Beratung · Prüfung · Service

Überörtliche Prüfung Informationstechnologie der Stadt Billerbeck vom 14.04. bis 07.06.2011

GPA NRW

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

Inhaltsverzeichnis

Zur GPA NRW und zur Prüfung

Prüfungsgrundlagen und Rahmenbedingungen

Wir führen die überörtliche Prüfung auf der Grundlage des § 105 der Gemeindeordnung NRW (GO NRW) durch. Dieser eröffnet die Möglichkeit, die Wirtschaftlichkeit und Sachgerechtigkeit auch vergleichend in den Blick zu nehmen.

Basis unserer Prüfung ist ein Leitfaden, der sich an aktuellen Fragestellungen orientiert und kontinuierlich weiter entwickelt wird. Hierdurch sichern wir die Qualität der Prüfungsinhalte und gewährleisten einheitliche Methoden und Maßstäbe.

Auch die Fachprüfung der IT bei den kleinen kreisangehörigen Städten und Gemeinden findet im Kontext der schwierigen Finanzlage der Gebietskörperschaften statt. Sie ist Teil einer flächendeckenden Prüfung der kommunalen IT-Strukturen, die wir in einem ersten Durchgang bis Ende 2012 abgeschlossen haben werden.

Nach unseren bisherigen Schätzungen werden in den kommunalen Körperschaften in NRW mehr als 500 Millionen Euro pro Jahr für den Einsatz von Informations- und Telekommunikationstechnologien aufgewendet. Bürger, Politik und Verwaltungsleitung erwarten gerade vom IT-Service als Betriebsaufgabe in Zeiten der Haushaltskonsolidierung zu Recht besondere Beiträge in Richtung Sparsamkeit und Wirtschaftlichkeit. Unsere Prüfung zeigt auf, ob hier Potenziale bestehen. Gleichzeitig wollen wir aber auch das Bewusstsein für Folgendes schärfen:

- Die Bedeutung der Informationstechnologie 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.

Methodik und Berichtsaufbau

Unser Prüfungsprozess vollzieht sich generell in drei Schritten:

- Schritt 1: Erfassung der Ist-Situation
- Schritt 2: Analyse
- Schritt 3: Ausarbeitung von Feststellungen und Empfehlungen.

Unsere grundsätzliche Zielsetzung ist es, die IT in den nordrhein-westfälischen Städten, Gemeinden und sonstigen Gebietskörperschaften nicht nur in Bezug auf ihr jeweiliges Aufwandsniveau zu vergleichen, sondern deren Wirtschaftlichkeit im engeren Sinne - d.h. als Verhältnis von Input und Output, von Aufwand und Nutzen, von Kosten und Leistungen - zu betrachten und zu bewerten.

Im Prüfbericht heben wir bestimmte Kernaussagen in Form einer **Feststellung** hervor. Diese Feststellungen können je nach Sachverhalt positive oder negative Wertaussagen enthalten. Zu negativen Feststellungen ist eine Stellungnahme der Kommune nur dann erforderlich, wenn im Bericht ausdrücklich darum gebeten wird.

Auf der Grundlage der Untersuchungen erkannte Verbesserungspotenziale werden als **Empfehlung** ausgewiesen.

Prüfung ist auch ein kommunikativer Vorgang. So werden viele Sachverhalte bereits im Verlauf der Prüfung mündlich erörtert und Probleme ausgeräumt. Im Textteil dieses Prüfberichts finden sich daher nur die wesentlichen Informationen wieder; die maßgeblichen Einzelheiten zu den im Rahmen der Prüfung gewonnenen Erkenntnissen sind dokumentiert und grafisch aufbereitet.

Informationen zum Prüfungsablauf

Wir haben die Prüfung in der Stadt Billerbeck vom 14.04. bis 07.06.2011 durchgeführt.

Die Mitarbeiter der IT haben an der Prüfung aktiv mitgewirkt. Anregungen im Verlauf der Prüfung haben wir gerne für zukünftige Prüfungen übernommen.

Geprüft hat: Marcus Meyer-Meiners

Wir haben das Prüfungsergebnis im Rahmen eines Abschlussgesprächs erörtert. Zur Durchsicht und inhaltlichen Überprüfung wurde vor der endgültigen Berichtsfassung ein Entwurf des Prüfberichts übersandt.

Ergebnisse der Prüfung

Ausgangslage in Billerbeck

Die Stadt Billerbeck fällt in die Größenklasse der kleinen kreisangehörigen Kommunen; zum Stichtag 31.12.2009 hatte die Gemeinde 11.547 Einwohner.

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

Die zentrale Bereitstellung und Betreuung der IT ist in Billerbeck aufbauorganisatorisch als „EDV-Systemadministration" dem Fachbereich Zentrale Dienste und Ordnung zugeordnet.

Die Stadt Billerbeck betreibt ihre IT autonom in eigener Verantwortung und ohne Anbindung an ein kommunales Rechenzentrum.

Gesamtergebnis

Das Gesamtergebnis der geprüften Stadt Billerbeck bilden wir nachfolgend in einer vergleichenden Matrixdarstellung ab.

