Beratung · Prüfung · Service

GPA NRW

Überörtliche Prüfung
Informationstechnik
der Gemeinde Havixbeck
vom 20.11.2012 bis 23.04.2013

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.

Auch die Fachprüfung der IT 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 Aspekte des In- und Outputs; 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 Ge-

samtbetrachtung der nordrhein-westfälischen IT-Landschaft weiter zu verbessern.

Wir haben die Prüfung in der Gemeinde Havixbeck vom 22.11.2012 bis 23.04.2013 durchgeführt.

Geprüft hat: Marcus Meiners

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 Havixbeck vor der endgültigen Fassung ein Entwurf des Prüfungsberichts übersandt.

Ergebnisse der Prüfung

Ausgangslage in Havixbeck

Die Gemeinde Havixbeck fällt in die Größenklasse der kleinen kreisangehörigen Kommunen; zum Stichtag 31.12.2010 hatte die Gemeinde 11.801 Einwohner.

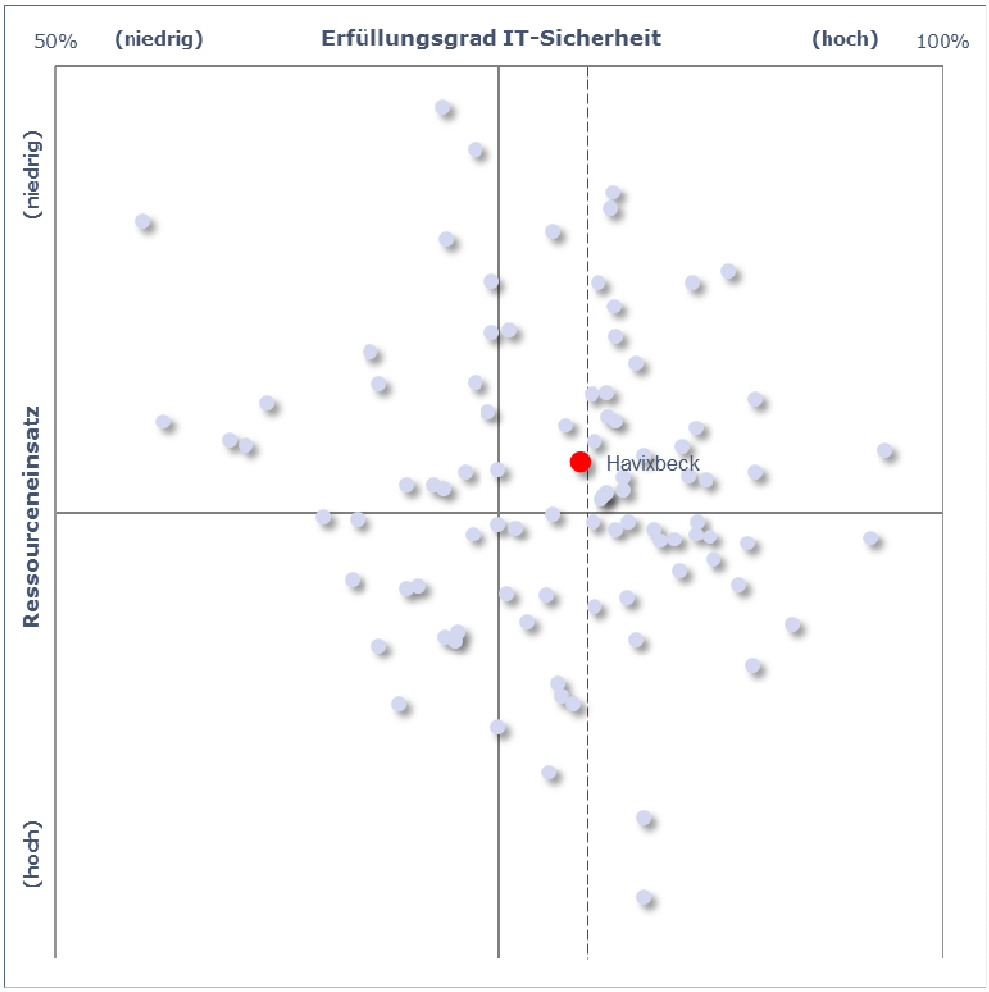
In den nordrhein-westfälischen Städten und Gemeinden ist die örtliche Konzeption und Organisation zur Erfüllung der Querschnittsaufgabe „Informationstechnik" sehr unterschiedlich ausgestaltet. Die zentrale Bereitstellung und Betreuung der IT ist in Havixbeck aufbauorganisatorisch als „EDV, Einkauf" organisiert. Dieser ist dem Bereich „Organisation" zugeordnet, welche zum Fachbereich I „Innere Verwaltung und Finanzen" gehört.

Die Gemeinde Havixbeck betreibt ihre IT in enger Kooperation mit dem IT-Dienstleister der Stadt Münster (citeq). Diese Form einer interkommunalen Zusammenarbeit ist über einen öffentlich-rechtlichen Vertrag ausgestaltet.

Standortbestimmung für die Gemeinde Havixbeck

Die nachfolgende Grafik zeigt für die Gemeinde Havixbeck 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 maßgebliches Kriterium für eine sichere und sachgerechte Aufgabenerfüllung an; Werte unterhalb dieser in der Grafik gestrichelt rot markierten Schwelle können ein Indikator 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.

Hinsichtlich des für die IT aufgewandten Ressourceneinsatzes nimmt die Gemeinde Havixbeck im aktuellen Vergleich eine Position im Mittelfeld ein. Hinsichtlich des Erfüllungsgrades in der IT-Sicherheit können wir einen Wert von 80 Prozent ausweisen.

Der Ressourceneinsatz im Bezugsjahr 2010 liegt bezogen auf den Einwohner mit 20,91 Euro leicht oberhalb des interkommunalen Mittelwertes (19,56 Euro je Einwohner). Bezogen auf den Arbeitsplatz mit IT-Ausstattung werden in der Gemeinde Havixbeck 3.291 Euro ermittelt, womit das Mittel der Vergleichskommunen leicht um 506 je Arbeitsplatz überschritten wird (3.797 Euro je Arbeitsplatz mit IT-Ausstattung).

Technische Risiken, die einen unmittelbaren Handlungsbedarf erfordern, waren im Rahmen der Prüfung u. a. im Bereich des Serverraumes erkennbar; zudem sollten einschlägige Dokumentationen und Regelungen erstellt bzw. aktualisiert werden.

Grundsätzlich profitiert die Gemeinde Havixbeck mit ihrer Anbindung an das Rechenzentrum der Stadt Münster (citeq) von den dort gewährleisteten und der GPA bekannten Sicherheitsmechanismen.

Ressourceneinsatz

Inhalt und Methodik

Um die Aufwendungen, die mit der Bereitstellung und Betreuung der IT entstehen, interkommunal vergleichen 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) aus dem Betrachtungsjahr 2010 heran.

