Beratung · Prüfung · Service

Überörtliche Prüfung Informationstechnologie der Stadt Hilden vom 13.08. bis 14.10.2009

Beratung · Prüfung · Service

GPA NRW

Überörtliche Prüfung Informationstechnologie der Stadt Hilden vom 13.08. bis 14.10.2009

Inhaltsverzeichnis

Zur GPA NRW und zur Prüfung

Worauf stützt sich die Prüfung?

Die GPA NRW führt die überörtliche Prüfung der Informationstechnologie auf der Grundlage des § 105 der Gemeindeordnung NRW (GO NRW) bei den Städten und Gemeinden, sowie bei den Gemeindeverbänden durch. Im Sinne des § 105 GO NRW sind dabei Wirtschaftlichkeit, Rechtmäßigkeit und sachgerechtes Handeln in den Blick zu nehmen.

Hierdurch wird der Gemeindeprüfung neben der traditionellen Rechtmäßigkeitsprüfung bewusst eine aktive Rolle zugedacht, die insbesondere auf den Modernisierungsprozess der öffentlichen Verwaltung ausgerichtet ist. Mit dem Gesetzesauftrag soll der GPA NRW somit die Möglichkeit eingeräumt werden, die Gemeinde als Ganzes in den Blick zu nehmen und im Rahmen der Prüfung steuerungsrelevante Informationen liefern[1].

Die Entscheidung, die IT in den kommunalen Verwaltungen einer intensiven Betrachtung zu unterziehen, hat vielerlei gute Gründe. Die Informationstechnologie spielt gerade in dem laufenden Modernisierungsprozess eine herausragende Rolle, denn in den meisten Fällen ist gerade mit den Entwicklungen der vergangenen Jahre auf dem Sektor der Computerindustrie der Grundstein für umfassende Modernisierungsmöglichkeiten gelegt worden. Das Maß der Steuerungs- und Optimierungsmöglichkeiten sowie die Wirtschaftlichkeitspotenziale sind hier außerordentlich hoch, wovon insbesondere die Organisationsbereiche der Verwaltungen immer häufiger Gebrauch machen. In zahlreichen Fällen ist der Einsatz von IT sogar oft die einzige Lösung, das einzige Organisationsmittel, um einen effizienten und effektiven Ablauf der Geschäftsprozesse gestalten zu können.

Neben den zahlreichen Chancen, die sich durch den Einsatz der IT für die Verwaltungen ergeben, bestehen jedoch auch Risiken, die mit der Nutzung der IT verbunden sind. Aus diesem Grund ist der konkrete Prüfauftrag um einen risikoorientierten Ansatz erweitert worden. Hier wird es Aufgabe der Prüfung sein, Sicherheitsrisiken im Sinne eines

[1] Vgl. Becker/Held Erl. Zu § 105 Absatz 3 GO NRW

Grundschutzes (Datenschutz und Datensicherheit) zu identifizieren und zu benennen.

Ziele und Inhalte

Mit unserer Prüfung wollen wir zu einem wirtschaftlichen, sachgerechten und rechtmäßigen Einsatz der Informationstechnologie in Hilden beitragen, indem wir

- Strukturen, Prozesse und Ergebnisse transparent machen,
- Kriterien und Maßstäbe zu deren Beurteilung liefern,
- einen Erreichungsgrad bestimmen und bewerten,
- Empfehlungen geben und Handlungsalternativen aufzeigen.

Die Verantwortung für die Realisierung der oben genannten Ziele bleibt bei der Stadt Hilden. Wir sind der Auffassung, dass der hohe Ressourcenverbrauch und das erhebliche persönliche Haftungsrisiko die Informationstechnologie zur Chefsache machen.

Methodik und Berichtsaufbau

Ergebnisse unserer Analyse werden im Bericht als **Feststellung** bezeichnet. Eine Stellungnahme der Kommune ist hierzu nur dann erforderlich, wenn dieses im Bericht entsprechend gekennzeichnet ist.

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

Der Prüfbericht beginnt mit einem **Überblick über die Ergebnisse**.

In unserem Bericht haben wir Feststellungen und Empfehlungen zu folgenden Bereichen ausgearbeitet:

- Kosten / Wirtschaftlichkeit
- Organisation und Steuerung

- Infrastruktur und Sicherheit
- Datenschutz.

Die spezifischen Ziele, Inhalte und Fragestellungen sind in den einzelnen Kapiteln beschrieben.

Unser Prüfungsprozess vollzieht sich generell in 3 Schritten:

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

Prüfung ist auch ein kommunikativer Vorgang. So werden viele Sachverhalte bereits im Verlauf der Prüfung mündlich erörtert und Probleme ausgeräumt. In diesem Prüfbericht finden sich daher nur die wesentlichen Informationen wieder.

Unsere Methodik haben wir unter den einzelnen Prüfungsfeldern konkreter beschrieben.

Der Prüfungsbericht ist im Nachrichtenstil aufgebaut. Deshalb stellen wir im Anschluss an diese Vorbemerkungen zunächst die wichtigsten Ergebnisse unserer Prüfung dar. Aus der Checkliste zur IT-Sicherheit, die zu Ihrer Kenntnis im Anhang beigefügt ist, können Sie entnehmen, welches Spektrum unsere Prüfung in diesem Bereich umfasst.

