Beratung · Prüfung · Service

Überörtliche Prüfung
Informationstechnik
der Gemeinde Rosendahl
vom 15.07. bis 04.12.2014

GPA NRW

Heinrichstraße 1 · 44623 Herne
Postfach 101879 · 44608 Herne
Tel. 02323/1480-0

Inhaltsverzeichnis

Allgemeines zur IT-Prüfung

Wir führen die Ergänzungsprüfung der Informationstechnik (IT) im Rahmen der überörtlichen Prüfung auf der Grundlage des § 105 Gemeindeordnung NRW durch.

Auch die IT-Prüfung bei den kleinen kreisangehörigen Städten und Gemeinden findet im Kontext der schwierigen Finanzlage der Gebietskörperschaften statt. Unsere landesweite Zuständigkeit verschafft uns einen umfassenden und detaillierten Blick auf die Situation in den kommunalen Körperschaften in NRW. Nach unseren bisherigen Schätzungen wird dort insgesamt mehr als ein halbe Milliarde Euro pro Jahr für den Einsatz von IT aufgewendet. Bürger, Politik und Verwaltungsleitung erwarten vom IT-Service als Betriebsaufgabe in Zeiten der Haushaltskonsolidierung zu Recht besondere Beiträge in Richtung Sparsamkeit und Wirtschaftlichkeit.

Vor diesem Hintergrund wollen wir das Bewusstsein für Folgendes schärfen:

- Die Bedeutung der Informationstechnik für die Erschließung von Entwicklungs- und Rationalisierungspotenzialen in den Verwaltungen ist weiterhin hoch. Das Sparen *mit* IT muss daher gleichrangig neben dem Sparen *an* IT stehen.

- Wegen der besonderen Risiken dieses Aufgabengebietes müssen Aspekte der Ordnungsmäßigkeit, Sachgerechtigkeit und Rechtmäßigkeit gleichrangig neben Sparsamkeit und Wirtschaftlichkeit betrachtet werden.

Wir betrachten in der Prüfung Input- und Outputaspekte; auf der Grundlage von Indikatoren erfolgt eine Standortbestimmung und es werden Entwicklungsrichtungen und Schwerpunkte des Handlungsbedarfs sichtbar gemacht.

Es lässt sich aufzeigen, dass es Lösungen gibt, die bereits ein ausgewogenes Verhältnis von Sparsamkeit und IT-Sicherheit realisiert haben. Ein Wirkungsziel der Prüfung besteht darin, dieses Verhältnis in der Gesamtbetrachtung der nordrhein-westfälischen IT-Landschaft weiter zu verbessern.

Wir haben die Prüfung in der Gemeinde Rosendahl vom 15.07. bis 04.12.2014 durchgeführt.

Geprüft hat:	Ulrich Sdunek

Im Prüfungsbericht sind bestimmte Kernaussagen in Form einer **Feststellung** hervorgehoben. Diese Feststellungen können je nach Sachverhalt positive oder negative Wertaussagen enthalten. Eine Stellungnahme der Kommune zu negativen Feststellungen ist nur dann erforderlich, wenn im Bericht ausdrücklich darum gebeten wird. Auf der Grundlage der Untersuchungen erkannte Verbesserungspotenziale werden als **Empfehlung** ausgewiesen.

Manche Sachverhalte lassen sich bereits im Verlauf der Prüfung mündlich erörtern. Das Prüfungsergebnis wurde im Rahmen eines Abschlussgesprächs vorgestellt. Dieser Bericht enthält daher nur Informationen zu wesentlichen Erkenntnissen aus der Prüfung. Zur Durchsicht und inhaltlichen Überprüfung wurde der Gemeinde Rosendahl vor der endgültigen Fassung ein Entwurf des Prüfungsberichts übersandt.

Ergebnisse der Prüfung

Ausgangslage in Rosendahl

Die Gemeinde Rosendahl fällt in die Größenklasse der kleinen kreisangehörigen Kommunen; zum Stichtag 31.12.2012 hatte die Gemeinde 11.062 Einwohner.

In den nordrhein-westfälischen Städten und Gemeinden ist die örtliche Konzeption und Organisation zur Erfüllung der Querschnittsaufgabe „Informationstechnik" sehr unterschiedlich ausgestaltet.

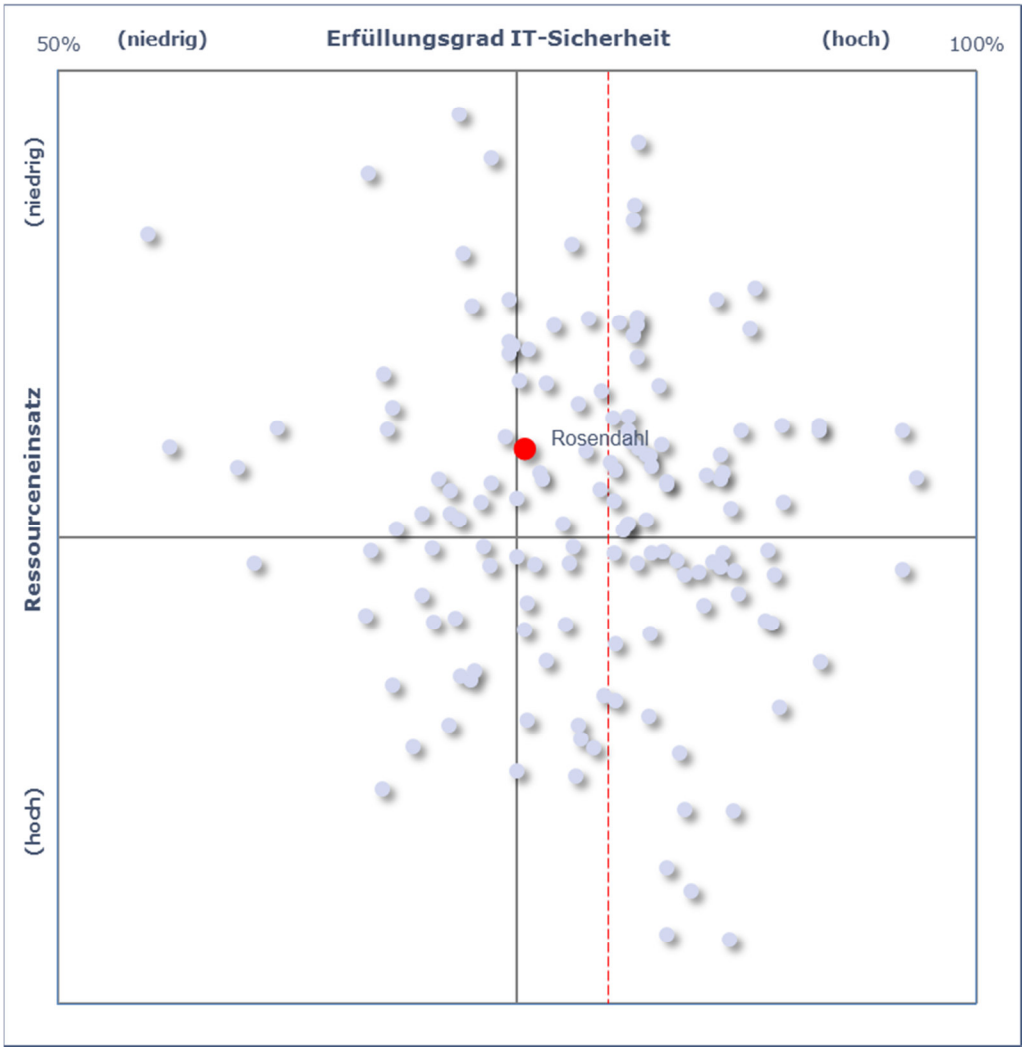
In Rosendahl ist die Betreuung der EDV-Systeme dem Fachbereich I „Zentrale Dienste und Immobilienmanagement" angegliedert. Die IT betreffende Aufgaben, die ausschließlich auf die Kernverwaltung entfallen, erledigen zwei Mitarbeiter, jedoch nur zu 1,2 vollzeitverrechneten Stellenanteilen. Durch die Verteilung der IT-Aufgaben auf zwei Mitarbeiter wird die dringend erforderliche personelle Redundanz und somit gegenseitige Vertretbarkeit hergestellt.

