Gutachten

zur Reauditierung

Auditverfahren gemäß § 43 Abs. 2 LDSG

Stadt Bad Schwartau

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstraße 98

24103 Kiel

Kiel, 18. April 2018

Auditor: Heiko Behrendt

Az.: 16.01/02.008

E-Mail: mail@datenschutzzentrum.de

Inhaltsverzeichnis

1 Reauditierung

1.1 Gegenstand

Der Stadtverwaltung Bad Schwartau wurde bereits am 16. Juni 2004 vom Unabhängigen Landeszentrum für Datenschutz (ULD) nach Durchführung eines Datenschutzaudits zu

- der „Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung der Stadtverwaltung Bad Schwartau ohne Berücksichtigung der Rechtmäßigkeit der Datenverarbeitung in den einzelnen Fachverfahren der Fachämter“ und
- dem „Anschluss des internen Netzes der Stadtverwaltung an das Internet“

ein Datenschutzauditzeichen für drei Jahre verliehen.

In den Jahren 2007, 2010 und 2013 fanden nach Ablauf der Gültigkeit Reauditierungen statt, in denen überprüft wurde, ob die Kriterien für die Verleihung des Datenschutzauditzeichens weiterhin Bestand hatten.

Die Stadtverwaltung Bad Schwartau hat so dann auch in 2016 nach Ablauf des Datenschutzauditzeichens eine erneute Reauditierung beantragt. Aufgrund der Erneuerung der technischen IT-Komponenten und Veränderungen im Datenschutzmanagement fand eine umfassende Begutachtung der implementierten Datenschutz- und Informationssicherheitsprozesse statt.

Das aktuelle Gutachten des Datenschutzauditverfahrens ist auf der o. a. ULD-Webseite „https://www.datenschutzzentrum.de/“ abrufbar.

1.2 Vorgehen

Die Reauditierung erfolgte unter Berücksichtigung der „Hinweise des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Datenschutz-Behördenaudits nach § 43 Abs. 2 LDSG“. Es wurden folgende Schritte durchgeführt:

- Überprüfung der Abgrenzung des Auditgegenstandes,
- Analyse der Dokumentation für den Nachweis zur Einhaltung der Datenschutzvorschriften,
- Begutachtung der Wirkungsweise des Datenschutz- und Informationssicherheitsmanagementsystems (DISMS) und der Erreichung der festgelegten Datenschutzziele,
- Hervorhebung von anerkennenswerten und datenschutzfreundlichen Datenverarbeitungsprozessen,
- stichprobenartige Überprüfung der Umsetzung der festgelegten Datenschutz- und IT-Sicherheitsmaßnahmen,
- Überprüfung der Einhaltung datenschutzrechtlicher und bereichsspezifischer Vorschriften in Bezug auf den Auditgegenstand,
- Erstellung eines Gutachtens,
- Verleihung des Datenschutzauditzeichens.

Die von der Stadtverwaltung Bad Schwartau vorgelegte Dokumentation für den Auditgegenstand bildete die Grundlage für die Begutachtung vor Ort.

2 Feststellungen im Rahmen der Begutachtung

2.1 Datenschutz- und Informationssicherheitsstrategie

In der Leitlinie für Datenschutz und Informationssicherheit hat die Stadtverwaltung Bad Schwartau Leitaussagen zu ihrer **Datenschutz- und Informationssicherheitsstrategie** zusammengefasst, um die festgelegten Datenschutz- und Sicherheitsziele und das angestrebte Datenschutz- und Sicherheitsniveau für alle Mitarbeiterinnen und Mitarbeiter zu dokumentieren. Mit der Datenschutz- und Sicherheitsleitlinie bekennt sich die Leitungsebene zu ihrer Verantwortung für Datenschutz und Informationssicherheit.

Für die Implementierung einer nachvollziehbaren und messbaren Sicherheit der IT orientiert sich die Stadtverwaltung an dem international anerkannten Grundschutzstandard des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Dabei werden die datenschutzrechtlichen Anforderungen für die personenbezogene Datenverarbeitung berücksichtigt.

Es wurden folgende Datenschutz- und Informationssicherheitsziele festgelegt:

- Es werden nur die für die Aufgabenerfüllung benötigten Daten gespeichert und vorgehalten (Datenminimierung),
- die bereichsspezifischen Vorschriften zur ordnungsgemäßen Datenverarbeitung und des Datenschutzes werden eingehalten (Vertraulichkeit),
- die Daten werden nur in der vorgeschriebenen Verfahrensweise verarbeitet (Integrität),
- die von den Nutzern benötigten Daten stehen kontinuierlich im erforderlichen Umfang zur Verfügung (Verfügbarkeit),
- Daten werden nur für den Zweck verarbeitet und ausgewertet, für den sie erhoben wurden (Nichtverkettbarkeit/Zweckbindung),
- Verfahren werden so gestaltet, dass die Stadtverwaltung in die Datenverarbeitung eingreifen kann und den Betroffenen die Ausübung der ihnen zustehenden Rechte (u. a. Auskunft, Berichtigung, Sperrung und Löschung) wirksam möglich ist (Intervenierbarkeit), und
- Betroffene und auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen können erkennen, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt (Transparenz).