Informationen...

... zum Prüfungsablauf

Wir haben die Prüfung in Ihrer Stadt Hilden vom 13.08. bis 14.10.2009 durchgeführt.

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

Um zukunftsgerichtete Aussagen zu treffen, haben wir neben den aktuellen Daten auch Daten früherer Jahre berücksichtigt.

Durchführung der Prüfung:	Alexander Ehrbar
	Michael Neumann

Wir haben das Prüfungsergebnis mit

- Herrn Bürgermeister Thiele
- Herrn Ersten Beigeordneten Danscheidt
- Herrn Kramer als IT-Leiter
- Herrn Witek als Leiter der Rechnungsprüfung

erörtert.

Der Entwurf des Prüfberichts wurde übersandt.

... zur Ausgangslage in der kommunalen IT-Landschaft

Die Informationstechnologie (IT) nimmt in den Verwaltungen eine elementare Funktion ein. Sie stellt nicht nur das technische Handwerkszeug für inzwischen nahezu alle Aufgabenbereiche dar, sondern hat grundle-

gende Bedeutung für Entwicklungs- und Rationalisierungspotenziale und die damit angestrebte Optimierung der Geschäftsprozesse in den Verwaltungen.

Der Einsatz moderner und komplexer IT stellt allerdings sehr hohe Anforderungen an die Kommune. Soweit IT in autonomer und teilautonomer Form praktiziert wird, vertreten wir die Auffassung, dass das Gebot einer ordnungsgemäßen und sicherheitsorientierten IT mindestens auf gleichrangiger Stufe mit dem Gebot der wirtschaftlichen Ablauffunktionalität steht.

In dieser Hinsicht unterscheidet sich der IT-Betrieb, der von einer Kommune in eigener Verantwortung geführt wird, kaum von dem eines Gebietsrechenzentrums, etwa eines IT-Zweckverbandes.

... zur Ausgangslage in Hilden

Die Stadt Hilden fällt in die Größenklasse der mittleren Kommunen; zum Stichtag 31.12.2008 hatte die Stadt 55.961 Einwohner.

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

Die Stadt Hilden betreibt ihre IT vollständig autonom in eigener Verantwortung und ohne Anbindung an ein kommunales Rechenzentrum. In einigen Aufgabenbereichen gibt es Kooperationen in Form einer interkommunalen Zusammenarbeit mit den Nachbarstädten Erkrath und Monheim. Nach dem gegenwärtigem Stand gibt es seitens der Stadt Hilden keine strategischen Bestrebungen, die örtliche IT an eine Datenzentrale anzubinden.

Die zentrale Bereitstellung und Betreuung der IT ist in Hilden aufbauorganisatorisch als Sachgebiet dem Haupt- und Personalamt angegliedert.

Der zentralen IT sind derzeit 14 Mitarbeiter mit 12,15 vollzeitverrechneten Stellen zugeordnet. Wir werden nachfolgend detailliert darstellen, wie sich die Stellenanteile auf von uns definierte IT-Aufgabenbereiche verteilen.

Vorbemerkung zu den Prüfungsergebnissen

Grundsätzlich halten wir es für erstrebenswert, die IT in den nordrhein-westfälischen Städten, Gemeinden und sonstigen Gebietskörperschaften nicht nur in Bezug auf ihr jeweiliges Aufwandsniveau zu vergleichen, sondern auch deren Wirtschaftlichkeit im engeren Sinne - d.h. als Verhältnis von Input und Output, von Aufwand und Nutzen, von Kosten zur Leistungen - zu betrachten und zu bewerten. Dies zu leisten stellt im Bereich öffentlicher Güter eine besondere Herausforderung dar, weil die Outputseite sich in aller Regel einer monetären Bewertung entzieht. Daher können wir die genannte mittel- bis langfristige Zielsetzung im Rahmen dieser Prüfung nur im Ansatz verfolgen, leisten aber bereits damit einen wichtigen Beitrag zur Schaffung von Transparenz in der IT-Landschaft im öffentlich-rechtlichen Bereich.

Ausgangspunkt unserer Bewertungen zur Wirtschaftlichkeit ist ein Kennzahlenvergleich. Dabei basiert die Betrachtung im Prüfgebiet Informationstechnologie auf den Kennzahlen

- IT-Aufwendungen je Einwohner und
- IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung.

Der von uns gewählte Ansatz basiert auf der Grundannahme, dass die elektronische Verarbeitung von Informationen ein hohes, teilweise auch explizit definiertes[2] Maß an Sicherheit erfordert, um diese Daten vor Verlust, ungewollter Veränderung, unberechtigtem Zugriff durch Dritte und anderen Risiken zu schützen. Dies gilt selbstverständlich auch und insbesondere für den kommunalen Sektor, in dem nahezu ausnahmslos alle zu verarbeitenden Informationen die Eigenschaft personenbezogener Daten im Sinne der datenschutzrechtlichen Bestimmungen aufweisen.

Zwar lässt sich keine Aussage darüber treffen, ob die Aufgabe, ordnungsgemäß und sachgerecht IT für die Verwaltung der Stadt Hilden bereitzustellen und zu betreuen, mit dem geringsten Mitteleinsatz - also in konsequenter Umsetzung des Minimalprinzips[3] - erfüllt wird.