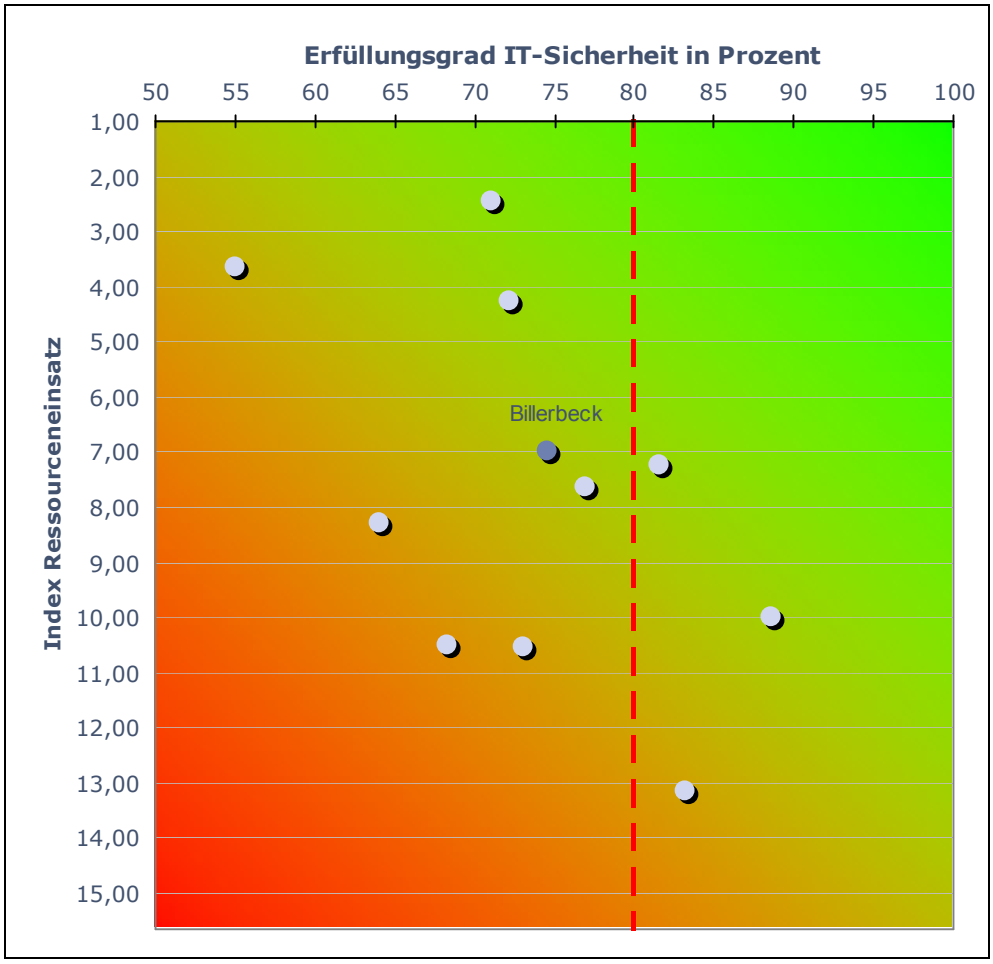
Ziel dieser Matrix ist die Darstellung des Verhältnisses zwischen eingesetzten Ressourcen und dem Erfüllungsgrad im Bereich der IT-Sicherheit im interkommunalen Vergleich. Auch versuchen wir über die Matrixdarstellung aufzuzeigen, ggf. in welchem Bereich (Ressourceneinsatz oder IT-Sicherheit) der größere Handlungsbedarf besteht.

Dazu wird auf der X-Achse der erreichte Grad der IT-Sicherheit abgebildet. Vor dem Hintergrund der Anforderungen des BSI-Grundschutzhandbuchs erscheint ein Erfüllungsgrad bei der IT-Sicherheit von mindestens 80 Prozent erstrebenswert. Zur Bestimmung der Positionierung auf der Y-Achse wurden u. a. die im Abschnitt „IT-Aufwendungen" behandelten Berichtskennzahlen gewichtet und der so ermittelte Gesamtrang der geprüften Verwaltung in den interkommunalen Vergleich eingestellt.

Allerdings lässt sich keine Aussage darüber treffen, ob die Aufgabe, ordnungsgemäß und sachgerecht IT für die Verwaltung der Stadt Billerbeck bereitzustellen und zu betreuen, mit dem geringst möglichen Mitteleinsatz erfüllt wird.

Dennoch liefert das Ergebnis der betrachteten Stadt oder Gemeinde zusammen mit den weiteren, anonymisierten Ergebnissen des aktuellen Vergleichs ein Abbild der kommunalen IT-Landschaft in Nordrhein-Westfalen.

Gesamtergebnis in Matrixdarstellung



Hinsichtlich der Betrachtung der IT-Aufwendungen nimmt die Stadt Billerbeck im interkommunalen Vergleich eine Position im oberen Mittelfeld ein.

Die Aufwendungen je Arbeitsplatz mit IT-Ausstattung betragen 3.304 Euro. Billerbeck liegt damit auf Höhe des derzeitigen Mittelwertes. Hinsichtlich der IT-Aufwendungen je Einwohner erreicht die Stadt Billerbeck

einen Wert von 14,13 Euro und liegt damit 3,58 Euro je Einwohner unter dem arithmetischen Mittel der geprüften kleinen kreisangehörigen Kommunen.

Die Betreuungsquote bewegt sich mit 41 zu betreuenden Arbeitsplätzen mit IT-Ausstattung rein rechnerisch unter dem bisherigen interkommunalen Mittelwert (70 zu betreuende Arbeitsplätze mit IT-Ausstattung je Vollzeitstelle).

Die Stadt Billerbeck betreibt ihre IT-Infrastruktur vollständig autark. Sie hostet alle betriebskritischen Applikationen selber und administriert auch das Sicherheitsgateway eigenverantwortlich. In diesem Zusammenhang ist auch die Betreuungsquote zu bewerten, die wir als durchaus nachvollziehbar erachten.