Darüber hinaus ist in der Leitlinie festgelegt, dass zur Erreichung der Datenschutz- und Informationssicherheitsziele ein behördlicher Datenschutzbeauftragter (DSB) ernannt und ein Datenschutz- und Informationssicherheitsmanagement-Team (DISM-Team) eingerichtet wird.

2.2 Datenschutz- und Informationssicherheitsmanagement-Team (DISM)

Das **DISM-Team** initiiert, steuert und kontrolliert den Datenschutz und Informationssicherheitsprozess in der Stadtverwaltung Bad Schwartau. Es besteht aus folgenden Personen:

- Herr Toll, Büroleitender Beamter,
- Herr Ratzmer, behördlicher Datenschutzbeauftragter,
- Herr Miotke, IT-Leitung.

Das DISM-Team führt regelmäßige oder anlassbezogen Sitzungen durch. Es

- steuert und koordiniert den Informationssicherheitsprozess und stellt den dazugehörigen Informationsfluss sicher,
- initiiert und koordiniert die Erstellung von allgemein notwendigen Datenschutz- und IT-Sicherheitsrichtlinien,
- erstellt und koordiniert datenschutz- und sicherheitsrelevante Konzepte und überwacht deren Umsetzung,
- erstellt und koordiniert weiterführende Konzepte, soweit sie für den Datenschutz und die Informationssicherheit erforderlich sind,
- legt in Zusammenarbeit mit den Verantwortlichen der Fachbereiche die Datenschutz- und Sicherheitsanforderungen / Sicherheitsstufe von Fachverfahren fest (Schutzbedarfsfeststellung) und überprüft diese,
- koordiniert datenschutz- und sicherheitsrelevante Projekte,
- untersucht datenschutz- und sicherheitsrelevante Zwischenfälle,
- kann alle relevanten Verträge und Konzepte oder deren Entwürfe einsehen,
- veranlasst oder erstellt Berichte über Datenschutz- und Sicherheitsvorfälle.

Die Aufgaben und Zuständigkeiten des DISM-Teams sowie die Aufgaben des behördlichen Datenschutzbeauftragten sind im Dokument „Datenschutz- und Informationssicherheitsmanagement“ festgelegt (vgl. Tzn. 2.3 und 2.7).

2.3 Behördlicher Datenschutzbeauftragter (DSB)

Im Rahmen des Audits fand aufgrund der organisatorischen Einrichtung des Datenschutz- und Informationssicherheitsmanagement auch eine Umbesetzung der Zuständigkeit für den Datenschutz statt. Als behördlicher Datenschutzbeauftragter wurde Herr Ratzmer gemäß § 10 LDSG schriftlich bestellt. Er ist für die organisatorische Abwicklung und Koordination der Datenschutzmanagementsitzungen, umzusetzender Maßnahmen und eines zugehörigen Berichtswesens einschließlich Managementberichten an die Leitung zuständig. Darüber hinaus werden von ihm in Zusammenarbeit mit der IT-Leitung folgende Aufgaben wahrgenommen:

- Führen der Verzeichnisse der Verarbeitungstätigkeiten,
- Organisation des Datenschutzes (Dienstanweisungen und Richtlinien),
- Mitwirkung bei der Planung, Durchführung und Weiterentwicklung von Qualifizierungsmaßnahmen,
- Mitwirkung bei der Planung und Gestaltung der informationstechnischen Infrastruktur,
- Schulung und Beratung der Mitarbeiterinnen und Mitarbeiter in datenschutzrelevanten und praktischen Fragen,
- Bearbeitung von Anfragen Betroffener, insbesondere zur Wahrnehmung von Rechten (Auskunft, Berichtigung, Sperrung, Löschung),
- Kontrolle der Datenverarbeitung der Dienststelle,
- Überprüfung der Einhaltung von technischen und organisatorischen Maßnahmen zur Datensicherheit,
- Kontrolle der Datenverarbeitung bei Auftragnehmern,
- Beteiligung bei der Freigabe von automatisierten Verfahren,
- Untersuchung datenschutz- und sicherheitsrelevanter Vorfälle,
- Ansprechpartner für die Landesbeauftragte für Datenschutz Schleswig-Holstein und
- Sensibilisierungs- und Schulungsmaßnahmen zum Datenschutz und zur Informationssicherheit.

Nach seiner Bestellung zum behördlichen Datenschutzbeauftragten wurde von ihm ein Schwerpunkt bei der Mitarbeiterschulung und Mitarbeitersensibilisierung gesetzt. In vier Veranstaltungsterminen schulte er alle Mitarbeiterinnen und Mitarbeiter der Stadtverwaltung. Themen waren u. a. der Stellenwert des Datenschutzes und der Informationssicherheit bei der Stadtverwaltung Bad Schwartau, Aufgaben des Datenschutz- und Informationssicherheitsmanagements sowie praktische Datenschutztipps für den Umgang mit Daten am Arbeitsplatz. Darüber hinaus hat er für die Mitarbeiterinnen und Mitarbeiter mehrere Hinweise zu verschiedenen Themen erstellt. Alle Informationen lassen sich auch im Intranet der Stadtverwaltung abrufen.