[2] Vgl. beispielsweise die technischen, organisatorischen, personellen und infrastrukturellen Maßnahmen in den Empfehlungen des BSI-Grundschutzkatalogs.

[3] Grundsätzlich lässt die Erfüllung der Aufgabe auch eine Orientierung an der anderen Variante des Wirtschaftlichkeitsprinzips, nämlich am Maximalprinzip, zu. In diesem Fall

Indem wir aber in relativ großer Detailtiefe eine Analyse der sicherheitsrelevanten Leistungsmerkmale durchführen, sind wir in der Lage, die Wirtschaftlichkeit der IT unter diesem elementaren Aspekt zu bewerten. So können wir individuell für die Stadt Hilden darstellen, ob das ermittelte Aufwandsniveau im interkommunalen Vergleich mit dem Leistungsniveau in Bezug auf eine sichere, ordnungsgemäße und sachgerechte Bereitstellung und Betreuung der IT korrespondiert oder ob signifikante Abweichungen erkennbar sind.

In der nachfolgenden Darstellung der Ergebnisse im Überblick haben wir zusammengefasst, zu welcher Einschätzung wir in Bezug auf das Verhältnis von Aufwand und Leistungsqualität der IT in der Stadt Hilden gelangt sind.

wäre bei vorgegebenem Mitteleinsatz das größtmögliche Leistungsniveau anzustreben. In der Realität wird allerdings faktisch meist eine Iteration stattfinden, da sich Mitteleinsatz und Ergebnis im Regelfall gegenseitig beeinflussen.

Ergebnisse im Überblick

Unter dem Gesichtspunkt der IT-Aufwendungen positioniert sich die Stadt Hilden im Vergleich der 21 bisher in die Prüfung einbezogenen Kommunen bei der Kennzahl *IT-Aufwendungen je Einwohner* recht ungünstig; die Aufwendungen überschreiten deutlich den Mittelwert. Hilden liegt hier in einer Rangfolgenbetrachtung auf dem vorletzten Platz. Eine Betrachtung der *IT-Aufwendungen je Arbeitsplatz mit IT–Ausstattung* relativiert das Ergebnis: Hier unterschreitet die Stadt Hilden den Mittelwert um mehrere Hundert Euro.

Diese Divergenz zwischen den Kennzahlenergebnissen kommt im Wesentlichen dadurch zustande, dass die Stadt im Vergleich zu den anderen geprüften Kommunen recht viele Bildschirmarbeitsplätze je tausend Einwohner einsetzt, so dass die IT-Gesamtaufwendungen auf eine größere Verteilungsmasse verrechnet werden.

Den Aufwendungen steht nach den von uns gewonnenen Erkenntnissen allerdings ein überdurchschnittlich hohes Leistungsniveau im Bereich der IT-Sicherheit und auch des IT-Managements, namentlich der betriebswirtschaftlichen Steuerung in der zentralen IT gegenüber.

Die Standortbestimmung in Hilden zeigt, dass die von der Stadt vollständig in Eigenregie betriebene IT-Infrastruktur technisch funktional ist und im interkommunalen Vergleich der bisher untersuchten Kommunen derzeit einen Spitzenplatz einnimmt. Mit den aktuellen Entwicklungen im Bereich des Sicherheitsmanagements und der Notfallvorsorge hat die Stadt Hilden sogar das Potenzial zu einem „Best Practice".

Der zentrale Serverraum der Stadt Hilden (Kellergeschoss) ist sehr funktional und unter Sicherheitsaspekten im interkommunalen Vergleich, auf einem auffallend hohen Niveau.

Der Sicherheitsleitlinien stellen ein sehr positives und nachahmenswertes Beispiel dar. In diesem Zusammenhang ist die Orientierung der IT am Grundschutzhandbuch des BSI der richtige Weg. Das Ziel, eine Arbeitsgruppe zum IT- Sicherheitsmanagement einzurichten, stellt ein weiteres positives Beispiel zur Erreichung der Sicherheitsziele dar.

Im Übrigen ergeben sich die noch möglichen Optimierungspotenziale aus den Checklisten, die als Anlage dem Bericht beigefügt sind.

Als Gesamtergebnis halten wir positiv fest, dass das Verhältnis der ermittelten Aufwendungen zum Leistungsniveau noch angemessen ist und die Bereitstellung und Betreuung von IT in Hilden insofern nicht unwirtschaftlich erfolgt.

In diesem Zusammenhang muss die gesamte finanzwirtschaftliche Situation einer Kommune gesehen werden: So lassen sich der Stadt Hilden kostenintensive hohe Standards eher zugestehen als einer Kommune, die den Restriktionen der Haushaltssicherung unterworfen ist. Gleichwohl zeigt insbesondere die relativ gute personelle Ausstattung des IT-Bereichs in Verbindung mit den hohen Aufwendungen je Einwohner, dass sich die Stadt Hilden zumindest mittelfristig mit der Frage auseinander setzen sollte, welche Optimierungsmöglichkeiten sich hinsichtlich der Wirtschaftlichkeit im IT-Bereich erschließen lassen.