Der Ressourceneinsatz fällt, wie dargestellt, leicht unterdurchschnittlich aus. Im Bereich der IT-Sicherheit bleibt der Erfüllungsgrad unter 80 Prozent, dennoch erreicht die Gemeinde im Vergleich ein noch akzeptables Niveau. Optimierungsbedarf haben wir zunächst einmal hinsichtlich der Räumlichkeiten zur Unterbringung der technischen Infrastruktur, überwiegend aber in solchen Teilbereichen festgestellt, in denen organisatorische Regelungen und Maßnahmen mit relativ geringem Aufwand bereits zu einer erkennbaren Verbesserung führen können.

Ressourceneinsatz

Grundlagen der Datenerhebung

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. Vor dem Hintergrund des Systemwechsels im kommunalen Rechnungswesen werden wir in Anlehnung an die Begrifflichkeiten des NKF in der Kennzahlenbildung im Bericht einheitlich von Aufwendungen sprechen, obwohl auch Ausgaben und Kostengrößen einfließen. Die in der betriebswirtschaftlichen Terminologie klare Trennung von Ausgaben, Aufwand und Kosten wird damit zugunsten einer pragmatischen Lösung teilweise aufgehoben.

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

Als Datengrundlage zur Ermittlung der Sachaufwendungen ziehen wir die Ergebnisse der Haushaltsrechnungen bzw. Jahresabschlüsse aus dem Betrachtungszeitraum 2006 bis 2009 heran. Daraus extrahieren wir die Wertgrößen, die unmittelbaren Bezug zur IT haben.

Soweit für einzelne Jahre ein vollständiger bzw. testierter Jahresabschluss noch nicht vorliegt, greifen wir auf vorläufige Ergebnisse oder auf Daten aus der internen Kostenrechnung zurück. Für die Haushaltsjahre, in denen noch nach kameralen Grundsätzen gebucht worden war, erreichen wir mit Hilfsrechnungen Werte, die weitgehende Analogie zur Ergebnisrechnung des NKF aufweisen.

Personalaufwendungen und Stellenausstattung

Zur Ermittlung des Personalaufwands im IT-Bereich sowie zur Betrachtung der Stellenausstattung haben wir einen zweistufigen Ansatz gewählt:

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.

Mit klaren Definitionen und Abgrenzungskriterien tragen wir also den unterschiedlichen Organisationskonzepten in den verglichenen Kommunen Rechnung. Im Ergebnis stehen damit folgende Informationen zur Verfügung:

- Die Anzahl der vollzeitverrechneten Stellen innerhalb der Organisationseinheit „zentrale IT".

- Die Anzahl der vollzeitverrechneten Stellen, die auf die Erfüllung der von uns definierten originären IT-Aufgaben entfallen, und zwar unabhängig von der aufbauorganisatorischen Zuordnung.

- Die Anzahl der vollzeitverrechneten Stellen, 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 unter Berücksichtigung der tatsächlichen Besoldungs- bzw. Entgeltgruppen der jeweiligen Mitarbeiter auf Basis der entsprechenden KGSt-Durchschnittswerte; diese Werte werden in der Regel jährlich ermittelt und in den KGSt-Berichten "Kosten eines Arbeitsplatzes" veröffentlicht. Damit blenden wir in der Kostenbetrachtung Unterschiede in der Personalstruktur der geprüften Kommunen bewusst aus; individuelle Personalkostenfaktoren wie etwa Dienstaltersstufen und Zuschläge sollen im Rahmen des interkommunalen Vergleichs ausdrücklich nicht einbezogen werden.

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 entsprechende KGSt-Gutachten folgende Zuschläge: Auf jede vollzeitverrechnete Stelle eine Sachkostenpauschale für Büroarbeitsplätze in Höhe von 5.400 Euro und auf die ermittelten Personalaufwendungen jeweils 10 Prozent für allgemeine (verwaltungsweite) Leistungen sowie für amts- bzw. fachbereichsinterne Leitungsaufgaben, insgesamt also einen Zuschlag für „Overhead"-Gemeinkosten in Höhe von 20 Prozent.

Ergebnisse im interkommunalen Kennzahlenvergleich

Um eine Verzerrung und überproportionale Einflussnahme durch Schwankungen oder zufällig im Vergleichsjahr entstandene einmalige Kosten zu verhindern, fließt grundsätzlich das arithmetische Mittel aus dem vierjährigen Betrachtungszeitraum in die Kennzahlenbildung ein. Die Personalaufwendungen werden dagegen für das aktuellste Betrachtungsjahr ermittelt und um eine Sachkostenpauschale sowie Gemeinkostenzuschläge ergänzt.

Grunddaten zur Kennzahlenbildung (Aufwendungen in Euro)	
IT-Sachaufwendungen (arithmetisches Mittel 4 Jahre)	67.243
Personalaufwendungen für originäre IT-Aufgaben (ermittelt nach KGSt-Pauschalen)	74.521
Sachkostenpauschale und Gemeinkostenzuschlag nach KGSt-Empfehlung	21.762
Gesamtaufwendungen IT	**163.526**

Zunächst stellen wir im Rahmen des interkommunalen Vergleichs den Einwohnerbezug in den Mittelpunkt. Die Einwohner einer Kommune sind die eigentlichen Adressaten der kommunalen Leistungserbringung. Damit sind sie letztendlich auch dann die maßgebliche Bezugsgröße, wenn es um die Abbildung interner, der Erstellung der kommunalen Endpro-

dukte vorgelagerter Leistungen – wie auch der Informationstechnologie - geht.

Hinsichtlich der IT-Aufwendungen je Einwohner erreicht die Stadt Billerbeck einen Wert von 14,13 Euro und liegt damit 3,58 Euro je Einwohner unter dem arithmetischen Mittel der geprüften kleinen kreisangehörigen Kommunen.