Personalaufwendungen und Stellenausstattung

Zur Ermittlung des Personalaufwands im IT-Bereich sowie zur Betrachtung der Stellenausstattung 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. 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 den KGSt-Berichten "Kosten eines Arbeitsplatzes". Damit blenden wir in unserer 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 entsprechende KGSt-Gutachten folgende Zuschläge: Auf jede vollzeitverrechnete Stelle eine Sachkostenpauschale für Büroarbeitsplätze in Höhe von 5.400 Euro und auf die ermittelten Personalaufwendungen einen Zuschlag von 20 Prozent für allgemeine Leistungen bzw. Leitungsaufgaben („Overhead"-Gemeinkosten).

Ergebnisse im interkommunalen Kennzahlenvergleich

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

Grunddaten zur Kennzahlenbildung (Aufwendungen in Euro)	
IT-Sachaufwendungen	170.640
Personalaufwendungen für originäre IT-Aufgaben (ermittelt nach KGSt-Pauschalen)	58.888
Sachkostenpauschale für Büroarbeitsplätze und Gemeinkostenzuschlag gemäß KGSt-Empfehlung	17.286
Gesamtaufwendungen IT	**246.814**

Im Rahmen des interkommunalen Vergleichs 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 Analysen im Rahmen interner Steuerungsprozesse.

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

IT-Aufwendungen je Einwohner			
Minimum	Maximum	Mittelwert	**Havixbeck**
10,69 Euro	30,28 Euro	19,56 Euro	**20,91 Euro**

IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung			
Minimum	Maximum	Mittelwert	**Havixbeck**
1.878 Euro	5.972 Euro	3.797 Euro	**3.291 Euro**

In der Gemeinde Havixbeck überschreiten die IT-Aufwendungen 2010 je Einwohner mit 20,91 Euro das arithmetische Mittel der bisher geprüften kleinen kreisangehörigen Kommunen um 1,35 Euro je Einwohner.

Neben der Kennzahl mit Einwohnerbezug nehmen wir auch die Betrachtung der IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung in den Blick. Die Aufwendungen je Arbeitsplatz mit IT-Ausstattung betragen 3.291 Euro je Arbeitsplatz. Damit liegt der Wert der Gemeinde Havixbeck 506 Euro unter dem Niveau des interkommunalen Mittelwertes in Höhe von 3.797 Euro.

Im interkommunalen Vergleich haben wir festgestellt, dass – bezogen auf 1.000 Einwohner – im interkommunalen Vergleich der kleinen, kreisangehörigen Kommunen durchschnittlich 5,24 Bildschirmarbeitsplätze ausgewiesen werden. Der Wert der Gemeinde Havixbeck liegt demgegenüber bei 6,36 Bildschirmarbeitsplätzen je 1.000 Einwohner und überschreitet damit den interkommunalen Mittelwert.

Dies ist u. a. darauf zurückzuführen, dass in die Berechnung der Arbeitsplätze die bei der in gemeindlicher Trägerschaft geführten Bibliothek vorhandenen Verwaltungsrechner mitberücksichtigt wurden. Diese Aufgabe ist jedoch nicht in allen betrachteten kleinen, kreisangehörigen Kommunen vorhanden. Zusätzlich wirkt sich auch der Verzicht auf Desk-Sharing[1] bei Teilzeitkräften auf diese Kennzahl aus.

[1] Beim Desk Sharing gibt es weniger Arbeitsplätze als Beschäftigte. Die Konsequenz: Mitarbeiter "besitzen" nicht mehr einen ihnen exklusiv bzw. persönlich zugewiesenen Arbeitsplatz, sondern teilen sich diesen mit anderen Kollegen.

Insofern beeinflusst die vergleichsweise höhere Anzahl von Bildschirmarbeitsplätzen die o. g. Kennzahl, da sich die Aufwendungen mit IT-Bezug (inkl. des nicht durch die reine Anzahl der Rechner beeinflussbaren Fixkostenblocks) auf einen größeren Nenner beziehen.

Aufgrund des entsprechenden Anteils an Dienstleistungsabnahmen bei der citeq tritt grundsätzlich ein Substitutionseffekt zwischen Personal- und Sachaufwendungen ein, der bei einer entsprechenden Differenzierung deutlich wird. Dabei stehen niedrige Personalaufwendungen (4,99 Euro je Einwohner) höheren Sachaufwendungen (14,46 Euro je Einwohner) gegenüber.

Die reinen IT-Personalaufwendungen der Gemeinde Havixbeck liegen mit 4,99 Euro je Einwohner bzw. 785 Euro je Arbeitsplatz etwas oberhalb der derzeitigen Mittelwerte (3,95 Euro bzw. 750 Euro). Der von der Gemeinde erreichte Wert liegt deutlich unterhalb des aktuellen interkommunalen Maximalwertes von 8,19 Euro je Einwohner.

Die Positionierung wird letztlich durch zwei Aspekte beeinflusst. Zum einen durch die Kooperation mit der citeq. Hier werden neben den betriebskritischen und personalintensiven Verfahren (u. a. Finanzwesen, Einwohnerwesen und Personalabrechnung) auch sicherheitsrelevante Aspekte wie z. B. das Sicherheitsgateway, Service- und Supportdienstleistungen bereitgestellt. Diese Leistungen werden durch entsprechenden IT-Sachaufwand abgebildet.

Zum anderen werden von Seiten der Gemeinde jedoch auch Personalressourcen für Tätigkeiten mit IT-Bezug bereitgestellt, welche so in den Vergleichskommunen nicht verzeichnet wurden (fachanwendungsbezogenes Formularwesen MESO). Diese Anteile fließen in die festgestellte Personalquote ein. Hier lässt sich ein Bezug auf die im Prüfbericht der GPA NRW festgestellte Personalintensität in diesem Bereich herstellen.

Empfehlung

Hieraus ergibt sich für die Gemeinde ein Ansatzpunkt, zu hinterfragen, wie diese Leistungen evtl. im Rahmen des Dienstleistungsvertrages mit der citeq Berücksichtigung finden könnten bzw. in welchem Umfang sie tatsächlich notwendig sind.

Hinsichtlich des IT-Sachaufwandes unterschreitet die Gemeinde mit 2.275 Euro je Arbeitsplatz den derzeitigen Mittelwert (2.820 Euro) um 545 Euro je Arbeitsplatz mit IT-Ausstattung. Hinsichtlich der IT-Sachaufwendungen je Einwohner positioniert sich die Gemeinde mit 14,46 Euro auf Höhe des interkommunalen Mittelwertes (14,42 Euro je Einwohner).

Gerade unter dem Blickwinkel, dass ein dauerhaft angemessenes IT-Sicherheitsniveau personelle und finanzielle Ressourcen bindet, sollte auch nicht außer Acht gelassen werden, betriebskritische Services und Anwendungen auf der Grundlage einer gewissen personellen Redundanz zur Verfügung zu stellen.