Der Datenschutzbeauftragte wird bei allen Projekten, die relevante Auswirkungen auf die Informationsverarbeitung haben, sowie bei der Einführung neuer Anwendungen und IT-Systeme beteiligt. Darüber hinaus ist festgelegt, dass der Datenschutzbeauftragte interne Audits durchführt, bei denen stichprobenartig die Umsetzung, Wirksamkeit und Praktikabilität der getroffenen Maßnahmen überprüft werden.

Im Rahmen des Datenschutz- und Informationssicherheitsmanagements hat die Stadtverwaltung für die Behandlung von Datenschutz- und Sicherheitsvorfällen Zuständigkeiten und Organisationsabläufe festgelegt. Die Mitarbeiterinnen und Mitarbeiter können einen identifizierten Datenschutz- und/oder Sicherheitsvorfall den zuständigen Personen anzeigen, so dass nach der Mitteilung der Vorfall sofort bearbeitet werden kann. Die Ergebnisse der Überprüfung werden schriftlich dokumentiert.

Diese Maßnahmen zeigen, dass die Mitarbeiterinnen und Mitarbeiter der Stadtverwaltung durch den Datenschutzbeauftragten vorbildlich sensibilisiert wurden.

2.4 Zentrale IT-Koordination

Die zentrale IT-Koordination erfolgt durch die IT-Abteilung. Dieser Aufgabenbereich ist unmittelbar der Amtsleitung „Zentrale Dienste und Finanzen“ zugeordnet. Aufgaben der IT-Abteilung sind insbesondere:

- Festlegen von IT-Standards durch das Amt für Zentrale Dienste und Finanzen im Abstimmung mit den Fachämtern,
- Unterstützung der Fachämter bei der Realisierung des IT-Konzeptes,
- Beschaffung der Hard- und Software für die Kernverwaltung (Rathaus),
- Installation der Hard- und Software, soweit dies nicht Dataport oder anderen externen Dienstleistern übertragen wurde,
- Hard- und Softwareadministration, soweit diese nicht im Einzelfall der Fachabteilung oder externen Dienstleistern übertragen wurde,
- Führung der technischen Dokumentation,
- Ermittlung von datenschutzrechtlichen Problemstellungen, Unzulänglichkeiten und Sicherheitsmängeln in Zusammenarbeit mit dem Datenschutzbeauftragten,
- Unterrichtung des Bürgermeisters über festgestellte Mängel und daraufhin getroffene Maßnahmen,
- Erstellung der Dokumentationen für alle eingesetzten Verfahren in Zusammenarbeit mit den Fachbereichen und dem Datenschutzbeauftragten,
- Systemadministration der Zentralrechner und der Arbeitsstationen,
- Schaffung der Einsatzvoraussetzungen,
- Einweisung der Mitarbeiterinnen und Mitarbeiter,
- Installation, Wartung und Instandsetzung soweit selbständig möglich,
- Benutzerverwaltung, soweit nicht im Fachverfahren implementiert (Active-Directory),
- Durchführung der Datensicherung,
- Überwachung des Systemverhaltens,
- Fehlerbehandlung,
- Software-Installation,
- Aufbau und Pflege des Acitve-Directorys,
- Lizenzverwaltung.

Die systembezogenen Arbeiten werden durch die IT-Administration dokumentiert. Über automatisierte Vordrucke beauftragen die Fachabteilungen die IT-Administration, Berechtigungen für Mitarbeiterinnen und Mitarbeiter auf der Arbeitsplatzebene zu konfigurieren. Darüber hinaus werden Systemarbeiten durch externe Dienstleister von der IT-Administration überwacht. Die Ausfallsi-

cherheit der zentralen IT-Komponenten und die Datensicherung wurden durch die Installation neuer technischer IT-Komponenten verbessert.

Die Ausbildung bzw. Fortbildung der IT-Administration wird stetig fortgeführt. Bei der Auswahl der Schulungen wird darauf geachtet, dass die Seminare aufeinander aufbauen und in regelmäßigen Zeitabständen stattfinden. Während des Audits wurde durch eine Fachfirma eine Schulung für die Administration der Firewall durchgeführt.

2.5 Schutzbedarfsfeststellung und Risikoanalyse

Die Stadtverwaltung Bad Schwartau hat mit der Schutzbedarfsfeststellung den Schutzbedarf für ihre Datenverarbeitung festgelegt. Die Festlegung des Schutzbedarfs orientierte sich an möglichen Schäden, die mit einer Beeinträchtigung der Datenverarbeitung und damit der jeweiligen Geschäftsprozesse und der Rechte und Freiheiten betroffener Personen verbunden sind.

Die Durchführung der Schutzbedarfsfeststellung wurde in dem Dokument „Schutzbedarfsfeststellung und Risikoanalyse“ nachvollziehbar anhand folgender Schadensszenarien beschrieben:

- Verstoß gegen Gesetze / Vorschriften / Verträge, insbesondere die Verpflichtung zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts bzw. Verletzung der Grundrechte und Grundfreiheiten natürlicher Personen,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Innen- oder Außenwirkung und
- finanzielle Auswirkungen.

Zusammenfassend wurde der Schutzbedarf für die Datenverarbeitung mit Fachanwendungen in die Schutzkategorie „hoch“ eingestuft. Demzufolge wurde der festgelegte Schutzbedarf auch auf die für die Fachanwendungen eingesetzten IT-Systeme, das Datenkommunikationsnetz sowie die Gebäude- und Rauminfrastruktur übertragen.