Neben der Kennzahl mit Einwohnerbezug nehmen wir auch die Betrachtung der IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung in den Blick. Die daraus generierte Kennzahl liefert wichtige Informationen für Analysen im Rahmen interner Steuerungsprozesse.

Die Aufwendungen je Arbeitsplatz mit IT-Ausstattung betragen 3.304 Euro. Billerbeck liegt damit auf der Höhe des derzeitigen interkommunalen Mittelwertes (3.306 Euro je Bildschirmarbeitsplatz).

Dass das Resultat beim Arbeitsplatzbezug etwas ungünstiger ausfällt, ist darin begründet, dass Billerbeck im Verhältnis zur Einwohnerzahl weniger Bildschirmarbeitsplätze einsetzt als der Durchschnitt der Vergleichsgemeinden. Hochgerechnet auf 1.000 Einwohner stellt die Stadt Billerbeck lediglich 4,28 Arbeitsplätze mit IT-Ausstattung zur Verfügung und stellt damit im derzeitigen interkommunalen Vergleich den Minimumwert. Durchschnittlich weisen die Vergleichskommunen bezogen auf 1.000 Einwohner 5,34 Arbeitsplätze mit IT-Ausstattung aus; durch die Nutzung von Desksharing hat die Stadt Billerbeck die Zahl der Bildschirmarbeitsplätze reduzieren können.

Dies bedeutet jedoch auch, dass die Position im interkommunalen Vergleich durch eine – bezogen auf die Einwohner - niedrige Anzahl von Bildschirmarbeitsplätzen negativ beeinflusst wird, weil die IT-Aufwendungen auf eine kleinere Verteilungsmenge verrechnet werden.

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

Feststellung

Die IT-Aufwendungen liegen sowohl im Einwohnerbezug Ausstattung interkommunal unter dem Mittelwert. In Bezug auf die Arbeitsplätze mit IT-Ausstattung liegt die Stadt auf Höhe des aktu-

ellen Mittelwertes.

Zwar weisen einige Vergleichskommunen erkennbar niedrigere IT-Gesamtaufwendungen auf; belastbare Anhaltspunkte dafür, dass der Ressourceneinsatz in der IT der Stadt Billerbeck ohne gleichzeitigen Einfluss auf das Leistungsniveau nennenswert verringert werden kann, haben sich im Rahmen der Prüfung jedoch nicht ergeben.

Empfehlung

Personal- und Sachressourcen sollten stets im Kontext der Wirtschaftlichkeit eingesetzt werden. In diesem Zusammenhang sollten Beschaffungsvorhaben und Verfahrenseinsätze weiterhin unter dem Blickwinkel von Wirtschaftlichkeitsanalysen und möglichen interkommunalen Zusammenarbeiten betrachtet werden.

Finanzwirtschaftliche Steuerung im IT-Bereich

Damit eine Verwaltung ihre Aufgaben unter wirtschaftlichen Gesichtspunkten sachgerecht und zweckmäßig erfüllen kann, ist neben inhaltlicher Qualität eine wirksame Finanzsteuerung unerlässlich. Unabdingbare Voraussetzung für eine funktionierende Steuerung auf der finanzwirtschaftlichen Ebene ist wiederum, dass die Kommune ihre spezifischen Kostenstrukturen kennt. Dies gilt naturgemäß auch für die Aufgabe IT. Dazu lassen sich drei elementare Kernfragen formulieren:

- Verfügt die Stadt Billerbeck 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 Stadt Billerbeck 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.

Im Rahmen der Prüfung sind uns die angeforderten Unterlagen und Informationen zeitnah und in nachvollziehbar aufbereiteter Form zur Verfügung gestellt worden. Gleichwohl ist der Eindruck entstanden, dass eine jederzeitige, auf einem sinnvoll konzipierten Controlling-System basierende Bereitstellung von Informationen in dem für interne Steuerungszwecke sinnvollen und wünschenswerten Umfang nur eingeschränkt möglich ist.

Damit echte finanzwirtschaftliche Steuerungsmöglichkeiten im IT-Bereich umgesetzt werden können, ist eine hohe Qualität der relevanten Informationen erforderlich.

Nach Umstellung des kommunalen Haushaltes auf die Systematik des Neuen Kommunalen Finanzmanagements (NKF) zum Jahre 2009 wurde ein Produkt „Organisation / EDV“ (01100) gebildet, eine Ausgestaltung im Hinblick auf konkrete Steuerungsfunktionen steht aber noch aus.

Dazu ist unter anderem die Definition von Zielen erforderlich, deren Erfüllungsgrad messbar sein muss. Zur Messbarkeit bzw. Darstellung des Zielerreichungsgrades sollten entsprechende Kennzahlen gebildet werden.

So ließe sich beispielsweise unter Einbeziehung individueller Anforderungen in der Kommune das Ziel „wirtschaftlicher Einsatz von Hard- und Software" definieren, anhand von Kennzahlen messen und fortschreiben.

Als Grundlage bieten sich z.B. die im vorliegenden Bericht verwendeten Kennzahlen für den interkommunalen Vergleich an.

Feststellung

Die Stadt Billerbeck hat die grundsätzlichen Voraussetzungen für eine Produktsteuerung im Bereich der IT geschaffen.

Empfehlung

Wir empfehlen die Einbeziehung von Kennzahlen in die Produktsteuerung.

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 gesetzlichen Vertreter der Körperschaften sind hier für die Einhaltung der Sicherheit der IT-Systeme und deren relevanten Daten in erster Linie verantwortlich.

