prozess der Begleitung und Überwachung des auditierten Verfahrens im Hinblick auf Datenschutz und Datensicherheit zu initiieren und damit das bereits erlangte Datenschutzniveau dauerhaft zu festigen. Insbesondere die Elemente der Schulungen der Administratoren sowie der regelmäßigen Berücksichtigung von datenschutzrelevanten Themen sind geeignet, die durch das Auditverfahren gewonnene Sensibilität der Mitarbeiter für Belange des Datenschutzes und der Datensicherheit auch für den Zeitraum nach der Verleihung des Auditzeichens zu erhalten.

7. Gesamtbewertung

Da sich aus der Bestandsaufnahme ergibt, dass das Verfahren der anonymen Nutzung des ParlaNet im Hinblick auf Datenschutz und Datensicherheit einwandfrei durchgeführt wird,

bedarf es für die Verleihung eines Audits aktuell keiner Verbesserung des Verfahrens. Erforderlich ist daher lediglich die dauerhafte Sicherstellung des gegenwärtigen Niveaus, das durch die von der Landtagsverwaltung festgelegten Datenschutzziele ausreichend gewährleistet wird.

Die Verleihung des Datenschutz-Audits gemäß § 43 Abs. 2 LDSG SH ist damit gerechtfertigt.

Kiel, den 9. Januar 2003

Dr. Helmut Bäumler