Mit einer ergänzenden Risikoanalyse hat die Stadtverwaltung Bad Schwartau bei der Umsetzung der Schutzmaßnahmen überprüft, ob die Gefährdungen für ein hohes Schutzniveau ausreichend eingedämmt sind.

2.6 Infrastruktur, IT-Systeme, Netz und Anwendungen

Die Stadtverwaltung Bad Schwartau hat zum Schutz ihrer Daten nach der Grundschutzmethode einen sogenannten Informationsverbund festgelegt. Dem Verbund wurden die schützenswerten Objekte – Infrastruktur, IT-Systeme, Netz und Anwendungen – mit den erforderlichen Bausteinen und Schutzmaßnahmen des Grundschutzkompendiums zugeordnet. Dabei wurden für die Gewährleistung der Rechte und Freiheiten betroffener Personen in einem eigenentwickelten Baustein auch Schutzmaßnahmen aus dem „Standard-Datenschutzmodell“ (SDM) des ULD ergänzt.

Bei der Anwendung der Grundschutz-Instrumente wurde die **Basisabsicherung des modernisier-**

ten Grundschutzes mit ca. 500 Schutzmaßnahmen umgesetzt. Durch diese Verfahrensweise wurde die Komplexität der Schutzmaßnahmen reduziert, aber nur insoweit, dass keine bedeutsamen Gefährdungen bzw. Risiken für die Datenverarbeitung der Stadtverwaltung Bad Schwartau oder für betroffene Personen eingegangen werden.

2.6.1 Gebäude und Büroräume

Die Stadtverwaltung Bad Schwartau ist in einem Gebäude untergebracht. Es ist eine ausreichende räumliche Abschottung der einzelnen Fachabteilungen vorhanden. Alle Büroräume sind mit einem Schließsystem ausgestattet. Räume mit schützenswerten Informationen verfügen über verschließbare Schränke. Für die Entsorgung sensibler papierener Daten ist ein verschließbarer Behälter vorhanden.

2.6.2 Serverraum

Die zentralen IT-Komponenten der Stadtverwaltung Bad Schwartau sind in zwei verschlossenen Serverräumen installiert. Nur die IT-Administration hat Zutritt. Die Serverräume sind mit einer Brandmeldeanlage sowie mit einem Klimatisierungssystem ausgestattet.

2.6.3 IT-Komponenten

Die Stadtverwaltung verfügt über folgende Hard- und Softwarekomponenten:

Server, Clients, Tablets:

3 Server HP DL 380 G9 als Hostsysteme für virtuelle Maschinen auf Basis Hyper-V

1 IBM Storwize V3700 als SAN

1 Server HP DL 380 G9 als SQL-Server

2 Server HP DL 380 G7 als Backup-Server mit 2 x QNAP NAS

1 Server HP DL 380 G7 als Monitoring-Server

17 Server Windows 2012 R2 – virtuelle Maschinen –

1 Server Linux (Monitoring-Server auf Basis Nagios)

2 Clients Windows 10 Professional

11 Clients Windows 7 Professional

56 Windows embedded (Betriebssystem Thin-Clients)

4 Linux (OS Thin-Client)

6 iPads, iOS

Virtuelle Applikationsserver mit Applikationen:

- **SRV-APP01**
  BauR-Archiv, Cip, Cip_Archiv, HSH (meso96), Iris (Migewa), PC-Wahl 9.0, RIB (Arriba), Vollkomm
- **SRV-APP02**
  Time3010
- **SRV-CA01**
  Zertifikats-Server
- **SRV-DC01 und SRV-DC02:**
  Domänencontroller, Lizenzserver, Active Directory
- **SRV-DDC01**
  Desktop Delivery Controller (Bereitstellung Virtueller Desktops)
- **SRV-EX01**
  Exchange-Server für die Postfachbereitstellung
- **SRV-File01**
  HC-Owig32, KGIS (Proton-GIS), Migewa, More-Rubin, PC-Wahl, ProsozBau, ProsozWohngeld, Reahdat Elan, Salto, Schuldenverwaltung, SFirm, Vollkomm, Speicherort für Benutzerprofile, Zentrale Ablage
- **SRV-KOM01**
  Iris (Meso), Transportagent E-Gewerbe
- **SRV-MGMT01**
  Management-Server, Windows Update Server, Zentrale AV-Console, Verwaltungskonsole für Igel Thin-Clients
- **SRV-print-01**
  Printserver für zentrale Druck-, Kopier-, Scan- und Faxsysteme
- **SRV-WEB01**
  More Rubin VIS, XAMPP
- **SRV-WI01**
  Bereitstellung Citrix WebInterface
- **SRV-XA01, SRV-XA02, SRV-XA03, SRV-XA04**
  Citrix Applikations-Server mit Load-Balancing. Installierte Software: Adobe Acrobat Reader, Arriba Client, Autodesk Design Review2013 (DWG-Viewer), RBBau-CD, Cip-Kommunal (Client), Citrix Receiver, Google Chrome, Java, Microsoft Office Standard 2010, Owi 21 Client local, PDF-Creator, ProsozBau Client, ProsozW Client, SFirm, Trend Micro OfficeScan Agent, VfSt StAZ Generalregister

Für die 3 Hyper-V-Hosts wurde ein Hyper-V-Cluster gebildet. Hierdurch ist es möglich, die virtuellen Maschinen im laufenden Betrieb von einem Host auf einen anderen „umziehen" zu lassen. Dadurch ist die Wartung einzelner Hosts möglich bzw. im Falle des Ausfalls eines Hosts können sämtliche Server weiter betrieben werden.