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 ein Mindestmaß an Anforderungen erfüllt ist, um einen ordnungsgemäßen und nachhaltigen IT-Betrieb zu gewährleisten. Das Maß der erfüllten Anforderungen im Sinne eines Grundschutzes wird, unter Einbeziehung der Sicherheitscheckliste, im Rahmen der Darstellung eines Erfüllungsgrades zum Ausdruck gebracht. Dabei wird der jeweilige erreichte Erfüllungsgrad in einen interkommunalen Vergleich gestellt, um einerseits eine Positionsbestimmung für die jeweilige geprüfte Kommune zu ermöglichen, und andererseits einen Überblick über die Standards zu erhalten, den die Kommunen diesbezüglich bereits erreicht haben. Es geht jedoch nicht darum, ein Szenario zu beschreiben, welche Maßnahmen möglich sind. Dies ist vielmehr eine Entscheidung der jeweiligen Organisation, mit welchen Mitteln das Mindestmaß an Sicherheitsanforderungen erreicht werden soll.

Die Betrachtung ist in folgende Fragenkreise untergliedert:

- IT-Räume und IT-Infrastrukturaufbau
- Technische Ausstattung der Arbeitsplätze
- IT-Management (Konzepte, Dienstanweisungen und Risikomanagement)
- Backup und Archivierung.

Die Prüfung ist durch die Verwendung von Checklisten systematisiert. Diese Checklisten werden gemeinsam mit den IT-Verantwortlichen vor Ort im Rahmen eines Interviews besprochen. Im Rahmen des Prüfungsumfanges ist nicht vorgesehen, die 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.

Mit den umgesetzten Maßnahmen zur IT-Sicherheit nimmt die Stadt Billerbeck im Vergleich der kleinen kreisangehörigen Kommunen eine Position im oberen Mittelfeld ein. Der mit dieser Prüfung festgestellte Gesamterfüllungsgrad beträgt für Billerbeck 74,6 Prozent, der Mittelwert liegt derzeit ebenfalls bei 73,5 Prozent.

Diese festgestellte Positionierung auf Höhe des interkommunalen Mittelwertes darf nicht darüber hinwegtäuschen, dass in einigen Bereichen Risiken bestehen bzw. der Sicherheitsstandard durch Maßnahmen gesteigert werden kann und auch werden sollte.

Angestrebtes Ziel sollte ein Erfüllungsgrad von mindestens 80 Prozent sein. 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

In nachstehenden Teilbereichen haben wir nennenswerte Defizite und daraus resultierende Optimierungspotenziale ermittelt und entsprechende Empfehlungen formuliert.

Fragenkreis „IT-Räume und Infrastrukturaufbau"

Serverraum

Im Serverraum haben wir Brandlasten vorgefunden (Papier, Kartonage). Sicherheitstüren, die über eine Einbruchs- und Brandschutzzertifizierung verfügen, sind nicht verbaut. Eine Gefahrenmeldeanlage wird nicht betrieben. Die Klimatisierung ist nicht redundant ausgelegt.

> **Empfehlung**
>
> Wir empfehlen,
>
> - die Brandlasten zu entfernen,
> - den Einbau von Sicherheitstüren zu prüfen,
> - die Installation eines geeigneten Gefahrenmeldesystems in Erwägung zu ziehen und
> - eine redundante Auslegung der Klimatisierung zu prüfen.

Fragenkreis „IT-Management"

Sicherheitsmanagement

Die Stadt Billerbeck verfügt über keine konzeptionellen Vorgaben zur IT-Sicherheit. Es gibt weder eine IT-Sicherheitsleitlinie noch ein IT-Sicherheitskonzept; teilweise finden sich Regelungen in Hausverfügungen, die jedoch schon bis zu zehn Jahre alt sind und nicht mehr den aktuellen Gegebenheiten entsprechen.

Empfehlung

Neben einer grundsätzlichen Leitlinie zur Informationssicherheit empfehlen wir, ein IT-Sicherheitskonzept nach den Vorgaben des Grundschutzhandbuchs des BSI zu erstellen.

Notfallvorsorge

Die Notfallvorsorge umfasst Maßnahmen, die auf die Wiederherstellung der Betriebsfähigkeit nach (technisch bedingtem bzw. durch fahrlässige oder vorsätzliche Handlungen herbeigeführtem) Ausfall eines IT-Systems ausgerichtet sind. Es ist sinnvoll, den hierzu bestimmbaren Maßnahmenkatalog im Rahmen eines Konzeptes zu definieren und damit verbindlich festzulegen.

Im Rahmen der Prüfung haben wir festgestellt, dass die Stadt Billerbeck über wesentliche Bausteine der Notfallvorsorge nicht verfügt.

Empfehlung

Es sollte ein Notfallvorsorgekonzept bzw. ein Notfallhandbuch nach BSI-Standard für die IT erstellt werden.

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 der Prüfung sind nicht eventuelle Verstöße gegen die materiell-rechtlichen Bestimmungen des Datenschutzes. Allerdings vertreten wir die Auffassung, dass mit dem formalen Akt der Bestellung 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 und stellt eine wesentliche Voraussetzung für die Erfüllung des öffentlichen Auskunftsanspruchs dar.

Feststellung

Die Funktion des Datenschutzbeauftragten ist in der Stadt Billerbeck ordnungsgemäß personell besetzt. Allerdings ist der in § 32a Abs. 1 Satz 1 DSG NRW explizit vorgeschriebene Vertreter des Datenschutzbeauftragten nicht bestellt.

Von der Stadt Billerbeck konnte in der Prüfung ein ordnungsgemäß geführtes Verfahrensverzeichnis nicht vorgelegt werden.