Rosendahl betreibt die IT autark und in eigener Verantwortung. Partiell werden Services und Dienstleistungen des IT-Dienstleisters der Stadt Münster (citeq) sowie anderer Anbieter in Anspruch genommen.

Standortbestimmung für die Gemeinde Rosendahl

Die nachfolgende Grafik zeigt für die Gemeinde Rosendahl die Standortbestimmung im interkommunalen Vergleich. Ziel ist es, das Verhältnis zwischen den eingesetzten Ressourcen und dem Erfüllungsgrad im Bereich der IT-Sicherheit im interkommunalen Vergleich zu veranschaulichen. Zudem zeigt die Positionierung der geprüften Kommune, ob und gegebenenfalls in welchem Bereich (Ressourceneinsatz oder IT-Sicherheit) vorrangiger Handlungsbedarf besteht.

Gesamtergebnis in grafischer Darstellung



Die Festlegung der Position auf der Y-Achse (Ressourceneinsatz) basiert auf betriebswirtschaftlichen Kennzahlen. Die festgestellten IT-Aufwendungen je Einwohner bzw. je Arbeitsplatz mit IT-Ausstattung werden über einen mathematischen Faktor so skaliert, dass deren Absolutwerte die gleiche Größenordnung erreichen. Dies ermöglicht, die Ausprägung der Aufwandskennzahlen in der Grafik kombiniert darzustellen.

Auf der X-Achse ist der erreichte Grad der IT-Sicherheit abgebildet. Vor dem Hintergrund der Anforderungen des BSI-Grundschutzkatalogs sehen wir einen Erfüllungsgrad von mindestens 80 Prozent als maßgeblichen Indikator für eine sichere und sachgerechte Aufgabenerfüllung an; Werte unterhalb dieser in der Grafik gestrichelt rot markierten Schwelle können ein Anzeichen für sicherheitskritische Defizite sein, die wir bei Bedarf konkret thematisieren.

Zur Einordnung des individuellen Ergebnisses in den interkommunalen Kontext ist die Grafik in vier Felder aufgeteilt, die folgenden Kombinationen von Ressourceneinsatz und Erfüllungsgrad in der IT-Sicherheit entsprechen:

- Niedriger Ressourceneinsatz, niedriger Grad der IT-Sicherheit
- Niedriger Ressourceneinsatz, hoher Grad der IT-Sicherheit
- Hoher Ressourceneinsatz, niedriger Grad der IT-Sicherheit
- Hoher Ressourceneinsatz, hoher Grad der IT-Sicherheit.

Diese Einordnung der von der geprüften Kommune erreichten Position ermöglicht die Formulierung zielgerichteter Maßnahmen im IT-Bereich.

Die in der Matrix dargestellte Positionierung von Ressourceneinsatz und Erfüllungsgrad in der IT-Sicherheit verdeutlicht zunächst einmal ein ungünstiges Verhältnis. Ungeachtet der sich in einem mittleren Vergleichsbereich befindlichen finanziellen Betrachtung haben wir im Rahmen der Prüfung den IT-Grundschutz betreffende Risiken festgestellt.

Die Aufwendungen für die IT-technische Unterstützung der Verwaltungsabläufe erreichen in der Kennzahlenbildung Werte, die im Einwohnerbezug mit 16,22 Euro unterhalb des interkommunalen Mittelwertes von 19,54 Euro und im Bildschirmarbeitsplatzbezug mit 3.818 Euro knapp oberhalb des Mittelwertes von 3.749 Euro angesiedelt sind.

Auffällig im Rahmen der Prüfung waren die hohen Abschreibungen auf Sachanlagen und immaterielle Vermögensgegenstände, die das Bewertungsergebnis für 2012 ungünstig beeinflusst haben. Ursächlich zurückzuführen sind diese Aufwendungen auf infrastrukturelle Erneuerungen, die erforderlich waren, um durch eine virtuelle Serverlandschaft einen möglichst ausfallsicheren Betrieb zu gewährleisten. Darüber hinaus hat die Gemeinde vor 2012 ein Dokumentenmanagementsystem beschafft und eingeführt. Dennoch haben wir im Rahmen der Prüfung keine Anhaltspunkte feststellen können, die auf Möglichkeiten eines kostenbewussteren Handelns hindeuten könnten.