Ergebnisse im Einzelnen

IT-Aufwendungen

Grundlagen der Datenerhebung

Um die Aufwendungen, die in den nordrhein-westfälischen Städten und Gemeinden im Zusammenhang mit der Bereitstellung und Betreuung der IT entstehen, einem interkommunalen Vergleich unterziehen zu können, legen wir einheitliche Maßstäbe und Methoden an. Grundsätzlich fließen in die Kennzahlenbildung Ausgabe- bzw. Aufwandsgrößen ein, die valide und rechtlich verbindlich sind.

Vor dem Hintergrund des Systemwechsels im kommunalen Rechnungswesen werden wir in Anlehnung an die Begrifflichkeiten des NKF in der Kennzahlenbildung künftig 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.

Sachaufwendungen

Als Datengrundlage zur Ermittlung der Sachaufwendungen ziehen wir die Ergebnisse der Haushaltsrechnungen bzw. Jahresabschlüsse aus dem Betrachtungszeitraum 2005 bis 2008 heran. Daraus extrahieren wir die Wertgrößen, die unmittelbaren Bezug zur IT haben. Soweit in Einzelfällen im Zuge der NKF-Umstellung ein vollständiger bzw. testierter Jahresabschluss aus dem Betrachtungszeitraum noch nicht vorliegt, greifen wir auf vorläufige Ergebnisse oder auf Daten aus der internen Kostenrechnung zurück und plausibilisieren diese hinreichend. Für die Haushaltsjahre, in denen noch nach kameralen Grundsätzen gebucht worden war, arbeiten wir mit Hilfsrechnungen, um trotz des Wechsels zur NKF-Systematik zu Werten zu gelangen, die weitgehende Analogie zur Ergebnisrechnung des NKF aufweisen.

Personalaufwendungen

Die Personalaufwendungen leiten wir aus verschiedenen Gründen nicht aus den tatsächlichen Haushaltsdaten ab. In der kommunalen Praxis finden wir eine Vielzahl von Varianten aufbauorganisatorischer Konzepte vor. Die nur auf den ersten, oberflächlichen Blick ausreichende Beschränkung auf die Organisationseinheit „zentrale IT" würde wegen der unterschiedlichen Gegebenheiten in den Städten und Gemeinden zu einem methodisch unzulänglichen interkommunalen Vergleich führen.

Daher haben wir für die Ermittlung des Personalaufwands im IT-Bereich sowie für die Betrachtung der Stellenausstattung und Aufgabenstruktur einen zweistufigen Ansatz gewählt:

Im ersten Schritt richten wir den Fokus auf die rein aufbauorganisatorische Ebene und ermitteln die vollzeitverrechneten Stellen in der IT-Abteilung.

Im zweiten Schritt differenzieren wir die Betrachtung, indem wir die funktionale Ebene in den Vordergrund stellen und anhand eines von uns festgelegten Kriterienkatalogs ermitteln, welche Arten von originären oder auch lediglich peripheren IT-Aufgaben in der jeweiligen Kommune wahrgenommen werden und in welchen Organisationsbereichen dies geschieht. Dabei verlassen wir also bewusst die Betrachtung der zentralen IT und ermitteln innerhalb der Gesamtverwaltung, ob und in welchem Umfang originäre IT-Aufgaben dezentral bearbeitet werden.

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.

Als Informationsgrundlage dienen uns für die Stellen der zentralen IT grundsätzlich die aktuellsten vorliegenden Stellen- bzw. Arbeitsplatzbeschreibungen. Zur Ermittlung dezentraler Stellenanteile führen wir nach einer Vorabklärung, welche Mitarbeiterinnen und Mitarbeiter in der Gesamtverwaltung für dezentrale IT-Aufgaben in Betracht kommen, im Regelfall kurze Interviews zur Feststellung von Art und Umfang der Aufgabe.

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[4]. 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.

[4] Diese Werte werden in der Regel jährlich ermittelt und in den KGSt-Berichten "Kosten eines Arbeitsplatzes" veröffentlicht.

Ergebnisse der Datenerhebung

Die Ergebnisse der Datenerhebung sowie die Bezugsgrößen zur Kennzahlenbildung sind nachfolgend dargestellt. Wegen der oben erläuterten unterschiedlichen Herangehensweise bei der Ermittlung und Berechnung der Grundlagen für die Kennzahlenbildung trennen wir die Sach- und Personalaufwendungen zunächst in der Übersicht; im Rahmen der Personalaufwendungen thematisieren wir zudem im Detail die Stellensituation im IT-Bereich.

Sachaufwendungen

Aus den nachfolgenden Tabellen ist ersichtlich, welche Haushaltsergebnisse (hier: nur Sachausgaben bzw. –aufwendungen) in die Kennzahlenbildung einfließen:

Ergebnis der Jahresrechnung 2005 und 2006 Verwaltungshaushalt in Euro		
	2005	**2006**
SN Sach- und Geschäftsausgaben	24.033	21.795
Wartung und Reparaturen	34.485	30.404
Softwarepflege (auch dezentral)	218.374	195.734
Nutzungsrechte Software (auch dezentral)[5]	8.633	12.640
Leasingkosten Hardware	193.450	193.450
Fortbildung TUIV/EDV (auch dezentral)	36.682	58.787
Sachkosten/Verbrauchsmaterial	41.092	47.552
TUIV Beratungsleistungen	39.562	47.478
Summe	596.312	607.840