Empfehlung

Die Bestellung eines stellvertretenden Datenschutzbeauftragten sollte zeitnah nachgeholt werden.

Mit der Erstellung eines Verzeichnisses, das die in § 8 DSG NRW vorgeschriebenen Angaben zu den eingesetzten Datenverarbeitungsverfahren enthält, sollte fortgesetzt werden.

Herne, den 07.06.2011

Michael Kuzniarek
Abteilungsleitung

Ulrich Sdunek
Projektleitung

Anlage 7: Datenerhebung (Checkliste) zur Prüfung der IT-Sicherheit - Blatt 1

GPA NRW

Überörtliche Prüfung Informationstechnologie
- Erhebungsbogen IT-Sicherheit -

Name der Körperschaft:
Stadt Billerbeck

Gesprächstermin:
14.04.2011

Prüfer:
3M

Gesprächspartner in der Kommune:
Herr Dierksmeier

Fragenkreis: IT-Räume und Infrastrukturaufbau

Serverraum

Baustein Serverraum:
von 21 Maßnahmen 10x JA, 10x NEIN, 1x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Angepasste Aufteilung der Stromkreise	ja	
Handfeuerlöscher	ja	
Verwendung von Sicherheitstüren und -fenstern	nein	Holztüren (Innenbereich) Empfehlung: Prüfung der Verwendung von Sicherheitstüren entsprechend dem BSI Grundschutzhandbuch
Geschlossene Fenster	ja	
Gefahrenmeldeanlage/Brandmelder	nein	Empfehlung: Prüfung der Installation geeigneter Gefahrenmelder für u. a. Einbruch, Brand, Wasser, Rauch etc. mit Aufschaltung der Alarmmeldung
Abgeschlossene Türen	ja	
Vermeidung von Risiken durch wasserführende Leitungen	nein	Heizung vorhanden Empfehlung: Prüfung von Maßnahmen zur Schadensvermeidung z. B. Ableitbleche, wasserdichte Ummantelung o. ä. im Sinne des BSI
Überspannungsschutz	ja	2 USV
Not-Aus-Schalter	nein	aber: Hauptsicherung der Unterverteilung im Serverraum
Klimatisierung	teilw.	
Lokale unterbrechungsfreie Stromversorgung	ja	Selbsttest (Meldung per Mail)
Fernanzeige von Störungen	nein	Angedacht: NetBots Empfehlung: Prüfung der Realisierbarkeit

Redundanzen in der technischen Infrastruktur (ohne Storage)	ja	keine Ersatzteile, aber: 3 X "Next Business Day"
Technische und organisatorische Vorgaben für Serverräume	nein	Serverraum aus baulichen Gegebenheiten heraus entstanden
Brandschutz von Patchfeldern	nein	Empfehlung: Prüfung der räumlichen Gegebenheiten durch einen Brandschutzbeauftragten
Zutrittsregelung und -kontrolle	ja	durch Schlüsselgewalt ausschließlich beim Admin.
Rauchverbot	ja	
Verwendung von hochverfügbaren Architekturen	nein	ein HyperV im Einsatz, geplant: zweiter HyperV und SAN (Haushaltsabhängig)
Zentrales Speichersystem vorhanden	nein	
Storage System redundant	nein	
Einsatz von Servervirtualisierung	ja	1 Hyper V
IT-Verkabelung		**Baustein IT-Verkabelung: von 12 Maßnahmen 11x JA, 1x NEIN, 0x teilweise, 0x entfällt**
Maßnahmen	**erfüllt?**	**Bemerkungen**
Verkabelungsart den technischen Anforderungen entsprechend	ja	
Netz-Topologie	ja	sternförmig, keine Unterverteilung
Erneuerung der IT-Verkabelung	ja	2001
Redundanzen für die Primärverkabelung	ja	
Redundanzen für die Gebäudeverkabelung	ja	
Brandabschottung von Trassen	nein	Empfehlung: Prüfung der räumlichen Gegebenheiten durch einen Brandschutzbeauftragten
Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht	ja	
Ausreichende Trassendimensionierung	ja	
Materielle Sicherung von Leitungen und Verteilern	ja	
Dimensionierung und Nutzung von Schranksystemen	ja	

Neutrale Dokumentation in den Verteilern	ja	im Rack und schriftlich
Laufende Fortschreibung und Revision der Netzdokumentation	ja	halbjährlich fortgeschrieben

Sicherheitsgateway		**Baustein Sicherheitsgateway: von 19 Maßnahmen 14x JA, 1x NEIN, 0x teilweise, 4x 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	DMZ
Content-Filter im Einsatz	ja	
Proxyserver im Einsatz	ja	kein Caching
Gateway redundant	ja	Möglichkeit der Wiederherstellung in einem angemessenen Zeitrahmen möglich
Schulung der Administratoren des Sicherheitsgateways	ja	Watchguard - Zertifizierung, Dipl. Ing. Elektrotechnik FR Prozessinformatik mit MS-Zertifikaten
Protokollierung der Sicherheitsgateway-Aktivitäten	ja	LogIn der Firewall
Integration von Proxyservern in das Sicherheitsgateway	ja	
Integration von VPN-Komponenten in ein Sicherheitsgateway	ja	statische und dynamische Tunnel
Integration von Virenscannern in ein Sicherheitsgateway	ja	
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	entfällt	nur Session; derzeit noch extern gehostet
Integration eines E-Mailservers in ein Sicherheitsgateway	ja	
Integration eines Datenbank-Servers in ein Sicherheitsgateway	entfällt	nur Session; derzeit noch extern gehostet
Integration eines DNS-Servers in ein Sicherheitsgateway	ja	
Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway	entfällt	
Notfallvorsorge bei Sicherheitsgateways	nein	nicht verschriftlicht