75,4 Prozent in der IT-Grundschutzdarstellung dokumentieren eine Vergleichsgröße, die unterhalb des Mittelwertes von 78,8 Prozent und des durch uns empfohlenen Wertes von 80 Prozent liegt.

Handlungsbedarf sehen wir zunächst einmal in der räumlichen Unterbringung der technischen Infrastruktur. Darüber hinaus sind wesentliche organisatorische Elemente der IT-Sicherheitsvorsorge nicht in die Betriebsabläufe integriert. Optimierungsbedarf im IT-Sicherheitsmanagement ist insbesondere unter dem Aspekt der Einhaltung der Rechtsnormen des Datenschutzes zu sehen, die technische und organisatorische Maßnahmen verlangen, die auf der Grundlage eines IT-Sicherheitskonzeptes ermittelt und dokumentiert sind. Gerade in Anbetracht der weitgehend eigenverantwortlich betriebenen Informationstechnik sind hohe Anforderungen an die Verfügbarkeit der Systeme, an die Wahrung der Integrität der Daten und Programme sowie hinsichtlich der Vertraulichkeit im Umgang mit dem sensiblen Datenmaterial zu stellen.

Insbesondere die Umsetzung von Maßnahmen, die die IT-Sicherheitsorganisation und Notfallvorsorge betreffen, würde dazu beitragen, dem Schutzbedarf an einen eigenverantwortlichen IT-Betrieb gerecht zu werden.

Ressourceneinsatz

Inhalt und Methodik

Um die Aufwendungen, die mit der Bereitstellung und Betreuung der IT entstehen, einem interkommunalen Vergleich unterziehen zu können, legen wir einheitliche Maßstäbe und Methoden an.

Soweit neben den IT-Aufwendungen in der Kernverwaltung auch solche in Eigenbetrieben oder eigenbetriebsähnlichen Einrichtungen zu berücksichtigen sind, beziehen wir diese ein. Maßgeblich ist also nicht die jeweilige Organisationsform, sondern die Frage, welche IT-Aufwendungen die kommunale Aufgabenwahrnehmung in der Gesamtsicht verursacht.

Sachaufwendungen

Zur Erhebung der IT-Sachaufwendungen ziehen wir grundsätzlich das Ergebnis der Jahresabschlüsse (Ergebnis- und Finanzrechnung der Verwaltung sowie der zu berücksichtigenden Sondervermögen) aus dem Betrachtungsjahr 2012 heran. Soweit ein vollständiger bzw. testierter Jahresabschluss noch nicht vorliegt, greifen wir auf vorläufige Ergebnisse bzw. auf Daten aus der Finanzbuchhaltung oder internen Kostenrechnung zurück.

Personalaufwendungen und Stellenausstattung

Zur Ermittlung des Personalaufwands im IT-Bereich sowie zur Betrachtung der Stellenausstattung haben wir einen zweistufigen Ansatz gewählt, der den unterschiedlichen Organisationskonzepten in den verglichenen Kommunen Rechnung trägt:

Im ersten Schritt ermitteln wir die vollzeitverrechneten Stellen in der zentralen Organisationseinheit, die für die Bereitstellung und Betreuung der IT verantwortlich ist.

Im zweiten Schritt differenzieren wir die Betrachtung, indem wir die funktionale Ebene in den Vordergrund stellen. Anhand eines von uns festgelegten Kriterienkatalogs ermitteln wir, welche Arten von originären IT-Aufgaben in der Verwaltung wahrgenommen werden und wo dies

geschieht. Dabei verlassen wir bewusst die Betrachtung der zentralen IT und beziehen dezentrale IT-Stellenanteile mit ein. In diesem Zusammenhang bereinigen wir bei Bedarf auch solche Stellenanteile, die zwar aufbauorganisatorisch der zentralen IT zugeordnet sind, aber nach unserer Definition keine originären IT-Aufgaben wahrnehmen. Die mit der Wahrnehmung originärer IT-Aufgaben entstehenden Personalkosten ermitteln wir anschließend auf Basis der tatsächlichen Besoldungs- bzw. Entgeltgruppen anhand der Durchschnittswerte aus dem KGSt-Bericht "Kosten eines Arbeitsplatzes" in der für das Betrachtungsjahr geltenden Fassung (M 1/2012, Anlage 1 - Personalkostentabellen). Damit blenden wir in der Betrachtung individuelle Personalkostenfaktoren wie etwa Dienstaltersstufen und Zuschläge explizit aus.

Sachkostenpauschale und Gemeinkostenzuschlag

Die ermittelten Personalaufwendungen bzw. Stellenanteile werden um eine Sachkostenpauschale sowie Gemeinkostenzuschläge ergänzt. Bezogen auf die vollzeitverrechneten Stellen zur Wahrnehmung originärer IT-Aufgaben und die auf diese Stellen entfallenden Personalaufwendungen berücksichtigen wir in Anlehnung an die Empfehlungen der KGSt (Bericht 7/2003) folgende Zuschläge: Eine Sachkostenpauschale für Büroarbeitsplätze in Höhe von 5.400 Euro je vollzeitverrechneter Stelle sowie ein Zuschlag für allgemeine Leistungen bzw. Leitungsaufgaben („Overhead"-Gemeinkosten) in Höhe von 20 Prozent der ermittelten Personalaufwendungen.

Ergebnisse im interkommunalen Kennzahlenvergleich

Welche Grunddaten in die Kennzahlenbildung eingeflossen sind, wird aus folgender Tabelle ersichtlich:

Grunddaten zur Kennzahlenbildung (Aufwendungen in Euro)	
IT-Sachaufwendungen	92.327
Personalaufwendungen für originäre IT-Aufgaben (ermittelt nach KGSt-Pauschalen)	67.200
Sachkostenpauschale für Büroarbeitsplätze und Gemeinkostenzuschlag gemäß KGSt-Empfehlung	19.920
Gesamtaufwendungen IT	**179.447**

Im interkommunalen Vergleich betrachten wir die Aufwendungen in Bezug auf die Einwohnerzahl bzw. die Zahl der Arbeitsplätze mit IT-Ausstattung. Die Einwohner einer Kommune sind die eigentlichen Adressaten der kommunalen Leistungserbringung. Damit sind sie auch dann eine maßgebliche Bezugsgröße, wenn es um die Abbildung interner, der Erstellung der kommunalen Endprodukte vorgelagerter Leistungen wie der IT geht. Ergänzend dazu liefert die Betrachtung der Aufwendungen je Arbeitsplatz mit IT-Ausstattung wichtige Informationen für Analysezwecke.