[5] In den kameralen Haushaltsjahren wurden Ausgaben für die Beschaffung von Software unabhängig von ihrer Höhe (fälschlicherweise) im Verwaltungshaushalt veranschlagt und gebucht. Da es sich bei der HHSt. „Nutzungsrechte Software" nahezu ausschließlich um Softwarebeschaffung handelt, wurde in dieser tabellarischen Darstellung nur ein Anteil von 10% als Ergebnisse des Verwaltungshaushalts ausgewiesen; ein geschätzter Anteil von 90% fällt unter die in der Haushaltsrechnung für die Jahre 2005 und 2006 faktisch nicht vorhandene HHSt. „Beschaffung Software" im Vermögenshaushalts. Diese wurden in der nachfolgenden Tabelle fiktiv gebildet, um die Größenordnung der Software-Investitionen annähernd korrekt darzustellen.

Ergebnis der Jahresrechnung 2005 und 2006 Vermögenshaushalt in Euro		
	2005	**2006**
Beschaffung Hardware und technischer Anlagen (zentral und dezentral)	87.071	168.731
Beschaffung Software (zentral und dezentral)[6]	77.698	113.759
Summe	164.769	282.491

Aufwendungen für IT 2007 und 2008 in Euro Jahresabschluss der Ergebnisrechnung		
	2007	**2008**
Aufwendungen für Unterhaltung der Maschinen und technischen Anlagen	28.797	18.435
Sonstige Aufwendungen für Sachleistungen	12.192	5.058
Aufwendungen für Verbrauchsmaterial	24.568	38.215
Unterhaltung der Betriebs-/Geschäftsausstattung und Sonstige Aufwendungen für Dienstleistungen	314.019	321.658
Abschreibungen auf immaterielle Vermögensgegenstände	113.790	123.836
Abschreibungen auf Gebäude, Aufbauten/Betriebsv.	1.632	0
Abschreibungen auf technische Anlagen	34.351	24.995
Abschreibungen auf Betriebs-/Geschäftsausstattung	95.696	66.178
Abschreibungen auf geringwertige Wirtschaftsgüter	36.872	15.259
Aufwendungen für Aus- und Fortbildung, Umschulung	24.649	16.253
Mieten für Telekommunikationseinrichtungen	12.339	25.487
Leasing	41.272	98.363
Sonstige Aufwendungen für die Inanspruchnahme von Rechten/Dienstleistungen	3.094	326
Zeitschriften, Fachliteratur, Gesetzesblätter	955	1.410
Aufwendungen aus der Veräußerung von beweglichem Vermögen (> 410 Euro)	66.723	7.132
Aufwendungen für Sach- und Dienstleistungen Telekommunikation	32.986	44.389
Bilanzielle Abschreibungen Telekommunikation	16.972	16.148
Mieten Telekommunikationseinrichtungen	89.032	22.310
Summe	949.938	845.451

[6] Siehe Anmerkungen in Fußnote 5.

Stellenausstattung und Personalaufwendungen für IT-Aufgaben

Wie im Abschnitt „Grundlagen der Datenerhebung" erläutert, fließen im Bereich der IT-Personalaufwendungen nicht die tatsächlichen Haushaltsdaten in den interkommunalen Vergleich ein. Wir differenzieren bezüglich der personellen Ausstattung die Betrachtung, so dass letztendlich nur die funktionale Ebene im Vordergrund steht. Aus der Zahl der so ermittelten vollzeitverrechneten Stellen ergeben sich nach Gewichtung mit den tatsächlichen Besoldungs- bzw. Entgeltgruppen die in die Kennzahlenbildung einfließenden Personalaufwendungen. Dabei beschränken wir uns auf das aktuellste Jahr des Betrachtungszeitraums, also 2008.

Das Ergebnis unserer Erhebung ist nachfolgend tabellarisch aufbereitet. Diese Übersicht dokumentiert sowohl die inhaltlichen Merkmale, aufgrund derer wir eine Differenzierung vornehmen, als auch die auf die Aufgabenbereiche entfallenden Stellenanteile und die damit verbundenen, auf Basis der jeweils aktuellen KGSt-Pauschalen berechneten Personalaufwendungen:

Stellenanteile und Personalaufwendungen für IT-Aufgaben		
	vollzeitverr. Stellenanteile	Personalaufwand in Euro
Stellenanteile für originäre IT-Aufgaben in zentraler IT dazu zählen: - IT-Management - Fachanwendungsbetreuung - Technische Betreuung	**9,65**	**522.382**
dezentrale Stellenanteile für originäre IT-Aufgaben Hier sind Stellenanteile erfasst, die außerhalb der zentralen IT Aufgaben aus den oben genannten Bereichen wahrnehmen.	**0,25**	**16.828**
Stellenanteile für originäre IT-Aufgaben (funktionale Ebene) gesamt	**9,90**	**539.210**
Nachrichtlich:		
Anteil für sonstige Aufgaben, die der zentralen IT zugeordnet sind Soweit in der zentralen IT Aufgaben wahrgenommen werden, die nicht zum originären IT-Aufgabenbereich gehören, werden diese abgegrenzt. Darunter fällt auch die Betreuung des pädagogischen Bereichs in den Schulen.	**2,50**	**143.230**[7]
Stellen in der zentralen IT (aufbauorganisatorische Ebene) gesamt	**12,15**	**665.612**

[7] Brutto-Personalaufwand; davon sind rund 72.000 Euro abzusetzen, die von der Stadt Erkrath für die Betreuung der dortigen Schulen durch die IT der Stadt Hilden erstattet werden und die tatsächliche Personalkostenbelastung entsprechend reduzieren.