Insofern können wir positiv feststellen, dass es zu einer personellen Verstärkung im IT-Bereich kommen wird.

Zur weiteren Analyse haben wir die gesamten IT-Aufwendungen des Jahres 2010 der Gemeinde Havixbeck absolut und mit Bezug auf die Einwohnerzahl differenziert:

IT-Aufwendungen der Gemeinde Havixbeck 2010			
Aufwandsart	**Absolut**	**relativ**	**Je Einwohner**
Sachaufwendungen	**170.640**	**69,1 %**	**14,46 Euro**
- Verbrauchsmaterial	4.370	1,8 %	0,37 Euro
- Wartung, Reparatur	364	0,1 %	0,03 Euro
- Softwarepflege	14.724	6,0 %	1,25 Euro
- fremde EDV-Dienstleistungen[2]	93.249	37,8 %	7,90 Euro
- Elektronikversicherung	205	0,1 %	0,02 Euro
- Abschreibungen Hard- und Software	17.970	7,3 %	1,52 Euro
- Miete Telefonanlage/Kopierer	39.758	16,1 %	3,37 Euro
Sachkostenpauschale	**17.286**	**7,0 %**	**1,46 Euro**
Personalaufwendungen	**58.888**	**23,9 %**	**4,99 Euro**
Gesamtaufwendungen	**246.814**	**100,0 %**	**20,91 Euro**

Die Aufstellung verdeutlicht, dass innerhalb der Sachaufwendungen die Aufwendungen für „fremde EDV-Dienstleistungen" den größten Posten ausmachen; hierunter fallen die Leistungsentgelte der citeq.

[2] Entspricht den Leistungen der citeq

Innerhalb der Leistungsentgelte stellt die Bereitstellung des Finanzwesens mit rund 56.000 Euro (ca. 51 Prozent) den größten Anteil. Gefolgt wird dies durch die mit dem Sicherheitsgateway verbundenen Aufwendungen (Virenschutz etc.) mit rund 15 Prozent, dem Sozialwesen (ca. sieben Prozent), dem Einwohnerwesen (ca. sechs Prozent), die Personalabrechnung (ca. fünf Prozent), die Einwohnerpauschale der citeq (ca. vier Prozent), sowie das Kindergarten-Verfahren (ca. drei Prozent). Die restlichen, rund neun Prozent verteilen sich auf kleinere Fachanwendungen und technische Applikationen.

In Bezug auf die Gesamtaufwendungen sind die für die Miete der Telefonanlage/Kopierer aufzuwendenden Entgelte auffällig, da hier fast ein Viertel der reinen Sachaufwendungen gebunden sind.

Allein für die Telefonanlage (Rathaus) wurden 2010 rund 11.350 Euro an Mietaufwendungen aufwendet. Erfahrungsgemäß liegt der Aufwand bei anderen Kommunen hier in einem niedrigeren Bereich.

Feststellung

Auf Nachfrage wurde von Seiten der Gemeinde dieser Eindruck bestätigt; gleichzeitig wurde darauf verwiesen, dass sich bezüglich der Telefonanlage eine wirtschaftlichere Lösung realisieren lässt. Hier ist insofern mit einer Entlastung zu rechnen.

Im Rahmen der Prüfung konnten uns auch die Aufwendungen des Jahres 2011 vorgelegt werden, so dass eine parallele Ermittlung der entsprechenden Kennzahlen möglich war.

Die oben beschriebenen Kennzahlenwerte stellen sich für das Jahr 2011 wie folgt dar:

IT-Aufwendungen je Einwohner: 21,82 Euro (+ 0,91 Euro)

IT-Aufwendungen je Arbeitsplatz: 3.446 Euro (+ 155 Euro)

Insgesamt ist damit eine leichte Steigerung der IT-Sachaufwendungen festzustellen. Die gesamten Sachaufwendungen absolut steigen um 11.633 Euro, dies entspricht einer Erhöhung um fast sieben Prozent.

Innerhalb der einzelnen Kostenblöcke stellen sich die Veränderungen wir folgt dar:

Kostenblock (nur Sachaufwand)	Aufwand 2010 in Euro	Aufwand 2011 in Euro	Steigerung absolut in Euro	Steigerung prozentual
Verbrauchsmaterial	4.370	8.445	+ 4.075	+ 93,3 %
Wartung / Reparatur	364	535	+ 171	+ 47,0 %
Softwarepflege	14.724	15.663	+ 939	+ 6,4 %
Fremde EDV-Dienstleistungen	93.249	105.054	+ 11.805	+ 12,7 %
Elektronikversicherung	205	205	-	-
Abschreibungen	17.970	14.969	- 3.001	- 16,7 %
Miete Telefon / Kopie-rer	39.758	37.403	- 2.355	- 5,9 %
IT Sachaufwand gesamt	**170.640**	**182.274**	**11.634**	**+ 6,8 %**

Der unter dem Kostenblock „Verbrauchsmaterial" erfasste Verbrauch von Toner und Tinte verdoppelt sich fast.

Feststellung

Die erhebliche Steigerung im Verbrauchsmaterial deutet auf Steuerungsbedarf in diesem Bereich hin.

Demgegenüber ist die Steigerung im Bereich der Leistungsentgelte der citeq nur bedingt auf Veränderungen in Bezug auf einzelne Applikationen zurückzuführen.

Vielmehr beinhaltet der Wert des Jahres 2010 Leistungsentgelt-Rückerstattungen im Umfang von 16.974 Euro. Im Jahr 2011 werden demgegenüber nur 7.717 Euro erstattet.

In den einzelnen Applikationen sind dagegen nur marginale und nachvollziehbare Veränderungen zu verzeichnen; die oben für das Jahr 2010 dargestellten Leistungsanteile bleiben im Großen und Ganzen erhalten.

Als Beispiel sei hier wieder auf die Anwendung INFOMA verwiesen, die mit fast 51 Prozent erneut den größten Anteil an den Leistungsentgelten stellt; hier ist gegenüber dem Jahr 2010 eine marginale Steigerung um 1.040,75 Euro festzustellen, dies entspricht einem prozentualen Wert von 1,9 Prozent.

Ohne die Berücksichtigung der Leistungsentgelt-Rückerstattung ergibt sich somit für das Jahr 2011 nur eine Steigerung bei den Leitungsentgelten von rund 2,7 Prozent.

Feststellung

Die gesamten IT-Aufwendungen der Gemeinde Havixbeck liegen im interkommunalen Vergleich beim Bezug auf den Einwohner nur leicht über dem derzeitigen interkommunalen Mittelwert; beim Bezug auf den Arbeitsplatz mit IT-Ausstattung unterschreiten sie diesen.

Da ein Teil der wesentlichen IT-Aufgaben an die citeq ausgelagert ist, weist die Gemeinde einen entsprechenden Anteil von Entgelten für externe IT-Leistungen an den Gesamtaufwendungen für IT auf.