Die IT-Ergänzungsprüfung erstreckt sich wegen der Vielzahl kleiner kreisangehöriger Kommunen über einen mehrjährigen Zeitraum. In die nachfolgenden Vergleichszahlen wurden auch die Daten aus den Prüfungen mit einem Betrachtungsjahr vor 2012 einbezogen. So ist gewährleistet, dass alle Ergebnisse aus der laufenden Prüfrunde in diesem Segment berücksichtigt werden.

Die Kennzahlenausprägung in Bezug auf die jeweiligen statistischen Vergleichswerte ergibt sich aus nachstehenden Tabellen:

IT-Aufwendungen je Einwohner			
Minimum	Maximum	Mittelwert	**Rosendahl**
10,69 Euro	30,28 Euro	19,54 Euro	**16,22 Euro**

IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung			
Minimum	Maximum	Mittelwert	**Rosendahl**
1.878 Euro	5.886 Euro	3.749 Euro	**3.818 Euro**

Die einwohnerbezogene Kennzahl unterschreitet den entsprechenden Mittelwert, die auf den Bildschirmarbeitsplatz bezogene Kennzahl ist nahe dem Mittelwert angesiedelt. Dies ist darin begründet, dass die Verwaltung der Gemeinde Rosendahl bezogen auf die Einwohnerzahl weniger Arbeitsplätze einsetzt als der Durchschnitt der Vergleichskommunen. Damit muss eine geringere Zahl von Verwaltungsarbeitsplätzen mit IT-Ausstattung versorgt werden als es durchschnittlich der Fall ist. Eine in der Relation niedrigere Anzahl von Bildschirmarbeitsplätzen führt jedoch dazu, dass die IT-Aufwendungen auf eine kleinere Verteilungsmenge verrechnet werden und die Kennzahlenausprägung weniger positiv ausfällt als beim Einwohnerbezug.

Mit dieser Feststellung verbinden wir keine Bewertung; sie dient hier lediglich zur Erläuterung, aus welchen Gründen die von uns ermittelten Kennzahlen keine gleichgerichtete Ausprägung zeigen.

Feststellung

Im Rahmen der Prüfung haben wir keine Anhaltspunkte erkennen können, die auf Möglichkeiten nennenswerter Kostenreduzierung schließen ließen.

Eine nähere Analyse der IT-Aufwendungen je Bildschirmarbeitsplatz nach Personal-, sonstigen Sachaufwendungen und Aufwendungen für die Inanspruchnahme von Rechenzentrumleistungen der citeq zeigt mit Ausnahme der Aufwendungen für die citeq überdurchschnittliche Werte auf. Die Personalaufwendungen liegen im Vergleichsjahr 2012 bei 1.716 Euro, der Mittelwert bei 933 Euro. Die durch die hohen Abschreibungen stark beeinflussten sonstigen Sachaufwendungen sind bei 1.980 Euro angesiedelt. Der Mittelwert errechnet sich bei einem Betrag von 1.336 Euro. Personalaufwendungen und sonstige Aufwendungen machen 45 und 52 Prozent der Gesamtaufwendungen der gemeindlichen IT aus, auf Dienstleistungen eines Rechenzentrums entfallen nur drei Prozent. Wir beurteilen die vergleichsweise hohen Personal- und sonstigen Aufwendungen nicht kritisch, da sie durch die autarke Betriebsform zu begründen sind. Hier zeigt sich deutlich ein zu erwartender Substitutionseffekt, der bei geringer Auslagerung von Services auf einen Dienstleister zwangsläufig zu höheren Aufwendungen beim eigenen Personaleinsatz und den sonstigen Aufwendungen führt. Maßgeblich ist, dass die Gemeinde im Rahmen der Gesamtbetrachtung aller Aufwendungen einen wirtschaftlichen Weg gefunden hat, IT-Dienstleistungen für die Verwaltung bereitzustellen.

Controllinginstrumente im IT-Bereich

Damit eine Verwaltung ihre Aufgaben unter wirtschaftlichen Gesichtspunkten sachgerecht und zweckmäßig erfüllen kann, ist neben inhaltlicher Qualität ein Instrumentarium notwendig, mit dem sich Risiken, Abweichungen von Zielen usw. erkennen und identifizieren lassen.

Unabdingbare Voraussetzung für eine funktionierende Steuerung auf der finanzwirtschaftlichen Ebene ist zudem, dass die Kommune ihre spezifischen Kostenstrukturen kennt. Dies gilt naturgemäß auch für die Aufgabe IT. Dazu lassen sich drei elementare Kernfragen formulieren:

- Verfügt die Gemeinde Rosendahl über Kosteninformationen bezüglich der IT, die eine Analyse und Darstellung der Kostenstrukturen (Fix- und variable Kosten; Einzel- und Gemeinkosten) ermöglichen?

- Sind die maßgeblichen Kostentreiber bekannt oder lassen Datenlage und -transparenz zumindest deren Identifizierung zu?

- Kann die Gemeinde Rosendahl im Ergebnis aktiven Einfluss auf die Höhe ihrer IT-Kosten nehmen?

Diese Fragestellungen gelten gleichermaßen für Kommunen mit einem hohen Auslagerungsgrad im Bereich der IT-Services wie auch für die Verwaltungen, in denen die IT weitestgehend autonom und ohne Inanspruchnahme externer Leistungen betrieben wird.

Ziel des Controlling-Ansatzes ist es, detailliert festzustellen, wo und aus welchem Grund Kosten entstehen und wer für Kostenentwicklungen verantwortlich zeichnet. Durch eine transparente Darstellung der Kostenblöcke sollen Informationen gewonnen werden, die eine unterjährige Überwachung zulassen und eine Entscheidungshilfe für zukünftige Investitionen bieten.

Im kommunalen Haushalt der Gemeinde Rosendahl wurde für die IT ein eigenes Produkt unter der Kennzeichnung 01.014 gebildet, unter dem alle Betriebskosten zentral erfasst werden. Darüber hinaus werden die IT betreffende Rechnungen aber auch dezentral zugeordnet. Diese Verfahrensweise lässt einen differenzierten und unterjährigen Überblick über die Kostenentwicklungen der IT zu.