Die Zentralrechner sowie die Netzwerkkomponenten sind mit unterbrechungsfreien Stromversorgungen ausgestattet, um Datenverlust bei Stromausfall vorzubeugen. Ferner verfügt das Rathaus über eine Notstromversorgung, die nach ca. 15 Sekunden die Stromversorgung u. a. für die zentralen IT-Systeme übernimmt.

2.6.4 Datenorganisation

Die mit den automatisierten Verfahren erzeugten Datenbestände werden in den eingerichteten Datenbanken bzw. in einer Datenstruktur, die der Ämtereinteilung entspricht, auf einem Zentralrechner gespeichert. Der Zugriff auf die Daten wird über die Vergabe von Berechtigungen gesteuert.

2.6.5 Arbeitsplätze

Es werden überwiegend Thin-Clients eingesetzt. PCs werden nur an Arbeitsplätzen eingesetzt, wo der Einsatz von Thin-Clients aus technischen Gründen nicht möglich ist. Die an den PCs und Thin-Clients vorhandenen Schnittstellen (u. a. USB, Bluetooth) und Laufwerke sollen mit einer neuen Sicherheitssoftware „DeviceWatch“ der Firma itWatch GmbH reglementiert werden, so dass nur berechtigte Geräte angeschlossen werden können.

Neben den Fachanwendungen wird eine einheitliche Bürokommunikation-Standardsoftware eingesetzt. Auf den Arbeitsstationen wurden die Gruppenrichtlinien von Microsoft aktiviert, so dass z. B. Systemfunktionen für die Mitarbeiterinnen und Mitarbeiter nicht im Zugriff stehen.

Die automatische Verteilung einer Virenscan-Engine wird ebenfalls durch eine entsprechende Gruppenrichtlinie sichergestellt.

2.6.6 Tablets

In den Fachbereichen (Bauamt und Bürgermeistervorzimmer) werden zur Unterstützung der umzusetzenden Aufgaben iPads der Firma Apple eingesetzt. Diese werden mit einer Mobile-Device-Management-Software „Sophos Mobil Control“ von der IT-Koordination auf die erforderlichen Funktionen und Anwendungen/Apps reglementiert. Die Managementsoftware ist lokal auf einem zentralen virtuellen Server installiert worden, so dass über die Software erstellte Sicherheitsrichtlinien auf die mobilen Geräte übertragen werden können. Über die zentral vorgegebenen Sicherheitsrichtlinien wurden die Zugriffe auf Funktionen der mobilen Geräte und die nutzbaren Apps bzw. Fachanwendungen eingestellt, so dass eine Absicherung der auf den Geräten befindlichen Daten gewährleistet wird. Darüber hinaus werden die Daten auf den iPads standardmäßig verschlüsselt.

2.6.7 Hard- und Softwarepflege durch externe Dienstleister

Die Hard- und Softwarepflege wird durch externe Dienstleister abgewickelt. Durchgeführte (Fern)wartungen werden überwacht und protokolliert.

2.6.8 Datensicherung

Für die Datensicherung setzt die Stadtverwaltung Bad Schwartau zwei separate physikalische Server mit gespiegelten Festplatten ein. Die Backupsysteme sind in separaten Technikräumen mit voneinander getrennten Brandabschnitten installiert. Die Datensicherung erfolgt jeweils auf ein Speichersystem mit 8 x 3 TB HDDs. Der Status der Datensicherung wird regelmäßig geprüft. Zusätzlich werden fehlgeschlagene Jobs den Administratoren per Mail zugesendet.

2.6.9 Internes Netz, Firewall und Netzübergänge

In der Stadtverwaltung Bad Schwartau wurde eine strukturierte Verkabelung für die Datenverarbeitung implementiert. Sämtliche aktive Netzgeräte (Switches und Router) sind in Serverschränken untergebracht. Das Netz der Stadtverwaltung Bad Schwartau ist für die Datenkommunikation mit Dataport über das Landesnetz Schleswig-Holstein angeschlossen. Die Netzübergabepunkte sind über eine Firewall geschützt. Der Datenverkehr des verwaltungsinternen Netzes mit externen Netzen wird an den Netzübergängen über die Firewall freigeschaltet. Es gilt das Prinzip: „Es ist alles verboten, was nicht ausdrücklich erlaubt ist."

Der Datenverkehr wird nicht nur auf seine Zulässigkeit, sondern bereits von der Firewall auch auf schadhafte Inhalte wie Viren, Würmer und Trojaner geprüft. Die Stadtverwaltung Bad Schwartau setzt hierfür eine Sicherheitssoftware ein, die die übertragenen Daten insbesondere bei der E-Mail- und Web-Kommunikation auf schadhafte Inhalte kontrolliert.

Darüber hinaus wird für den Einsatz der Tablets ein internes verschlüsseltes WLAN-Netz eingesetzt. Nur befugte Mitarbeiterinnen und Mitarbeiter erhalten einen Zugriff.