Empfehlung

Veränderungen zu den für das Jahr 2010 festgestellten Rahmenbedingungen sollten dahingehend beobachtet werden, dass weiterhin die jeweils wirtschaftlichste Lösung in Hinblick auf die kommunale IT verwirklicht. Dies gilt z. B. für die festgestellten Aufwendungen im Bereich der TK-Anlage sowie der Verbrauchsmaterialien.

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 Gemeinde Havixbeck 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 Havixbeck 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.

Feststellung

Im Rahmen der Prüfung sind uns alle angeforderten Unterlagen und Informationen zeitnah und in nachvollziehbar aufbereiteter Form zur Verfügung gestellt worden.

Während in der Gemeinde Havixbeck die IT ein Bestandteil des Produktes 0105 „Zentrale Dienste" ist, zeigt der laufende interkommunale Vergleich, dass in der überwiegenden Anzahl der geprüften Kommunen IT als eigenständiges Produkt gesteuert wird.

So wurde nach Umstellung des kommunalen Haushaltes auf die Systematik des NKF ein Produkt gebildet, welches „Zentralen Dienste" gebündelt darstellt. Eine weitergehende Differenzierung der entstehenden

Aufwendungen z. B. in den Haushaltsplänen ist zunächst nicht vorgesehen.

Letztlich steht auch eine Ausgestaltung im Hinblick auf konkrete Steuerungsfunktionen der einzelnen Produkte noch aus. Dazu wäre unter anderem die Definition von konkreteren Zielen erforderlich, deren Erfüllungsgrad messbar sein müsste. Zur Messbarkeit bzw. Darstellung des Zielerreichungsgrades sollten entsprechende Kennzahlen gebildet werden.

Diese im Rahmen des NKF übliche Vorgehensweise ist bei einem abstrakten Produkt wie den „Zentralen Diensten" jedoch zunächst nicht möglich. Als Teil dieses Produktes gehen die Aufwendungen für IT in der Haushaltsdarstellung mehr oder weniger unter.

Eine entsprechende Differenzierung findet z. Z. nur hinsichtlich der internen Darstellung von Sachkonten. So werden wichtige Informationen zu einzelnen Kostenentwicklungen jedoch nur bei gezielten Auswertungen möglich.

Dabei bietet die eingesetzte Finanzsoftware Möglichkeiten, auch die Kostenströme der IT zu verdeutlichen und Kostentreiber zu lokalisieren. Nur wenn diese Kostentreiber bekannt sind, kann letztlich eine sinnvolle Steuerung der IT-Aufwendungen – ob als Bestandteil eines übergeordneten Produktes oder als eigenständiges Produkt - erfolgreich sein.

Empfehlung

Wenn die Ausweisung eines eigenständigen IT-Produktes nicht angedacht ist, sollten dennoch die intern geführten Instrumente genutzt werden.

Zur Steuerung des Teilbereichs IT könnten z. B. die im vorliegenden Bericht verwendeten Kennzahlen für den interkommunalen Vergleich intern fortgeschrieben werden.

Um weitere Steuerungsfunktionen im IT-Bereich zu nutzen, empfehlen wir zudem eine Definition von spezifischeren Zielen, deren Erfüllungsgrad messbar ist. Zur Messbarkeit bzw. Darstellung des Zielerreichungsgrades sollten entsprechende Kennzahlenquoten gebildet werden.

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

Als Grundlage bieten sich z.B. die im vorliegenden Bericht verwendeten Kennzahlen („IT-Aufwendungen je Einwohner bzw. Arbeitsplatz") an.

Empfehlung

Wir empfehlen, das Ziel „wirtschaftlicher Einsatz von Hard- und Software" zu definieren und anhand von Kennzahlen zu messen und fortzuschreiben.

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

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 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.

Feststellung

Mit den umgesetzten Maßnahmen zur IT-Sicherheit nimmt die Gemeinde Havixbeck im Vergleich der kleinen kreisangehörigen Kommunen eine gute Position im Mittelfeld ein.

Der mit dieser Prüfung festgestellte Gesamterfüllungsgrad beträgt für Havixbeck knapp 80 Prozent und liegt damit am Wert, der nach unserer Empfehlung als Voraussetzung für einen sicheren und ordnungsgemäßen IT-Betrieb mindestens erreicht werden sollte. Der Mittelwert für die bisher geprüften Kommunen liegt bei 78 Prozent, der aktuelle interkommunale Minimumwert liegt bei 55 Prozent.

Das Ergebnis wird dabei insbesondere durch das Sicherheitsniveau des Dienstleisters citeq geprägt, von dem die Gemeinde hier klar profitiert.

Festgestellte Optimierungspotenziale zur IT-Sicherheit

Im Detail sind die Ergebnisse der IT-Sicherheitsprüfung in der Checkliste dokumentiert, die diesem Bericht beigefügt ist. Daraus lassen sich konkrete Einzelmaßnahmen ableiten, mit deren Umsetzung eine weitere Erhöhung des Erfüllungsgrades verbunden wäre.

Darüber hinaus wird ausdrücklich auf die Verbesserungsmöglichkeiten hinsichtlich des vorbeugenden Brandschutzes, der Notfallvorsorge und des Sicherheitsmanagements hingewiesen.

Fragenkreis „IT-Räume und Infrastrukturaufbau"

Serverraum

Mögliche Risiken, die die Betriebsbereitschaft der örtlichen IT stören könnten, sehen wir zunächst einmal im Bereich der Serverräumlichkeiten im Keller des Rathauses.

Grundsätzlich handelt es sich um eine geeignete Räumlichkeit, welche jedoch in der Ausgestaltung erhebliche Mängel aufweist. Der Zugang zum Serverraum erfolgt über Heizungsraum, welcher mit einer Brandschutztür ausgestattet ist. Der eigentliche Zugang zum Serverraum verfügt jedoch über keine Sicherheitstür. Weiterhin sind im Serverraum keine Sicherheitsfenster verbaut. Beides wird vom BSI für Technikräume empfohlen.

Empfehlung

Es sollte geprüft werden, inwieweit eine sicherheitszertifizierte Tür als Zugang zum Serverraum sowie ein entsprechendes Fenster verbaut werden könnten.

Im Rahmen der interkommunalen Betrachtung hat die bisherige Prüfung gezeigt, dass Brände in Technikräumen nicht so selten sind, wie man dies vielleicht vermuten könnte.

Technikräume stellen aufgrund ihrer Zweckbestimmung und der hohen Dichte an technischen Geräten ein erhöhtes Brandrisiko dar. Hier sollten daher angemessene und geeignete Maßnahmen zur Brandvermeidung und Früherkennung obligatorisch sein.

Im gesamten Rathaus der Gemeinde Havixbeck besteht derzeit kein Gefahrenmeldesystem (Meldung bei Feuer, Einbruch etc.). Mindestens für den Serverraum sollte ein Alarmierungssystem bestehen, zumal hier zusätzliche Brandlasten gelagert sind.