Feststellung

Im Rahmen der Prüfung sind uns die angeforderten Unterlagen und Informationen zeitnah und in nachvollziehbar aufbereiteter Form zur Verfügung gestellt worden. Die Grundlagen für die Beantwortung der oben genannten Kernfragen sind vorhanden.

IT-Sicherheit

Voraussetzung für einen ordnungsgemäßen Ablauf der Datenverarbeitung und die erforderliche Verlässlichkeit im Zusammenhang mit der Abwicklung der Geschäftsprozesse ist die Sicherheit der verarbeiteten Daten. Die grundsätzliche und formale Verantwortung für die Sicherheit der IT-Systeme und der Datenhaltung tragen zunächst die gesetzlichen Vertreter der kommunalen Körperschaften.

IT-Systeme haben grundsätzlich folgende Sicherheitsanforderungen (= Basisziele) zu erfüllen:

- Verfügbarkeit; die Systeme müssen die geforderten Aufgaben zum verlangten Zeitpunkt in der angeforderten Weise erfüllen.
- Integrität; Programme und Daten müssen vor Fälschung bzw. Verfälschung, Veränderung und Vernichtung geschützt werden.
- Vertraulichkeit; Daten müssen vor unbefugtem Zugriff sowie unbefugter Be- und Verarbeitung geschützt sein. Maßnahmen zur Gewährleistung der Vertraulichkeit unterstützen auch die Einhaltung von Rechtsnormen, z.B. Datenschutzgesetz oder HGB.

Grundlagen der Informationserhebung

Die Betrachtung der Sicherheitsanforderung im Rahmen der überörtlichen Prüfung beschäftigt sich mit der Frage, ob die Anforderungen in einem Umfang erfüllt sind, der einen ordnungsgemäßen und nachhaltigen IT-Betrieb gewährleistet. Das festgestellte Ergebnis drücken wir in einem Erfüllungsgrad aus. Der erreichte Erfüllungsgrad wird in einen interkommunalen Vergleich eingestellt, um der geprüften Kommune eine Positionsbestimmung zu geben und einen Überblick über die Standards zu erhalten, den die Kommunen diesbezüglich bereits erreicht haben.

Die Betrachtung ist in folgende Fragenkreise untergliedert:

- IT-Räume und IT-Infrastrukturaufbau
- Technische Ausstattung der Arbeitsplätze

- IT-Management (Konzepte, Dienstanweisungen und vergleichbare formale Regelungen sowie Risikomanagement)
- Backup und Archivierung.

Die Prüfung ist durch die Verwendung von Checklisten systematisiert. Diese Checklisten werden gemeinsam mit den IT-Verantwortlichen vor Ort ausgefüllt. Im Rahmen des Prüfungsumfanges ist nicht vorgesehen, alle Ergebnisse der Interviews zu überprüfen; dies kann nur in Einzelfällen als Stichprobe erfolgen.

Erfüllungsgrad der IT-Sicherheit im interkommunalen Vergleich

Um eine Standortbestimmung für die geprüfte Kommune zu ermöglichen, stellen wir zunächst den erreichen Gesamterfüllungsgrad in einen interkommunalen Vergleich ein. Konkrete Optimierungspotenziale thematisieren wir näher, wenn innerhalb eines Fragenkreises einzelne Prüfbausteine nennenswerte Defizite aufweisen.

> **Feststellung**
>
> Wir haben im Rahmen der Prüfung eine risikobehaftete räumliche Absicherung der technischen Infrastruktur festgestellt. Darüber hinaus fehlen wesentliche Komponenten des IT-Sicherheitsmanagements. Der mit dieser Prüfung festgestellte Gesamterfüllungsgrad beträgt für Rosendahl 75,4 Prozent, der Mittelwert liegt derzeit bei 78,8 Prozent.

Angestrebtes Ziel wäre ein Erfüllungsgrad von mindestens 80 Prozent. Dieser Wert kann jedoch nur erreicht werden, wenn ein auf dieses Ziel ausgerichteter Maßnahmenkatalog für die unterschiedlichen, im Bericht benannten Bereiche aufgestellt und planmäßig abgearbeitet wird.

Festgestellte Optimierungspotenziale zur IT-Sicherheit

Optimierungsmöglichkeiten sehen wir zunächst einmal in einer besseren Absicherung der technischen Infrastruktur. Die Konzeption eines Serverraums sieht einen abgeschlossenen Sicherheitsbereich vor. Er sollte möglichst gut zu sichernde Zugangstüren und Fenster haben, die vor Gefährdungen durch Umgebungseinflüsse, insbesondere aber gegen Feuer und Einbruch schützen.

Bei der Tür zum Serverraum handelt sich um eine Holztür, die keine Brand- bzw. Rauchschutzzertifizierung ausweist. Genauso wie die Fenster des Serverraumes bietet auch die Zugangstür keinen Schutz gegen Einbruchsversuche. Das ausgesprochen gute Alarmsystem stellt dahingehend nur einen sekundären Schutz dar.

Auch der Netzzugangspunkt für die externe Kommunikation sowie die Netzkomponenten der Unterverteilung sind in einem Raum untergebracht, der frei zugänglich ist. Darüber hinaus wird dieser betriebskritische Raum auch als Papierlager genutzt. Hier besteht die Gefahr eines unberechtigten Zugriffs auf sensible Daten, ein erhöhtes Brandrisiko und durch den ungeschützten Zugang auch von Vandalismusschäden.

Weiter sind sowohl Verteiler als auch aktive Komponenten (Server, Router, etc.) in einem Raum untergebracht. Durch einen Brand der aktiven IT könnten auch die Leitungsverteiler und Patchfelder beschädigt werden.

Darüber hinaus haben wir im Serverraum wasserführende Leitungen sowie einen Heizkörper vorgefunden.