Für die Stadt Hilden haben wir demnach innerhalb der zentralen IT-Abteilung 9,65 vollzeitverrechnete Stellenanteile ermittelt, die auf die Wahrnehmung originärer IT-Aufgaben entfallen. In den meisten bisher geprüften mittleren kreisangehörigen Städten haben wir neben den Stellen in der zentralen IT weitere Stellenanteile für die dezentrale Erledigung von Aufgaben aus dem Bereich der Fachanwendungs- und Technikbetreuung identifiziert.

Im konkreten Fall der Stadt Hilden haben wir verwaltungsweit 0,25 dezentrale Stellenanteile für die Erledigung originärer IT-Aufgaben ermittelt. Die Bereitstellung und Betreuung von IT ist in Hilden also nicht vollständig zentralisiert ausgerichtet.

Mit dieser Feststellung verbinden wir zunächst keine Wertung. Es ist eine individuelle Entscheidung der Verwaltungsleitung, ob dem Gedanken eines Vollservices durch die zentrale IT gefolgt wird oder ob Expertenwissen in Bezug auf bestimmte Fachanwendungen um zumindest eingeschränkte Administratorenrechte ergänzt wird und damit gleichzeitig die IT-Mitarbeiter entlastet werden. Das Gleiche gilt, soweit dezentrale Stellenanteile auf die technische Betreuung von Hardware, etwa die Wartung von Etagendruckern, entfallen.

Die Stadt Hilden weist mit 45,3 betreuten Bildschirmarbeitsplätzen je vollzeitverrechneter IT-Stelle[8] eine relativ niedrige Betreuungsquote im Vergleich der bisher in dieser Prüfrunde von uns betrachteten Städte auf. Die Betreuungsquote liegt uns derzeit für 17 von bisher insgesamt 21 geprüften Städten vor und liegt in einem Spektrum von rund 27 bis 86 betreuten Bildschirmarbeitsplätzen.

Beim interkommunalen Vergleich der Betreuungsquoten muss allerdings berücksichtigt werden, dass die mittleren kreisangehörigen Städte in sehr unterschiedlicher Ausprägung IT-Leistungen ausgelagert haben. In den bisher geprüften Kommunen finden wir die gesamte Bandbreite von einer vollständig autonom betriebenen IT bis hin zu einer umfangreichen Auslagerung mit Tendenz zum externen IT-Vollservice. Im Rahmen dieser Prüfung ist es allerdings nicht möglich, die unterschiedlichen Auslagerungsgrade präzise zu ermitteln und gewissermaßen als Gewichtungsfaktor in die Betreuungsquote einfließen zu lassen. Dies würde eine de-

[8] Bei funktionaler Betrachtung; Bildschirmarbeitsplätze = Arbeitsplätze mit IT-Ausstattung im Bereich der Kernverwaltung und des Sondervermögens, soweit diese von der Stadt finanziert und von der zentralen IT betreut werden; Schulungsrechner, Rechner im pädagogischen Bereich der Schulen, Selbstbedienungsterminals usw. zählen nicht dazu.

taillierte Bewertung nicht nur der vertraglich vereinbarten Leistungen, sondern auch des faktischen Serviceumfangs und der Leistungsqualität erfordern, damit beurteilt werden könnte, welcher Stellenbedarf zur Erfüllung der Gesamtaufgabe objektiv in der örtlichen IT verbleiben würde.

Für die Stadt Hilden können wir feststellen, dass die Leistungsstandards in der vollkommen autonom betriebenen IT unter vielerlei Aspekten überdurchschnittlich hoch sind. Zudem finden wir in Hilden die Ausnahmesituation vor, dass eine – wenngleich nicht mehr aktuelle, weil aus dem Jahr 2004 stammende – Mitarbeiterbefragung vorliegt. Seinerzeit wurde unter anderem die Zufriedenheit mit der technischen Ausstattung und auch explizit die Servicequalität der zentralen IT in Bezug auf Anwenderbetreuung etc. abgefragt. Insbesondere die Einzelfragen, die sich auf den Bereich der Unterstützung durch die IT-Mitarbeiter bezogen, wurden recht positiv beantwortet.

In der Summe lässt sich feststellen, dass die personelle Ausstattung zwar nicht eben restriktiv ausfällt, angesichts der vollkommenen Autonomie und des von uns im Rahmen der Prüfung feststellbaren Gesamt-Leistungsniveaus der IT in Hilden allerdings auch nicht unangemessen erscheint.

Feststellung

Die IT wird in der Stadt Hilden in weitgehender Zentralisierung mit geringfügiger Unterstützung durch dezentrale Stellenanteile und ohne Auslagerung von Aufgaben an eine Datenzentrale betrieben.