Empfehlung

Es sollte geprüft werden, welche Gefahren durch eine Meldeanlage im Bereich des Serverraumes abgedeckt werden könnten (Einbruch, Brand, Rauch, Wasser). Ein ausgelöster Alarm sollte auch außerhalb der Betriebszeiten explizit einen Empfänger haben.

Die im Serverraum vorhandenen Brandlasten sollten entfernt werden.

Durch den Serverraum werden Versorgungsleitungen (u. a. vom Blockheizkraftwerk der Schule) geführt. Als Risiko muss dabei gesehen werden, dass diese Rohrleitungen über den Serverracks verlaufen und damit bei einer Leckage ein entsprechendes Risiko darstellen.

Empfehlung

Es sollte geprüft werden, inwieweit Maßnahmen zur Schadensvermeidung (z.B. Ableitbleche, zusätzliche wasserdichte Ummantelung der Leitung) realisiert werden können.

Bei der Begehung des Serverraumes wurde festgestellt, dass die Umgebungstemperatur deutlich zu warm war. Eine Klimatisierung ist derzeit

nicht vorhanden. Das BSI weist in seinem Grundschutzhandbuch darauf hin, dass eine dauerhaft hohe Umgebungstemperatur zu Ausfällen im laufenden Betrieb führen kann. Ähnliche Hinweise geben die Hardwarehersteller unter Hinweis auf damit verbundene Garantieverluste.

Empfehlung

Es sollte geprüft werden, inwieweit eine redundante Klimatisierung realisiert werden kann. Ergänzt werden sollte eine entsprechende Überwachung, die sicherstellt, dass ein Ausfall der Klimatisierung auch außerhalb der üblichen Betriebszeiten gemeldet wird.

Der Zugang zum Serverraum an sich ist personenscharf eingrenzbar; allerdings kann nicht nachvollzogen werden, wann der Raum betreten wurde. Eine Nachvollziehbarkeit kann jedoch im Schadensfall notwendig sein.

Empfehlung

Es sollte geprüft werden, wie das Betreten des Raumes durch technische Maßnahmen erfasst und personenscharf zugeordnet werden kann.

In diesem Zusammenhang empfehlen wir grundsätzlich, den Serverraum im Rathaus in Zusammenarbeit mit dem vorbeugenden Brandschutz der Feuerwehr, der kriminalpolizeilichen Beratung und der technischen Gebäudewirtschaft einer Wertung zu unterziehen und ggf. Lösungsmöglichkeiten zu erarbeiten, die die vorgenannten Risiken minimieren.

Sicherheitsmanagement

Die sichere Verarbeitung von Informationen ist heutzutage für nahezu alle Behörden von existenzieller Bedeutung. Dabei können Informationen entweder auf Papier, in Rechnern oder auch in Köpfen gespeichert

sein. Für den Schutz der Informationen reicht es nicht aus, nur technische Sicherheitslösungen einzusetzen.

Ein angemessenes IT-Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Sicherheitsmaßnahmen ist eine systematische Vorgehensweise. Diese Planungs-, Lenkungs- und Kontrollaufgabe wird als Informationssicherheitsmanagement oder auch als IT-Sicherheitsmanagement bezeichnet.

> **Empfehlung**
>
> Als grundlegendes Element des IT-Sicherheitsmanagements sollten die vorhandenen Regelungen und Dokumentationen zum Umgang mit IT in der Verwaltung regelmäßig aktualisiert und fortgeschrieben werden.

Notfallmanagement

Verfügbarkeitsanforderungen

Verfügbarkeitsanforderungen sind Teil eines IT-Notfallvorsorgemanagements und stellen die Grundlage für Ausgestaltung der IT- Infrastruktur sowie der Notfallplanung dar.

In Bezug auf die zukünftige strategische Ausrichtung sollte daher die bestehende IT- Strategie um Verfügbarkeitsanforderungen ergänzt werden.

Die Verfügbarkeit von Daten ist eine wirtschaftliche Komponente in der Datenverarbeitung und der Datenübertragung. Die Verfügbarkeit kann sich gleichermaßen auf die Systeme und deren Funktionalität, auf die von Daten oder Informationen beziehen. Zwischen der Verfügbarkeit und der mit den Systemen zu erzielenden Arbeitsleistung besteht eine Wechselwirkung. Da bei Ausfall eines Systems ein hoher wirtschaftlicher Schaden entstehen kann, sollten Datenverarbeitungssysteme und Kommunikationswege möglichst so gestaltet und ausgelegt sein, dass eine hohe Verfügbarkeit zugesichert werden kann.

Im Rahmen der Überlegungen, welche Systemverfügbarkeiten erforderlich sind, ist es eine praktikable Vorgehensweise, zu den einzelnen IT-Anwendungen die Verfahrensverantwortlichen, in letzter Instanz auch die Behördenleitung, nach den tolerierbaren Ausfallzeiten der benutzten IT-Komponenten zu befragen, um danach die Ergebnisse (nach IT-System und Komponenten geordnet) in einer Übersicht aufzuführen.

Soweit IT-Leistungen von Dienstleistern erbracht werden, stellen die Verfügbarkeitsanforderungen eine wichtige Grundlage für die Vereinbarung von Serviceverträgen oder Dienstgütevereinbarungen dar. Derartige Vereinbarungen werden auch als Service Level Agreements (SLA) ausgestaltet und stellen den Umfang einer vertraglich zugesicherten Leistung dar, auf dessen Erfüllung sich der Kunde berufen kann.

Empfehlung

Bei der Gemeinde Havixbeck sollten Verfügbarkeitsanforderungen definiert werden.

Notfallvorsorgekonzept

Die Gemeinde Havixbeck verfügt derzeit über kein explizites Notfallvorsorgekonzept, allerdings sind wichtige Aspekte in Zusammenarbeit mit der citeq geregelt. Dennoch bedarf es auf Seiten der Gemeinde der Festlegung von bestimmten Entscheidungen, die im Bedarfsfall auch einem sachkundigen Dritten die Möglichkeit eröffnen, einen geregelten IT-Betrieb weiter zu führen.

Hierzu zählen u. a. die o. g. Verfügbarkeitsanforderungen aber auch Festlegungen zu Ausweichstandorten und Alarmierungspläne. Hier bietet es sich an, an einem gesicherten Ort (z. B. Tresor der Gemeindekasse) ein Notfallblatt mit den wichtigsten Informationen zu hinterlegen.

Empfehlung

Wir empfehlen, die wichtigsten Aspekte einer Notfallvorsorge in einem Notfallkonzept zusammenzufassen und an einem gesicher-

ten Ort zu hinterlegen.

Im Detail sind die Ergebnisse der IT-Sicherheitsprüfung in der Checkliste dokumentiert, die diesem Bericht beigefügt ist. Daraus lassen sich weitere konkrete Einzelmaßnahmen ableiten.