Empfehlung

Wir sehen in der Unterbringung der Serverinfrastruktur ein Risikopotenzial und empfehlen, gemeinsam mit dem vorbeugenden Brandschutz der Feuerwehr, dem Baubereich sowie der kriminalpolizeilichen Beratung eine Schutzbedarfsanalyse zu erstellen und nach Abwägung der Erkenntnisse für eine verbesserte Absicherung der Räumlichkeiten Sorge zu tragen. In diesem Zusammenhang sollten die Risiken von Feuer und Einbruchsversuchen, das Abtrennen der wasserführenden Leitungen vom Heizungssystem, der Feuerschutz der Patchfelder sowie die Unterbringung der

technischen Netzkomponenten im Kellerbereich erörtert werden.

Optimierungsmöglichkeiten sehen wir auch hinsichtlich der Bausteine Sicherheitsmanagement und Notfallvorsorge. Insbesondere das Sicherheitsmanagement ist als Komponente der IT-Basissicherheit in der kommunalen IT-Praxis nach unseren bisherigen Erkenntnissen generell schwach ausgeprägt. Jedoch ohne eine Leitlinie zur Informationssicherheit, ohne eine geeignete Organisationsstruktur, ohne ein IT-Sicherheitskonzept, das Schutzbedarfsfeststellungen und Einwirkungsmaßnahmen enthält, ohne Dokumentationen in der Rechtevergabe fehlen wesentliche Grundlagen, die im Rahmen eines eigenständigen IT-Betriebes geboten erscheinen. Darüber hinaus verlangen die Bestimmungen des Datenschutzrechts, technische und organisatorische Maßnahmen zu ermitteln, um mögliche Gefahren bei der Verarbeitung personenbezogener Daten auszuschließen. Die vorgenannten Maßnahmen sind nach den Rechtsnormen des DSG NRW über ein fortschreibbares IT-Sicherheitskonzept zu dokumentieren.

Auch in Bezug auf vorbeuge Maßnahmen im Rahmen der Notfallvorsorge haben wir ein organisatorisches Umfeld vorgefunden, das Ansätze zur Optimierung aufzeigt. Wesentlich ist, dass die gemeindliche IT über kein Notfallhandbuch verfügt, das zumindest die Grundkomponenten, wie die Festlegung von Verantwortlichkeiten, Pläne für Sofortmaßnahmen bzw. eingeschränkte Betriebsfortführung, Wiederanlaufpläne oder Krisenkommunikationspläne enthält.

Empfehlung

Wir empfehlen zur Optimierung des IT-Sicherheitsmanagements sowie der Notfallvorsorge ein IT-Sicherheitskonzept und darüber hinaus ein Notfallhandbuch zu entwerfen.

Datenschutz

Die Gemeinden und Gemeindeverbände, deren juristische Personen öffentlichen Rechts und deren Vereinigungen führen den Datenschutz in eigener Verantwortung durch. Unter dem Gesichtspunkt der Rechtmäßigkeit der Aufgabenerfüllung ziehen wir auch in die Betrachtung ein, ob die formalen Bestimmungen des Landesdatenschutzgesetzes NRW (DSG NRW) eingehalten werden. Dabei fragen wir ab, ob gemäß § 32a DSG NRW ein Datenschutzbeauftragter mit Stellvertreter bestellt worden ist und ob ein Verfahrensverzeichnis im Sinne des § 8 DSG NRW geführt wird.

Grundsätzlich ist ein interner Datenschutzbeauftragter, d.h. ein Beschäftigter der öffentlichen Stelle, vorgesehen. Abweichend ist die Bestellung eines gemeinsamen Datenschutzbeauftragten durch mehrere öffentliche Stellen zulässig. Die Bestellung ist durch eine förmliche Organisationsverfügung gegenüber allen Beschäftigten bekannt zu geben.

Gegenstand unserer Prüfung sind nicht eventuelle Verstöße gegen die materiell-rechtlichen Bestimmungen des Datenschutzes. Allerdings vertreten wir die Auffassung, dass mit der formellen Bestellung eines Datenschutzbeauftragten elementare Voraussetzungen für die Beachtung und Einhaltung des Datenschutzes geschaffen sind. Gleiches gilt für die Führung des Verfahrensverzeichnisses, also die gesetzlich vorgeschriebene Dokumentation aller automatisierten Verfahren, mit denen die verantwortliche Stelle personenbezogene Daten aufgrund einer bestimmten Rechtsgrundlage für einen bestimmten Zweck verarbeitet. Das Verfahrensverzeichnis ist für die datenschutzrechtliche Eigen- und Fremdkontrolle unverzichtbar; es ist wesentliche Voraussetzung für die Erfüllung des öffentlichen Auskunftsanspruchs.

Feststellung

Die Funktion des Datenschutzbeauftragten ist in der Gemeinde Rosendahl ordnungsgemäß personell besetzt; eine Stellvertreterin ist bestellt.

Von der Gemeinde Rosendahl konnte in der Prüfung ein ordnungsgemäß geführtes Verfahrensverzeichnis nicht vorgelegt werden.

Empfehlung

Mit der Erstellung eines Verzeichnisses, das die in § 8 DSG NRW vorgeschriebenen Angaben zu den eingesetzten Datenverarbeitungsverfahren enthält, sollte zeitnah und mit hoher Priorität begonnen werden.