2.6.10 Virenschutz

Für die Nutzung der Internetdienste E-Mail und Web sowie die Datenkommunikation über Schnittstellen und angeschlossene externe Netze setzt die Stadtverwaltung Bad Schwartau zum Schutz der Daten mehrere Antivirenprodukte ein. Auf der Firewall werden Module von Sophos und Avira eingesetzt, während auf den Servern und Clients eine Antivirensoftware der Firma Trend Micro zum Einsatz kommt. Die typischen Schutzfunktionen, wie z. B. Blockieren von Viren, Spyware, Würmer und Trojaner, sind enthalten.

2.6.11 Penetrationstest

Im Juli 2017 ließ die Stadtverwaltung Bad Schwartau von einer Fachfirma einen Penetrationstest des internen Netzes durchführen. Es wurden von über das Internet erreichbare IT-Systeme sowie auch interne IT-Systeme auf Schwachstellen überprüft. Festgestellte Sicherheitslücken wurden anschließend unter Berücksichtigung der Empfehlungen der Fachfirma beseitigt.

2.7 Dokumentation und Nachweise für die Einhaltung datenschutzrechtlicher Vorschriften

Die Stadtverwaltung Bad Schwartau hat für die automatisierte Datenverarbeitung folgende Dokumentation und Nachweise erstellt und im Rahmen der Begutachtung vorgelegt:

- Leitlinie für Datenschutz und Informationssicherheit (siehe Tz. 2.1)
- Datenschutz- und Informationssicherheitsmanagement (siehe Tz. 2.2)
- Schutzbedarfsfeststellung und Risikoanalyse (siehe Tz. 2.5)
- Konzept zur Entwicklung und Realisierung IT-gestützter Verwaltungsabläufe (siehe Tz. 2.6)
- Report Informationsverbund mit Infrastruktur, Systeme, Netz und Anwendungen
- Report Technische und organisatorische Maßnahmen
- Datensicherungskonzept
- Virenschutzkonzept
- Dienstanweisungen für die Administrationsebene und für die Nutzung der Internetdienste
- Aufgabenplan des Datenschutzbeauftragten für 2018
- Antragsverfahren über die Einrichtung, Änderung und Löschung von Benutzerkonten
- Dokumentation über die Firewallregeln
- Dokumentation über das Storage
- Dokumentation der Gruppenrichtlinien
- Checkliste für die Installation von Servern
- Merkblatt „Kennwortrichtlinien für Fachanwendungen“
- Merkblatt „Löschung von Daten“
- Merkblatt „Nutzung von Wechseldatenträgern“
- Merkblatt „Sicherer Arbeitsplatz“
- Merkblatt „Umgang mit E-Mail“
- Merkblatt „Verhalten bei Auftreten von Schadprogrammen“
- Merkblatt „Verhalten bei Datenschutz- und Informationssicherheitsvorfällen“

Für die Dokumentation wurde auf einem Fileserver folgende Struktur angelegt:

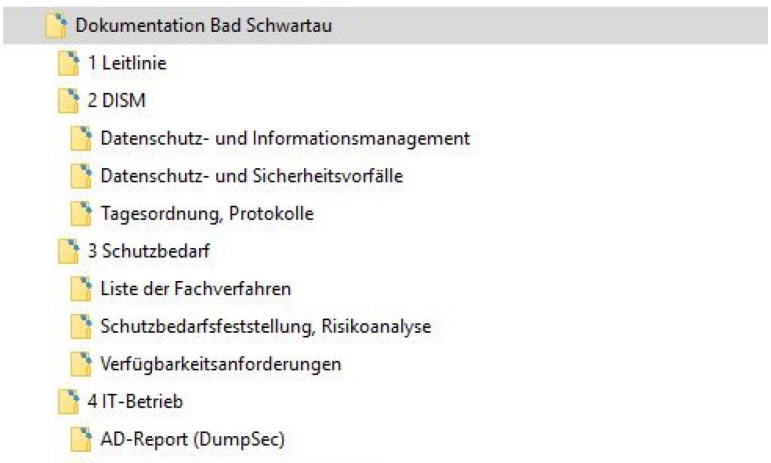

Abb. 1: Ablagestruktur Datenschutz- und Informationssicherheit

2.7.1 Report „Informationsverbund mit Infrastruktur, Systeme, Netz und Anwendungen“

Der Informationsverbund der Stadtverwaltung Bad Schwartau enthält die Objekte für Infrastruktur, Systeme, Netz und Anwendungen. Die im Rahmen einer Bestandsaufnahme erhobenen Objekte wurden mit der Software „Verinice“ erfasst und können über den Report dargestellt werden.

Abb. 2: Ausschnitt Informationsverbund Bad Schwartau

2.7.2 Report „Modellierung der Grundschutzbausteine“

Der Report „Modellierung der Grundschutzbausteine“ enthält die dem Informationsverbund zugewiesenen Prozess- und Systembausteine der entsprechenden Schichten mit den umzusetzenden Anforderungen.