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 Gemeinde Havixbeck hat zum Zeitpunkt der Prüfung keinen Datenschutzbeauftragten sowie keinen Stellvertreter gemäß den gesetzlichen Bestimmungen des DSG NRW bestellt.

Ein ordnungsgemäß geführtes Verfahrensverzeichnis gem. § 8 DSG NRW konnte nicht vorgelegt werden.

Empfehlung

Die Bestellung eines Datenschutzbeauftragten sowie eines Vertreters, welche die Voraussetzungen des DSG NRW erfüllen, sollte unverzüglich in die Wege geleitet werden. Evtl. bietet sich hier eine interkommunale Zusammenarbeit an.

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

Herne, den 23.04.2012

Michael Kuzniarek
Abteilungsleitung

Marcus Meiners
Prüfer

Überörtliche Prüfung Informationstechnik
- Erhebungsbogen IT-Sicherheit -

Name der Körperschaft:
Gemeinde Havixbeck

Gesprächstermin:
20.11.2012

Prüfer:
3M

Gesprächspartner in der Kommune:
Herr Wessels

Fragenkreis: IT-Räume und Infrastrukturaufbau

Serverraum

Baustein Serverraum:
von 21 Maßnahmen 7x JA, 9x NEIN, 2x teilweise, 3x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Angepasste Aufteilung der Stromkreise	ja	
Handfeuerlöscher	ja	im Kellerflur erreichbar
Verwendung von Sicherheitstüren und -fenstern	nein	Zugang zum Serverraum erfolgt über Heizungsraum (Brandschutztür); der eigentliche Zugang zum Serverraum verfügt über keine Sicherheitstür. Im Serverraum sind keine Sicherheitsfenster verbaut. Empfehlung: Prüfung, inwieweit eine sicherheitszertifizierte Tür und Fenster verbaut werden könnten.
Geschlossene Fenster	nein	Im Serverraum ist keine Klimatisierung vorgesehen, so dass es zu einer entsprechenden Wärmebildung kommt. Um ansatzweise Abhilfe zu schaffen, ist das einzige Fenster (Einfachverglasung) ununterbrochen geöffnet. Hier kann es zu Staubeinwirkungen, Wassereinlauf etc. kommen. Empfehlung: Wir eine Klimatisierung installiert, kann das Fenster geschlossen werden. Mittelfristig sollte ein Sicherheitsfenster eingebaut werden.
Gefahrenmeldeanlage/Brandmelder	nein	Im gesamten Rathaus besteht keine Gefahrenmeldeanlage. Empfehlung: Prüfung, welche Gefahren durch eine Meldeanlage abgedeckt werden könnten (Einbruch, Brand, Rauch, Wasser). Ein ausgelöster Alarm sollte explizit einen Empfänger haben (auch außerhalb der Betriebszeiten!)
Abgeschlossene Türen	ja	
Vermeidung von Risiken durch wasserführende Leitungen	nein	Durch den Serverraum gehen Versorgungsleitungen (u. a. vom Blockheizkraftwerk Schule); diese verlaufen über den Serverracks und stellen bei Leckage ein entsprechendes Risiko dar. Empfehlung: Prüfung, inwieweit Maßnahmen zur Schadensvermeidung (z.B. Ableitbleche, zusätzliche wasserdichte Ummantelung der Leitung) realisiert werden können.
Überspannungsschutz	ja	
Not-Aus-Schalter	nein	Empfehlung: Prüfung, inwieweit ein Not-Aus-Schalter aus Gründen des Personenschutzes installiert werden kann.
Klimatisierung	nein	Eine Klimatisierung ist derzeit nicht vorhanden. Der Serverraum ist deutlich zu warm; die hohe Umgebungstemperatur kann zu Ausfällen im laufenden Betrieb führen. Empfehlung: Prüfung, inwieweit eine (redundante) Klimatisierung realisiert werden kann. Ergänzt werden sollte eine entsprechende Überwachung, die sicherstellt, dass ein Ausfall der Klimatisierung gemeldet wird.

Lokale unterbrechungsfreie Stromversorgung	**teilw.**	Keine redundante USV. Empfehlung: Prüfung, inwieweit eine Redundaz notwendig ist und hergestellt werden könnte.
Fernanzeige von Störungen	**ja**	Gilt für Server über die citeq; jedoch erfolgt keine Weiterleitung einer Störung an Verantwortliche vor Ort. Empfehlung: Zukünftig sollte auch sichergestellt werden, dass Schadensereignisse außerhalb der Dienstzeit auch an Verantwortliche in der Verwaltung weitergeleitet werden.
Redundanzen in der technischen Infrastruktur (ohne Storage)	**ja**	über HP Verträge und citeq
Technische und organisatorische Vorgaben für Serverräume	**nein**	Empfehlung: Festlegung und Dokumentation organisatorischer Regelungen, in denen die wichtigsten Anforderungen, die an einen Serverraum zu stellen sind, grundsätzlich dokumentiert sind (z.B. Zutrittsregelungen, Raumplanungskonzept mit grober Definition der Anforderungen).
Brandschutz von Patchfeldern	**nein**	Eine Trennung der Verteiler von der Serverinfrastruktur ist derzeit praktisch nicht vorhanden. Empfehlung: Prüfung, inwieweit eine Abschottung der Verteiler gegenüber der Serverinfrastruktur realisiert werden könnte, mit dem Ziel, die Ausbreitung eines Brandes im Serverbereich auf die Verteiler zu verhindern. Eine technische Umsetzung ergäbe sich z. B. durch räumliche oder sonstige physische Trennung (z.B. eigenes Rack mit besonderem Brandschutz).
Zutrittsregelung und -kontrolle	**nein**	Der Zugang zum Serverraum an sich ist personenscharf eingrenzbar; allerdings kann nicht nachvollzogen werden, wann der Raum betreten wurde. Empfehlung: Der Zugang zum Serverraum sollte dokumentiert werden und evtl. durch technische Maßnahmen erfasst und für einen möglichen Schadensfall personenscharf zugeordnet werden.
Rauchverbot	**ja**	
Verwendung von hochverfügbaren Architekturen	**teilw.**	über citeq für große Wesen
Zentrales Speichersystem vorhanden	**entfällt**	
Storage System redundant	**entfällt**	
Einsatz von Servervirtualisierung	**entfällt**	

IT-Verkabelung		**Baustein IT-Verkabelung:** **von 12 Maßnahmen 8x JA, 1x NEIN, 3x teilweise, 0x entfällt**
Maßnahmen	**erfüllt?**	**Bemerkungen**
Verkabelungsart den technischen Anforderungen entsprechend	**ja**	1999 CAT V
Netz-Topologie	**ja**	ethneret stern
Erneuerung der IT-Verkabelung	**ja**	1999 Anbindung Bauamt über Lichtwelle
Redundanzen für die Primärverkabelung	**ja**	
Redundanzen für die Gebäudeverkabelung	**ja**	
Brandabschottung von Trassen	**teilw.**	Im Serverraum wurden Wanddurchbrüche nicht rauchdicht versiegelt. Empfehlung: Nachträgliche Versiegelung der Öffnungen.

Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht	ja	
Ausreichende Trassendimensionierung	ja	
Materielle Sicherung von Leitungen und Verteilern	ja	
Dimensionierung und Nutzung von Schranksystemen	teilw.	Derzeit werden im Serverraum nur teilweise Racksysteme genutzt. Grund hierfür ist der offensichtliche Platzmangel. Empfehlung: Nach Entfernung der Brandlasten sollte geprüft werden, ob ein weiteres Racksystem die übrigen Komponenten aufnehmen könnte.
Neutrale Dokumentation in den Verteilern	teilw.	Derzeit kann die vorhandene Verteilung nur über die Bezeichnung der Dosen nachvollzogen werden, was für einen sachkundigen Dritten (z. B. citeq) im Vertretungsfall schwierig sein dürfte. Empfehlung: Erstellung und Fortschreibung einer entsprechenden Dokumentation und Vorhaltung in der Nähe des Verteilerschrankes.
Laufende Fortschreibung und Revision der Netzdokumentation	nein	s. o.

Sicherheitsgateway

Baustein Sicherheitsgateway:
von 19 Maßnahmen 19x 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	"erfüllt"-Annahme wegen Auslagerung
Auswahl geeigneter Grundstrukturen für Sicherheitsgateways	ja	"erfüllt"-Annahme wegen Auslagerung
Content-Filter im Einsatz	ja	"erfüllt"-Annahme wegen Auslagerung
Proxyserver im Einsatz	ja	"erfüllt"-Annahme wegen Auslagerung
Gateway redundant	ja	"erfüllt"-Annahme wegen Auslagerung
Schulung der Administratoren des Sicherheitsgateways	ja	"erfüllt"-Annahme wegen Auslagerung
Protokollierung der Sicherheitsgateway-Aktivitäten	ja	"erfüllt"-Annahme wegen Auslagerung
Integration von Proxyservern in das Sicherheitsgateway	ja	"erfüllt"-Annahme wegen Auslagerung
Integration von VPN-Komponenten in ein Sicherheitsgateway	ja	"erfüllt"-Annahme wegen Auslagerung
Integration von Virenscannern in ein Sicherheitsgateway	ja	"erfüllt"-Annahme wegen Auslagerung
Einsatz von Stand-alone-Systemen zur Nutzung des Internets	ja	"erfüllt"-Annahme wegen Auslagerung
Adressumsetzung - NAT (Network Address Translation)	ja	"erfüllt"-Annahme wegen Auslagerung
Intrusion Detection und Intrusion Prevention Systeme	ja	"erfüllt"-Annahme wegen Auslagerung
Integration eines Webservers in ein Sicherheitsgateway	ja	"erfüllt"-Annahme wegen Auslagerung
Integration eines E-Mailservers in ein Sicherheitsgateway	ja	"erfüllt"-Annahme wegen Auslagerung
Integration eines Datenbank-Servers in ein Sicherheitsgateway	ja	"erfüllt"-Annahme wegen Auslagerung
Integration eines DNS-Servers in ein Sicherheitsgateway	ja	"erfüllt"-Annahme wegen Auslagerung

Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway	ja	"erfüllt"-Annahme wegen Auslagerung
Notfallvorsorge bei Sicherheitsgateways	ja	"erfüllt"-Annahme wegen Auslagerung

WLAN		**Baustein WLAN: von 9 Maßnahmen 0x JA, 0x NEIN, 0x teilweise, 9x 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 6x JA, 2x NEIN, 0x teilweise, 1x entfällt**
Maßnahmen	**erfüllt?**	**Bemerkungen**
Existiert bei Notebooks Homogenität?	ja	Win7, XP
Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz	entfällt	werden nicht transportiert.
Einsatz von Diebstahl-Sicherungen	nein	Empfehlung: Prüfung, inwieweit die Sicherung über z. B. Kensington Schlösser sinnvoll ist.
Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung	nein	Empfehlung: Ergänzung der vorhandenen Regelung um Aspekte bezüglich der Aufbewahrung und Handhabung der mobilen Geräte, Sperrung, Verbot der Einwahl in fremde WLANs usw.
Regelmäßiger Einsatz eines Anti-Viren-Programms	ja	McAffee
Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme	ja	
Sichere Kommunikation von unterwegs	ja	
Sicherer Anschluss von Notebooks an lokale Netze	ja	
Datensicherung bei mobiler Nutzung des IT-Systems	ja	keine lokale Datensicherung vorgesehen.

Allgemeiner Client		**Baustein Allgemeiner Client: von 14 Maßnahmen 10x JA, 0x NEIN, 2x teilweise, 2x entfällt**
Maßnahmen	**erfüllt?**	**Bemerkungen**
Existiert ein homogenes Umfeld bei den Client PC? Hardware	ja	XP/ Win 7

Existiert ein homogenes Umfeld bei den Client PC? Software	ja	
Austauschzyklen	entfällt	
Wie alt sind die Geräte?		bis zu 5 Jahren
Wird ein Systemmanagement eingesetzt?	ja	Nagios
Wird Remote Desktop genutzt?	ja	
Herausgabe einer PC-Richtlinie	ja	aber veraltete Version
Dokumentation der Systemkonfiguration	teilw.	
Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	ja	WSUS
Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz	ja	aber veraltete Version
Geregelte Außerbetriebnahme eines Clients	ja	
Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung	ja	
Regelmäßiger Einsatz eines Anti-Viren-Programms	ja	McAffee
Einrichten einer Referenzinstallation für Clients	teilw.	beim WSUS wird dies über die Testgruppe sichergestellt
Regelmäßige Datensicherung	entfällt	

Fragenkreis: IT-Management

Sicherheitsmanagement

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

Maßnahmen	erfüllt?	Bemerkungen
Erstellung einer Leitlinie zur Informationssicherheit	nein	Empfehlung: Aufnahme einer expliziten Erklärung der Verwaltungsleitung in die Dienstanweisung, dass der IT-Sicherheit in der Kommune ein hoher Stellenwert eingeräumt wird; kann z.B. auch als Präambel in ein IT-Konzept, eine Dienstanweisung zu Datenschutz und Datensicherheit o.ä. ausgestaltet sein.
Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	teilw.	Bedingt werden über Arbeitskreise der citeq auch Sicherheitsaspekte bedient, über die der BM bzw. der Verwaltungsleitung direkt infomiert werden. Ein speziellen IT-Sicherheitsbeauftragtert ist in Havixbeck nicht bestellt.
Erstellung eines Sicherheitskonzepts	ja	Die Gemeinde ist dem Sicherheitskonzeot der citeq beigetreten.
Management-Berichte zur Informationssicherheit	ja	über citeq, Arbeitsausschuss / Zentralausschuss ist BM informiert
Dokumentation des Sicherheitsprozesses	ja	Ansprechpartner von Seiten citeq benannt
Festlegung der Sicherheitsziele und -strategie	ja	citeq
Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	nein	s. o.
Erstellung von zielgruppengerechten Sicherheitsrichtlinien	ja	Regelung über Fachanwendungsadmins bzw. citeq