Herne, den 04.12.2014

gez.	gez.
Michael Kuzniarek Abteilungsleitung	Ulrich Sdunek Projektleitung

Überörtliche Prüfung Informationstechnik
- Erhebungsbogen IT-Sicherheit -

Name der Körperschaft:
Gemeinde Rosendahl

Gesprächstermin:
15.07.2014

geprüft hat:
Herr Sdunek

Gesprächspartner in der Kommune:
Herr Tombrink

Fragenkreis: IT-Räume und Infrastrukturaufbau

Serverraum

Baustein Serverraum:
von 21 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Angepasste Aufteilung der Stromkreise	ja	
Handfeuerlöscher	ja	
Verwendung von Sicherheitstüren und -fenstern	nein	Einfache Holztür ohne Feuer- und Rauchschutzzertifizierung; Fenster ohne bauliche Härtung gegen Einbrüche; Empfehlung: örtliche Situation mit dem vorbeugenden Brandschutz, dem technischen Baubereich sowie der kriminalpolizeilichen Beratung einschätzen
Geschlossene Fenster	ja	
Gefahrenmeldeanlage/Brandmelder	ja	
Abgeschlossene Türen	ja	
Vermeidung von Risiken durch wasserführende Leitungen	nein	Heizkörper im Serverraum; Empfehlung: Prüfung, inwieweit der Heizkörper vom wasserführenden System abgetrennt werden kann
Überspannungsschutz	ja	
Not-Aus-Schalter	nein	
Klimatisierung	ja	
Lokale unterbrechungsfreie Stromversorgung	ja	
Fernanzeige von Störungen	ja	umfassendes System von NAGIOS
Redundanzen in der technischen Infrastruktur (ohne Storage)	ja	
Technische und organisatorische Vorgaben für Serverräume	ja	
Brandschutz von Patchfeldern	nein	Patchfelder im Rack verbaut, jedoch keine räumliche Trennung von Servern und Netz
Zutrittsregelung und -kontrolle	ja	
Rauchverbot	ja	
Verwendung von hochverfügbaren Architekturen	nein	
Zentrales Speichersystem vorhanden	ja	NAS
Storage System redundant	ja	
Einsatz von Servervirtualisierung	ja	

Datenerhebung (Checkliste) zur Prüfung der IT-Sicherheit - Blatt 2

IT-Verkabelung		Baustein IT-Verkabelung: von 12 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 0x entfällt
Maßnahmen	**erfüllt?**	**Bemerkungen**
Verkabelungsart den technischen Anforderungen entsprechend	ja	CAT 5 / CAT 7
Netz-Topologie	ja	
Erneuerung der IT-Verkabelung	ja	
Redundanzen für die Primärverkabelung	nein	
Redundanzen für die Gebäudeverkabelung	ja	
Brandabschottung von Trassen	ja	
Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht	ja	
Ausreichende Trassendimensionierung	ja	
Materielle Sicherung von Leitungen und Verteilern	teilw.	Der Netzzugangspunkt für die externe Kommunikation sowie die Unterverteilung befindet sich in einem Raum, in dem auch Papier gelagert wird. Weiter ist das Racksystem zwar in die Alarmsicherung eingebunden, jedoch frei zugänglich. Empfehlung: Räumliche Trennung von der Papierlagerung in einen abgeschlossenen, nicht frei zugänglichen Bereich bzw. anderweitige Lagerung der Verbrauchsmaterialien; Erörterung mit dem technischen Baubereich
Dimensionierung und Nutzung von Schranksystemen	ja	
Neutrale Dokumentation in den Verteilern	ja	
Laufende Fortschreibung und Revision der Netzdokumentation	ja	

Sicherheitsgateway		Baustein Sicherheitsgateway: von 19 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 0x entfällt
Maßnahmen	**erfüllt?**	**Bemerkungen**
Outsourcing des Sicherheitsgateway	☐	Sicherheitsgateway ausgelagert, keine unmittelbare Prüfung erfolgt
Entwicklung eines Konzepts für Sicherheitsgateways	ja	
Auswahl geeigneter Grundstrukturen für Sicherheitsgateways	ja	
Content-Filter im Einsatz	ja	
Proxyserver im Einsatz	ja	
Gateway redundant	ja	
Schulung der Administratoren des Sicherheitsgateways	ja	
Protokollierung der Sicherheitsgateway-Aktivitäten	ja	
Integration von Proxyservern in das Sicherheitsgateway	ja	
Integration von VPN-Komponenten in ein Sicherheitsgateway	ja	
Integration von Virenscannern in ein Sicherheitsgateway	nein	
Einsatz von Stand-alone-Systemen zur Nutzung des Internets	entfällt	
Adressumsetzung - NAT (Network Address Translation)	ja	
Intrusion Detection und Intrusion Prevention Systeme	ja	
Integration eines Webservers in ein Sicherheitsgateway	ja	
Integration eines E-Mailservers in ein Sicherheitsgateway	ja	
Integration eines Datenbank-Servers in ein Sicherheitsgateway	ja	
Integration eines DNS-Servers in ein Sicherheitsgateway	ja	
Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway	ja	
Notfallvorsorge bei Sicherheitsgateways	ja	

WLAN		Baustein WLAN: von 9 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 0x entfällt
Maßnahmen	**erfüllt?**	**Bemerkungen**
Geeignete Aufstellung von Access Points	entfällt	
Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung	entfällt	
Auswahl eines geeigneten WLAN-Standards	entfällt	
Auswahl geeigneter Kryptoverfahren für WLAN	entfällt	
Geeignetes WLAN-Schlüsselmanagement	entfällt	
Schulung zum sicheren WLAN-Einsatz	entfällt	
Sichere Konfiguration der Access Points	entfällt	
Sichere Konfiguration der WLAN-Clients	entfällt	
Regelmäßige Sicherheitschecks in WLANs	entfällt	

Fragenkreis: Technische Ausstattung der Arbeitsplätze

Notebooks		Baustein Notebooks: von 9 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 0x entfällt
Maßnahmen	**erfüllt?**	**Bemerkungen**
Existiert bei Notebooks Homogenität?	ja	
Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz	ja	
Einsatz von Diebstahl-Sicherungen	nein	
Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung	nein	Empfehlung: Aufnahme in die neue Dienstanweisung
Regelmäßiger Einsatz eines Anti-Viren-Programms	ja	
Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme	ja	
Sichere Kommunikation von unterwegs	ja	VPN-Client
Sicherer Anschluss von Notebooks an lokale Netze	ja	
Datensicherung bei mobiler Nutzung des IT-Systems	ja	keine lokale Datenhaltung

Allgemeiner Client		Baustein Allgemeiner Client: von 14 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 0x entfällt
Maßnahmen	**erfüllt?**	**Bemerkungen**
Existiert ein homogenes Umfeld bei den Client PC? Hardware	ja	
Existiert ein homogenes Umfeld bei den Client PC? Software	ja	
Austauschzyklen	entfällt	
Wie alt sind die Geräte?		max. 5 Jahre
Wird ein Systemmanagement eingesetzt?	ja	
Wird Remote Desktop genutzt?	ja	
Herausgabe einer PC-Richtlinie	teilw.	teilweise in alter TUI-Dienstanweisung geregelt; Empfehlung: Überarbeitung
Dokumentation der Systemkonfiguration	ja	
Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	ja	
Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz	nein	
Geregelte Außerbetriebnahme eines Clients	teilw.	keine Dokumentation
Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung	teilw.	teilweise in alter TUI-Dienstanweisung geregelt; Empfehlung: Überarbeitung
Regelmäßiger Einsatz eines Anti-Viren-Programms	ja	
Einrichten einer Referenzinstallation für Clients	ja	
Regelmäßige Datensicherung	ja	