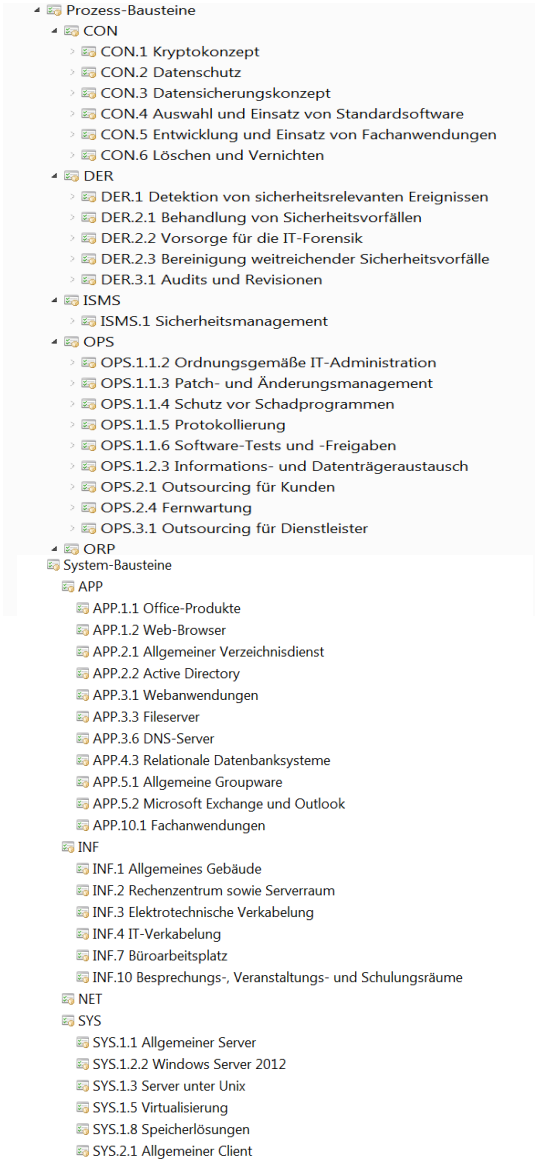

Abb. 3: Ausschnitt Prozess- und Systembausteine

Die nachfolgende Abbildung enthält einen Auszug der umzusetzenden Anforderungen für das

Datenschutz- und Informationssicherheitsmanagement. Da das Grundschutzkompendium des BSI für den Datenschutz keine konkreten Anforderungen bereitstellt, wurde der Baustein „CON2 Datenschutz“ vom ULD für die Datenverarbeitungsprozesse der Stadt Bad Schwartau als Vorlage vorgegeben.

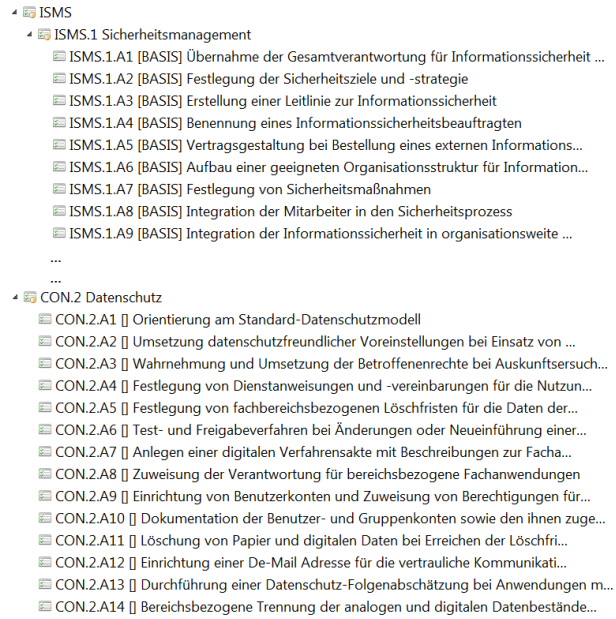

Abb. 4: Ausschnitt Bausteine zum Datenschutz- und Informationssicherheitsmanagement

2.7.3 Verfahrensakten mit Verfahrensbeschreibungen

In den überprüften Verfahrensakten befinden sich Informationen über die Einführung und den Betrieb des Verfahrens. In digitaler Form wird die „Verfahrensakte“ mit folgender Gliederung geführt:

- Allgemeiner Schriftverkehr
- Verfahrensbeschreibung
- Verzeichnis von Verarbeitungstätigkeiten
- Risikoanalyse
- Test und Freigabe
- Berechtigungskonzept
- Verträge mit Dienstleistern
- Handbücher
- Protokolle und Kontrollen
- Updates

- Hardware

Dokumente, die nicht digitalisiert vorliegen, werden in einer entsprechenden papierenen Verfahrensakte geführt.

2.7.4 IT-Konzept

Die Stadtverwaltung Bad Schwartau hat die technischen und organisatorischen Vorgaben für die Verarbeitung personenbezogener Daten in einem informationstechnischen Konzept zusammengefasst.

Neben Vorgaben für die IT-Systeme und Netzinfrastruktur sind im IT-Konzept die Aufgaben der IT-Administration festgelegt. Das IT-Konzept dokumentiert zusammen mit der Systemdokumentation und den Verfahrensakten den Ist-Stand der Informations- und Kommunikationsinfrastruktur der Stadtverwaltung Bad Schwartau.