WLAN		**Baustein WLAN: von 9 Maßnahmen 7x JA, 2x NEIN, 0x teilweise, 0x entfällt**
Maßnahmen	**erfüllt?**	**Bemerkungen**
Geeignete Aufstellung von Access Points	ja	nur im Serverraum
Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung	nein	Empfehlung: Aufnahme entsprechender Regelungen in umfänglicher IT-Dienstanweisung.
Auswahl eines geeigneten WLAN-Standards	ja	WPA2
Auswahl geeigneter Kryptoverfahren für WLAN	ja	WPA2

Geeignetes WLAN-Schlüsselmanagement	ja	
Schulung zum sicheren WLAN-Einsatz	ja	
Sichere Konfiguration der Access Points	ja	
Sichere Konfiguration der WLAN-Clients	nein	nur über Windows Standardssoftware Empfehlung: Prüfung alternativer Sicherungsschlüssel
Regelmäßige Sicherheitschecks in WLANs	ja	über Firewall

Fragenkreis: Technische Ausstattung der Arbeitsplätze

Notebooks

Baustein Notebooks:
von 9 Maßnahmen 4x JA, 1x NEIN, 0x teilweise, 4x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Existiert bei Notebooks Homogenität?	ja	1 NB, Windows 7
Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz	ja	Tasche
Einsatz von Diebstahl-Sicherungen	entfällt	NB grundsätzlich verschlossen aufbewahrt, keine unbewachte Ausgabe möglich.
Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung	nein	Empfehlung: Aufnahme entsprechender Regelungen in umfänglicher IT-Dienstanweisung.
Regelmäßiger Einsatz eines Anti-Viren-Programms	ja	Symantec
Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme	entfällt	weil nicht lokal gespeichert wird
Sichere Kommunikation von unterwegs	entfällt	
Sicherer Anschluss von Notebooks an lokale Netze	ja	
Datensicherung bei mobiler Nutzung des IT-Systems	entfällt	

Allgemeiner Client

Baustein Allgemeiner Client:
von 14 Maßnahmen 8x JA, 0x NEIN, 4x teilweise, 2x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Existiert ein homogenes Umfeld bei den Client PC? Hardware	ja	XP
Existiert ein homogenes Umfeld bei den Client PC? Software	ja	
Austauschzyklen	entfällt	
Wie alt sind die Geräte?		maximal acht Jahre
Wird ein Systemmanagement eingesetzt?	ja	LogInventory
Wird Remote Desktop genutzt?	teilw.	nur bei Rechnern in Außenbereichen
Herausgabe einer PC-Richtlinie	teilw.	Teilaspekte sind in Hausverfügungen geregelt
Dokumentation der Systemkonfiguration	ja	LogInventory
Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	ja	WSUS
Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz	teilw.	Teilaspekte sind in Hausverfügungen geregelt

Geregelte Außerbetriebnahme eines Clients	ja	mechanische Zerstörung; E-Schrott beim Wertstoffhof
Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung	teilw.	aber: Eingerichtete Gruppenrichtlinie (passwortgeschützter BSS)
Regelmäßiger Einsatz eines Anti-Viren-Programms	ja	
Einrichten einer Referenzinstallation für Clients	ja	
Regelmäßige Datensicherung	entfällt	

Fragenkreis: IT-Management

Sicherheitsmanagement

Baustein Sicherheitsmanagement:
von 8 Maßnahmen 1x JA, 5x NEIN, 2x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Erstellung einer Leitlinie zur Informationssicherheit	teilw.	Teilaspekte sind in Hausverfügungen geregelt
Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	ja	IT-Sicherheitsbeauftragte benannt
Erstellung eines Sicherheitskonzepts	nein	Empfehlung: Aufnahme entsprechender Regelungen in umfänglicher IT-Dienstanweisung.
Management-Berichte zur Informationssicherheit	nein	aber: IT-Sicherheitsbeauftragter infomiert Admin. Empfehlung: Prüfung von Abstimmungsmöglichkeiten auf interkommunaler Ebene
Dokumentation des Sicherheitsprozesses	nein	Empfehlung: Aufnahme entsprechender Regelungen in umfänglicher IT-Dienstanweisung.
Festlegung der Sicherheitsziele und -strategie	nein	Empfehlung: Aufnahme entsprechender Regelungen in umfänglicher IT-Dienstanweisung.
Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	nein	Empfehlung: Aufnahme entsprechender Regelungen in umfänglicher IT-Dienstanweisung.
Erstellung von zielgruppengerechten Sicherheitsrichtlinien	teilw.	nicht verschriftlicht, aber umgesetzt durch tatsächliche Einstellungen

Sicherheitsorganisation

Baustein Sicherheitsorganisation:
von 7 Maßnahmen 6x JA, 0x NEIN, 0x teilweise, 1x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz	ja	Stellenbeschreibung
Vergabe von Zutrittsberechtigungen	ja	
Vergabe von Zugangsberechtigungen	ja	Vergabe durch Admin in Zusammenarbeit mit FB
Vergabe von Zugriffsrechten	ja	Vergabe durch Admin in Zusammenarbeit mit FB
Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln	ja	Entsorgung im E-Schrott

Schlüsselverwaltung	ja	
Kontrollgänge	entfällt	

Sicherheit Personal		**Baustein Sicherheit Personal:** **von 8 Maßnahmen 8x JA, 0x NEIN, 0x teilweise, 0x entfällt**
Maßnahmen	**erfüllt?**	**Bemerkungen**
Geregelte Einarbeitung/Einweisung neuer Mitarbeiter	ja	Ablaufplan liegt vor
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	ja	Ablaufplan liegt vor
Schulung des Wartungs- und Administrationspersonals	ja	nach Bedarf
Personaleinsatz und -qualifizierung	ja	
Vertraulichkeitsvereinbarungen	ja	