Die im Vergleich niedrige Betreuungsquote, also quantitativ relativ hohe Personalausstattung, geht einher mit einem recht hohen Leistungsniveau, das sich nicht nur auf die technische Ausstattung erstreckt, sondern sich beispielsweise auch in einer aktiven betriebswirtschaftlichen Steuerung zeigt, die naturgemäß Personalressourcen erfordert.

Empfehlung

Im Rahmen der Prüfung haben wir neben der quantitativ ermittelten Betreuungsquote keine Indikatoren dafür vorgefunden, dass die Personalausstattung unangemessen hoch ist.

Gleichwohl sehen wir angesichts allgemein enger finanzieller Spielräume für die Kommunen auch in einer Stadt wie Hilden, die nicht den Restriktionen der Haushaltssicherung unterliegt, die Notwendigkeit, eine tendenziell hohe Personalausstattung kritisch zu beobachten. Dies gilt aus unserer Sicht auch dann, wenn gegenwärtig kein Handlungsbedarf in Richtung einer systematischen Aufgabenkritik besteht.

Interkommunaler Kennzahlenvergleich

Die im vorherigen Kapitel für die Stadt Hilden hergeleiteten Aufwendungen fließen mit folgenden Summen in den Kennzahlenvergleich ein:

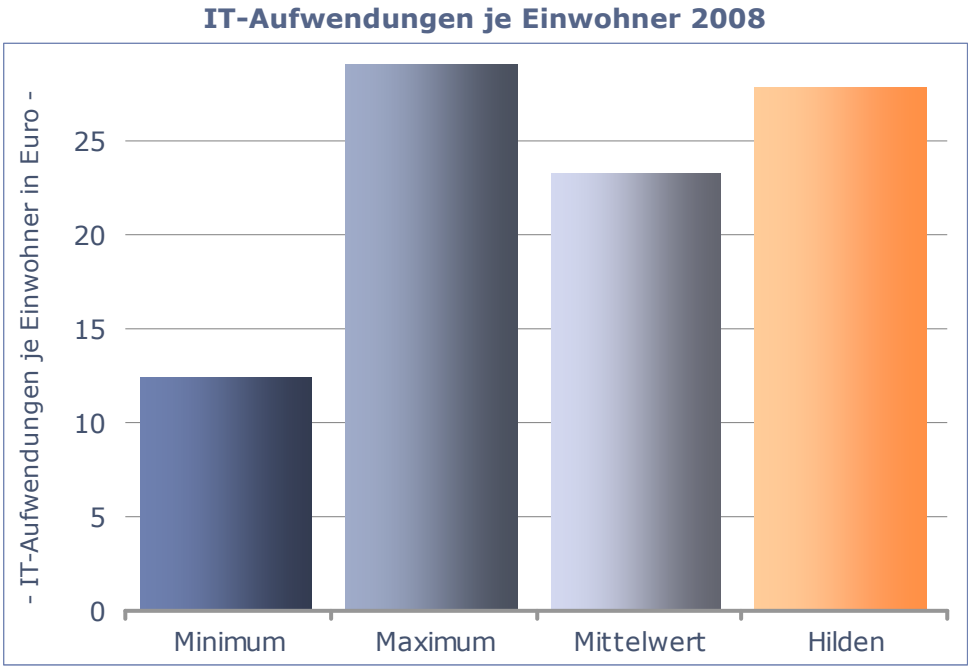
Grunddaten zur Kennzahlenbildung (Aufwendungen in Euro)	
IT-Sachaufwendungen (arithmetisches Mittel 4 Jahre)	861.700
Personalaufwendungen für originäre IT-Aufgaben (ermittelt nach KGSt-Pauschalen)	539.210
Sachkostenpauschale und Gemeinkostenzuschlag nach KGSt-Empfehlung	161.302
Gesamtaufwendungen IT	**1.562.212**

Zunächst stellen wir zur Kennzahlenbildung 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 Endprodukte vorgelagerter Leistungen – wie auch der Informationstechnologie - geht.

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.[9]

Als Bezugsgrößen legen wir neben den in den abgeschlossenen Prüfungen festgestellten Minimal- und Maximalwerten den einfachen Mittelwert als Orientierungsgröße zugrunde. Wie sich die Stadt Hilden hinsichtlich ihrer IT-Aufwendungen in der einwohnerbezogenen Betrachtung positioniert, geht aus nachstehender Grafik hervor.

[9] 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% für allgemeine (verwaltungsweite) Leistungen sowie für amts- bzw. fachbereichsinterne Leitungsaufgaben, insgesamt also einen Zuschlag für „Overhead"-Gemeinkosten in Höhe von 20%.



Vergleichsbasis: 21 Kommunen

IT-Aufwendungen je Einwohner			
Minimum	Maximum	Mittelwert	**Hilden**
12,29 Euro	29,02 Euro	23,13 Euro	**27,77 Euro**

Bei der auf Einwohner bezogenen Kennzahl positioniert sich die Stadt Hilden mit 27,77 Euro deutlich oberhalb des Mittelwertes und weist unter den bisher in die Prüfung einbezogenen Kommunen der gleichen Größenklasse die zweithöchsten IT-Aufwendungen je Einwohner auf.