Sicherheitsorganisation

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

Maßnahmen	erfüllt?	Bemerkungen

Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz	ja	Geschäftsverteilungsplan
Vergabe von Zutrittsberechtigungen	ja	über IT Admin.
Vergabe von Zugangsberechtigungen	ja	IT Admins auf Zuruf der FB´s (über Personalamt)
Vergabe von Zugriffsrechten	ja	IT Admins auf Zuruf der FB´s (über Personalamt) Active Directory gilt als Dokumentation
Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln	ja	
Schlüsselverwaltung	teilw.	Die Schlüssel zum Serverraum stehen lediglich dem IT-Admin und dem Hausmeister zur Verfügung. Empfehlung: Formalisierung der Schlüsselgewalt in der Dienstanweisung.
Kontrollgänge	ja	

Sicherheit Personal

Baustein Sicherheit Personal:
von 8 Maßnahmen 7x JA, 1x NEIN, 0x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Geregelte Einarbeitung/Einweisung neuer Mitarbeiter	ja	Einarbeitung durch FB
Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen	ja	
Schulung vor Programmnutzung	ja	citeq
Schulung zu IT-Sicherheitsmaßnahmen	nein	Empfehlung: Stärkung des Bewusstseins für IT-Sicherheit und der Eigenverantwortung durch z. B. Nutzung des BITS (Behörden-IT-Sicherheitstraining - www.bits-training.de).
Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern	ja	
Schulung des Wartungs- und Administrationspersonals	ja	
Personaleinsatz und -qualifizierung	ja	
Vertraulichkeitsvereinbarungen	ja	

Notfallvorsorgekonzept

Baustein Notfallvorsorgekonzept:
von 15 Maßnahmen 3x JA, 2x NEIN, 3x teilweise, 7x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Erstellung einer Übersicht über Verfügbarkeitsanforderungen	teilw.	Hinsichtlich der großen Wesen ist dies durch die citeq geregelt. Empfehlung: Dennoch sollte vor Ort eine Festlegungerfolgen, welche Systeme bzw. Anwendungen nach einem Totalausfall wie schnell wieder verfügbar sein müssen.
Notfall-Definition, Notfall-Verantwortlicher	nein	Empfehlung: Festlegung für den Notfall, der diesen Fall erstens definiert und zweitens Zuständigkeiten regelt.

Erstellung eines Notfall-Handbuches	**teilw.**	evtl. über citeq vorhanden. Empfehlung: Auch bei hoher Auslagerung sollte für bestimmte Notfallszenarien dokumentiert sein, wer beim IT-Dienstleister verbindlicher Ansprechpartner ist. Ein hinterlegtes "Notfallblatt" mit diesen Angaben ist ausreichend.
Dokumentation der Kapazitätsanforderungen der IT-Anwendungen	**entfällt**	
Definition des eingeschränkten IT-Betriebs	**entfällt**	
Untersuchung interner und externer Ausweichmöglichkeiten	**nein**	Empfehlung: Festlegung, ob und welchen Ausweichstandort es bei einem Totalausfall (durch Brand, Großschadensereignis usw.) gibt.
Regelung der Verantwortung im Notfall	**ja**	
Alarmierungsplan	**teilw.**	indirekt über citeq; Empfehlung: Ausgestaltung vor Ort und Aufnahme in Notfallhandbuch
Notfall-Pläne für ausgewählte Schadensereignisse	**entfällt**	
Erstellung eines Wiederanlaufplans	**entfällt**	
Durchführung von Notfallübungen	**entfällt**	
Erstellung eines Datensicherungsplans	**entfällt**	
Ersatzbeschaffungsplan	**entfällt**	
Abschließen von Versicherungen	**ja**	
Redundante Kommunikationsverbindungen	**ja**	

Hard- und Softwaremanagement		**Baustein Hard- und Softwaremanagement: von 9 Maßnahmen 6x JA, 0x NEIN, 2x teilweise, 1x entfällt**
Maßnahmen	**erfüllt?**	**Bemerkungen**
Regelung des Passwortgebrauchs	**ja**	
Hinterlegen des Passwortes	**ja**	citeq
Dokumentation der Systemkonfiguration	**teilw.**	Einrichtung erfolgte über die citeq; es besteht keine nachvollziehbare Dokumentation vor Ort.
Regelung für die Einrichtung von Benutzern / Benutzergruppen	**ja**	über LogIn Script
Dokumentation der zugelassenen Benutzer und Rechteprofile	**ja**	

Dokumentation der Veränderungen an einem bestehenden System	entfällt	
Informationsbeschaffung über Sicherheitslücken des Systems	ja	
Software-Abnahme- und Freigabe-Verfahren	teilw.	Hinsichtlich der großen Wesen über citeq; kleine Applikationen sind jedoch nicht nachvollziehbar.
Kontrolle der Protokolldateien	ja	über Nagios

Virenschutz

Baustein Virenschutz:
von 4 Maßnahmen 4x JA, 0x NEIN, 0x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Erstellung eines Computer-Virenschutzkonzepts	ja	über citeq für große Wesen
Aktualisierung der eingesetzten Computer-Viren-Suchprogramme	ja	McAffee
Regelmäßiger Einsatz eines Anti-Viren-Programms	ja	
Verhaltensregeln bei Auftreten eines Computer-Virus	ja	

Fragenkreis: Backup und Archivierung

Datensicherung

Baustein Datensicherung:
von 9 Maßnahmen 7x JA, 0x NEIN, 1x teilweise, 1x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Verpflichtung der Mitarbeiter zur Datensicherung	ja	
Beschaffung eines geeigneten Datensicherungssystems	ja	BackUp Exec Tagesvollsicherung
Geeignete Aufbewahrung der Backup-Datenträger	ja	im Tresor; prüfen, ob Sparkassen Tresor möglich
Sicherungskopie der eingesetzten Software	entfällt	
Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen	ja	
Regelmäßige Datensicherung	ja	
Entwicklung eines Datensicherungskonzepts	teilw.	Tatsächliche Sicherung durch citeq; eine eigene Dokumentation der Datensicherung liegt nicht vor. Empfehlung: Sollte zum Zwecke der Nachvollziehbarkeit erstellt werden.
Dokumentation der Datensicherung	ja	über BackUp Exec

Datenerhebung (Checkliste) zur Prüfung der IT-Sicherheit - Blatt 9

Übungen zur Datenrekonstruktion	**ja**	