2.7.5 Dienstanweisungen und Richtlinien

Die festgelegten technischen und organisatorischen Maßnahmen wurden zum Teil in Handlungsanweisungen im Rahmen von Dienstanweisungen und/oder Richtlinien mitarbeiterbezogen übertragen.

2.7.6 Auftragsdatenverarbeitung mit Dienstleistern

Die Stadtverwaltung Bad Schwartau hat im Rahmen einer Auftragsdatenverarbeitung u. a. folgende Dienstleister beauftragt:

- **Reisswolf-Papierentsorgung**

Die Stadtverwaltung Bad Schwartau entsorgt über Sicherheitsbehälter Papierabfälle und ausgesonderte digitale Datenträger über die Firma Reisswolf GmbH. Die Firma sichert eine Vernichtung im Rahmen der DIN 66399 mit der Schutzklasse 2 zu.

- **Bosch Data GmbH und fat IT solutions GmbH**

Die Firmen sind u. a. damit beauftragt, die IT-Administration in den Bereichen Netz und Wartung der Server zu unterstützen. Erforderliche Dienstleistungen werden von der Stadtverwaltung Bad Schwartau anlassbezogen beauftragt und kontrolliert.

- **Dataport, CIP und HSH-Kommunalsoftware**

Von den Dienstleistern werden einzelne Fachverfahren administriert. Der Zugriff erfolgt überwie-

gend im Rahmen einer durch die IT-Administration der Stadtverwaltung Bad Schwartau kontrollierten (Fern-)Wartung.

3 Datenschutzrechtliche Bewertung

Die automatisierte Verarbeitung personenbezogener Daten erfordert technische und organisatorische Maßnahmen, die 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 in konkrete Datensicherungsmaßnahmen umgesetzt werden und ihre Einhaltung durch das Datenschutz- und Informationssicherheitsmanagement kontrolliert wird. Dabei sind z. B. 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
- § 17 Verarbeitung personenbezogener Daten im Auftrag, Wartung

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 Überprüfung hat ergeben, dass die festgelegten Schutzmaßnahmen für Datenschutz und Informationssicherheit angemessen sind und umgesetzt werden.

Ein neuer behördlicher Datenschutzbeauftragter wurde bestellt. Er verfügt über die erforderliche Sachkunde und Zuverlässigkeit. Die ihm übertragenen Aufgaben führt er motiviert durch und sorgt bei den Mitarbeitern für Akzeptanz für die einzuhaltenden Schutzmaßnahmen. Zusätzlich führte er Datenschutz- und Informationssicherheitsschulungen für die Mitarbeiterinnen und Mitarbeiter der Stadtverwaltung durch und stellt für sie praktische Tipps für den Arbeitsalltag im Intranet der Stadtverwaltung bereit. Die IT-Koordination sorgt dafür, dass die eingesetzten IT-Komponenten dem Stand der Technik entsprechen und die erforderlichen IT-Sicherheitsprodukte eingesetzt werden.

Das Datenschutz- und Informationssicherheitsmanagement nimmt seine Aufgaben im erforderlichen Maße wahr und steuert die Datenschutz- und Informationssicherheitsprozesse.

Die im Rahmen des Datenschutz-Behördenaudits bei der Stadtverwaltung Bad Schwartau erfassten Verarbeitungsprozesse zeichnen sich besonders durch folgende datenschutzfreundliche Aspekte aus:

- Durch die Anwendung der Grundschutz-Instrumente lassen sich Schutzmaßnahmen zu den schützenswerten Bereichen – Gebäude, Räume, Clients, Server, Router, Firewall, Fachanwendungen, etc. – direkt zuordnen, so dass Datenschutz und Informationssicherheit besonders gut umgesetzt werden.
- Über einen Penetrationstest wurden von einer Fachfirma die IT-Komponenten (z. B. die Firewall und die Serverbetriebssysteme) der Stadtverwaltung Bad Schwartau auf Schwachstellen überprüft. Festgestellte Sicherheitslücken wurden von der Stadtverwaltung Bad Schwartau sofort beseitigt.
- Von der Stadtverwaltung Bad Schwartau werden überwiegend an Arbeitsplätzen Thin-Clients eingesetzt, so dass damit eine Standardisierung der Arbeitsumgebung sichergestellt wird. Ferner lassen sich Sicherheitsfunktionen zentral und einheitlich administrieren.
- Für den Anschluss des internen Verwaltungsnetzes an das Internet werden Sicherheitskomponenten eingesetzt, die unerwünschte Zugriffe abwehren. Tablets werden durch den Einsatz einer Sicherheitssoftware reglementiert und auf Systemen der Stadtverwaltung Bad Schwartau zentral verwaltet.
- Das Datenschutz- und Informationssicherheitsmanagement führt in regelmäßigen Abständen Sitzungen durch, in denen Datenschutz- und Informationssicherheitsaspekte bearbeitet werden. Darüber hinaus wurden organisatorische Abläufe für die Behandlung von auftretenden Datenschutz- und Sicherheitsvorfällen festgelegt.
- Auf die Beachtung und Umsetzung der ab dem 25. Mai 2018 geltenden Datenschutzvorschriften der Datenschutz-Grundverordnung ist die Stadtverwaltung Bad Schwartau bereits gut aufgestellt und vorbereitet.

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

Kiel, 18. April 2018 Heiko Behrendt