Notfallvorsorgekonzept		**Baustein Notfallvorsorgekonzept:** **von 15 Maßnahmen 4x JA, 9x NEIN, 2x teilweise, 0x entfällt**
Maßnahmen	**erfüllt?**	**Bemerkungen**
Erstellung einer Übersicht über Verfügbarkeitsanforderungen	nein	Empfehlung: Festlegung, welche Systeme bzw. Anwendungen nach einem Totalausfall wie schnell wieder verfügbar sein müssen. Aufnahme in ein umfängliches IT-Notfallvorsorgekonzept nach BSI.
Notfall-Definition, Notfall-Verantwortlicher	teilw.	nicht verschriftlicht Empfehlung: Aufnahme in ein umfängliches IT-Notfallvorsorgekonzept nach BSI.
Erstellung eines Notfall-Handbuches	ja	aber: Teilaspekte sind vorhanden
Dokumentation der Kapazitätsanforderungen der IT-Anwendungen	nein	Aufnahme in ein umfängliches IT-Notfallvorsorgekonzept nach BSI.
Definition des eingeschränkten IT-Betriebs	nein	Grundsätzlich sollte definiert sein, welche Verfahren und Dienste im eingeschränkten Betrieb unbedingt zur Verfügung stehen müssen. Empfehlung: Aufnahme in ein umfängliches IT-Notfallvorsorgekonzept nach BSI.
Untersuchung interner und externer Ausweichmöglichkeiten	teilw.	Möglichkeiten bekannt, aber nicht festgelegt Empfehlung: Aufnahme in ein umfängliches IT-Notfallvorsorgekonzept nach BSI.
Regelung der Verantwortung im Notfall	nein	Empfehlung: Aufnahme in ein umfängliches IT-Notfallvorsorgekonzept nach BSI und Festlegung in Dienstanweisung IT.

Alarmierungsplan	nein	Empfehlung: Aufnahme in ein umfängliches IT-Notfallvorsorgekonzept nach BSI.
Notfall-Pläne für ausgewählte Schadensereignisse	nein	Empfehlung: Aufnahme in ein umfängliches IT-Notfallvorsorgekonzept nach BSI; Anlehung an bestehenden Notfallplan für Grossschadensereignisse sinnvoll.
Erstellung eines Wiederanlaufplans	nein	Empfehlung: Aufnahme in ein umfängliches IT-Notfallvorsorgekonzept nach BSI.
Durchführung von Notfallübungen	nein	Empfehlung: Aufnahme in ein umfängliches IT-Notfallvorsorgekonzept nach BSI.
Erstellung eines Datensicherungsplans	ja	Über Definition des BckUp und der Wiederherstellung
Ersatzbeschaffungsplan	nein	Empfehlung: Aufnahme in ein umfängliches IT-Notfallvorsorgekonzept nach BSI.
Abschließen von Versicherungen	ja	
Redundante Kommunikationsverbindungen	ja	
Hard- und Softwaremanagement		**Baustein Hard- und Softwaremanagement: von 9 Maßnahmen 9x JA, 0x NEIN, 0x teilweise, 0x entfällt**
Maßnahmen	**erfüllt?**	**Bemerkungen**
Regelung des Passwortgebrauchs	ja	durch Admin.
Hinterlegen des Passwortes	ja	in verschlüsselter Excel-Tabelle hinterlegt
Dokumentation der Systemkonfiguration	ja	LogInventory
Regelung für die Einrichtung von Benutzern / Benutzergruppen	ja	
Dokumentation der zugelassenen Benutzer und Rechteprofile	ja	
Dokumentation der Veränderungen an einem bestehenden System	ja	LogInventory
Informationsbeschaffung über Sicherheitslücken des Systems	ja	
Software-Abnahme- und Freigabe-Verfahren	ja	
Kontrolle der Protokolldateien	ja	bei der Serverwartung (Serverwartungsplan)
Virenschutz		**Baustein Virenschutz: von 4 Maßnahmen 4x JA, 0x NEIN, 0x teilweise, 0x entfällt**
Maßnahmen	**erfüllt?**	**Bemerkungen**
Erstellung eines Computer-Virenschutzkonzepts	ja	

Aktualisierung der eingesetzten Computer-Viren-Suchprogramme	**ja**	
Regelmäßiger Einsatz eines Anti-Viren-Programms	**ja**	
Verhaltensregeln bei Auftreten eines Computer-Virus	**ja**	

Fragenkreis: Backup und Archivierung

Datensicherung

Baustein Datensicherung:
von 9 Maßnahmen 8x JA, 0x NEIN, 0x teilweise, 1x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Verpflichtung der Mitarbeiter zur Datensicherung	**ja**	
Beschaffung eines geeigneten Datensicherungssystems	**ja**	USB-Festplatten
Geeignete Aufbewahrung der Backup-Datenträger	**ja**	Tresor, Sparkasse
Sicherungskopie der eingesetzten Software	**entfällt**	
Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen	**ja**	Sichern mit Prüflesen
Regelmäßige Datensicherung	**ja**	Tagesvollsicherung, Monatssicherung auf zwei Platten und Jahressicherung auf Bändern
Entwicklung eines Datensicherungskonzepts	**ja**	
Dokumentation der Datensicherung	**ja**	
Übungen zur Datenrekonstruktion	**ja**	