Fragenkreis: IT-Management

Sicherheitsmanagement

Baustein Sicherheitsmanagement:
von 8 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Erstellung einer Leitlinie zur Informationssicherheit	nein	
Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	teilw.	Zusammenarbeit Orga-Stelle und IT mit zukünftiger Ausrichtung auch hinsichtlich IT-Sicherheit
Erstellung eines Sicherheitskonzepts	nein	Empfehlung: den örtlichen Gegebenheiten und der Größenordnung angepasstes Sicherheitskonzept entwickeln
Management-Berichte zur Informationssicherheit	teilw.	Empfehlung: Ergänzung des Berichtswesens um regelmäßige Beschreibung von Sicherheitsvorfällen, Lösungen, Information über entstandene Kosten
Dokumentation des Sicherheitsprozesses	nein	
Festlegung der Sicherheitsziele und -strategie	nein	
Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	nein	
Erstellung von zielgruppengerechten Sicherheitsrichtlinien	nein	

Sicherheitsorganisation

Baustein Sicherheitsorganisation:
von 7 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz	ja	TUI-Dienstanweisung vom 05.07.2000 Ziffer 2.1; Empfehlung: Aktualisierung der Dienstanweisung
Vergabe von Zutrittsberechtigungen	ja	
Vergabe von Zugangsberechtigungen	nein	Empfehlung: Einrichtung eines dokumentierten Workflows
Vergabe von Zugriffsrechten	nein	s. o.
Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln	teilw.	physische Zerstörung, jedoch keine Dokumentation
Schlüsselverwaltung	ja	Zahlenschloss
Kontrollgänge	ja	

Sicherheit Personal

Baustein Sicherheit Personal:
von 8 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Geregelte Einarbeitung/Einweisung neuer Mitarbeiter	ja	
Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen	ja	
Schulung vor Programmnutzung	ja	
Schulung zu IT-Sicherheitsmaßnahmen	ja	
Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern	nein	Empfehlung: Einrichtung eines dokumentierten Workflows
Schulung des Wartungs- und Administrationspersonals	ja	
Personaleinsatz und -qualifizierung	ja	
Vertraulichkeitsvereinbarungen	ja	

Datenerhebung (Checkliste) zur Prüfung der IT-Sicherheit - Blatt 5

Notfallvorsorgekonzept		Baustein Notfallvorsorgekonzept: von 15 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 0x entfällt
Maßnahmen	**erfüllt?**	**Bemerkungen**
Erstellung einer Übersicht über Verfügbarkeitsanforderungen	**teilw.**	
Notfall-Definition, Notfall-Verantwortlicher	**nein**	Empfehlung: schriftliche Dokumentation der Verantwortlichkeit
Erstellung eines Notfall-Handbuches	**nein**	
Dokumentation der Kapazitätsanforderungen der IT-Anwendungen	**ja**	
Definition des eingeschränkten IT-Betriebs	**nein**	Empfehlung: Festlegung und Abstimmung innerhalb des Hauses im Notfallhandbuch
Untersuchung interner und externer Ausweichmöglichkeiten	**nein**	Empfehlung: Festlegung und Abstimmung innerhalb des Hauses im Notfallhandbuch
Regelung der Verantwortung im Notfall	**nein**	s. o.
Alarmierungsplan	**ja**	
Notfall-Pläne für ausgewählte Schadensereignisse	**nein**	
Erstellung eines Wiederanlaufplans	**nein**	Empfehlung: Dokumentation im Notfallhandbuch
Durchführung von Notfallübungen	**ja**	
Erstellung eines Datensicherungsplans	**ja**	
Ersatzbeschaffungsplan	**ja**	
Abschließen von Versicherungen	**ja**	
Redundante Kommunikationsverbindungen	**ja**	

Hard- und Softwaremanagement		Baustein Hard- und Softwaremanagement: von 9 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 0x entfällt
Maßnahmen	**erfüllt?**	**Bemerkungen**
Regelung des Passwortgebrauchs	**teilw.**	TUI-Dienstanweisung vom 05.07.2000 Ziffer 2.3; Empfehlung: Aktualisierung der Dienstanweisung
Hinterlegen des Passwortes	**ja**	
Dokumentation der Systemkonfiguration	**ja**	
Regelung für die Einrichtung von Benutzern / Benutzergruppen	**teilw.**	AD sowie DMS-System (Arbeitsgruppen)
Dokumentation der zugelassenen Benutzer und Rechteprofile	**ja**	AD sowie DMS-System (Arbeitsgruppen)
Dokumentation der Veränderungen an einem bestehenden System	**ja**	
Informationsbeschaffung über Sicherheitslücken des Systems	**ja**	
Software-Abnahme- und Freigabe-Verfahren	**ja**	
Kontrolle der Protokolldateien	**ja**	

Virenschutz		Baustein Virenschutz: von 4 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 0x entfällt
Maßnahmen	**erfüllt?**	**Bemerkungen**
Erstellung eines Computer-Virenschutzkonzepts	**teilw.**	
Aktualisierung der eingesetzten Computer-Viren-Suchprogramme	**ja**	
Regelmäßiger Einsatz eines Anti-Viren-Programms	**ja**	
Verhaltensregeln bei Auftreten eines Computer-Virus	**nein**	Empfehlung: Aufnahme in die neue Dienstanweisung

Fragenkreis: Backup und Archivierung

Datensicherung

Baustein Datensicherung:
von 9 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Verpflichtung der Mitarbeiter zur Datensicherung	**ja**	Sicherung nur im Netz
Beschaffung eines geeigneten Datensicherungssystems	**ja**	
Geeignete Aufbewahrung der Backup-Datenträger	**ja**	Aufbewahrung in einem Schließfach bei der Sparkasse
Sicherungskopie der eingesetzten Software	**entfällt**	
Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen	**ja**	
Regelmäßige Datensicherung	**ja**	
Entwicklung eines Datensicherungskonzepts	**ja**	
Dokumentation der Datensicherung	**ja**	
Übungen zur Datenrekonstruktion	**ja**	