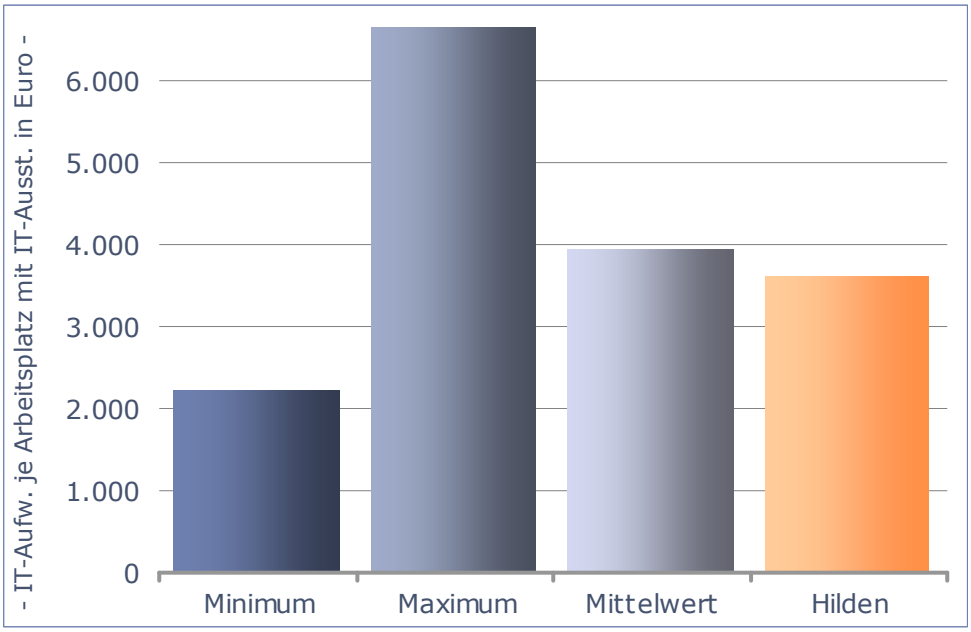
Neben der Kennzahl mit Einwohnerbezug nehmen wir auch die Betrachtung der IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung in den Blick. Die daraus generierte Kennzahl liefert wichtige Informationen für Analysen im Rahmen interner Steuerungsprozesse.

Bei der Interpretation und Wertung dieser Kennzahl muss jedoch beachtet werden, dass hier die Anzahl der Bildschirmarbeitsplätze im Verhältnis zu der Einwohnerzahl eine maßgebliche Rolle spielt. Die Positionierung im interkommunalen Vergleich wird durch eine – bezogen auf die Einwohner - niedrige Anzahl von Bildschirmarbeitsplätzen negativ und durch eine zahlenmäßig hohe technische Ausstattung positiv beeinflusst, weil die IT-Aufwendungen auf eine kleinere bzw. größere Verteilungsmenge fließen.

Eine wichtige Rolle spielt zudem die Frage, wie groß der Fixkostenanteil an den Gesamtkosten ist. Kriterium für die Zuordnung einer bestimmten Kostengröße bzw. Kostenart zu Fixkosten oder variablen Kosten ist zunächst die Abhängigkeit von der Ausbringungs- oder Leistungsmenge; dabei hängt es aber letztlich entscheidend vom Zeitfaktor - genauer: von der Länge des Planungs- und Entscheidungszeitraums – ab, ob Fixkosten oder variable Kosten vorliegen. Insofern entbindet die Tatsache, dass Teile der Kosten und des Aufwands zunächst als nicht veränderbar erscheinen, die Kommune nicht davon, diese Anteile zu ermitteln und den Möglichkeiten einer aktiven betriebswirtschaftlichen Steuerung zu unterwerfen.

Die Positionierung der Stadt Hilden hinsichtlich ihrer IT-Aufwendungen in der arbeitsplatzbezogenen Betrachtung zeigt die nachstehende Grafik.

IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung 2008



Bezugsgröße ist das arithmetische Mittel der Arbeitsplätze mit IT-Ausstattung im Betrachtungszeitraum in der Kernverwaltung und in den Sondervermögen (= 437).

IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung			
Minimum	Maximum	Mittelwert	**Hilden**
2.194 Euro	6.630 Euro	3.930 Euro	**3.575 Euro**

Bei der auf Arbeitsplätze mit IT-Ausstattung bezogenen Kennzahl liegt die Stadt Hilden mit 3.575 Euro mehrere Hundert Euro unter dem Mittelwert und positioniert sich damit wesentlich positiver als bei der Kennzahl mit Einwohnerbezug.

Im Vergleich wird deutlich, dass die Kennzahlen abhängig von der Bezugsgröße Einwohner bzw. Bildschirmarbeitsplatz im konkreten Fall der Stadt Hilden ein stark gegenläufiges Ergebnis liefern. Zwischen diesen Ergebnissen besteht deshalb keine Proportionalität, weil als rechnerischer Faktor die Anzahl der Bildschirmarbeitsplätze im Verhältnis zur Einwohnerzahl, oder anders ausgedrückt, die relative Größe der Stadtverwaltung, entscheidend ist. In der Relation – dies zeigt der Abstand der Werte der Stadt Hilden zum jeweiligen Mittelwert – fällt das Resultat beim Arbeitsplatzbezug besser aus. Dies ist ein Indikator dafür, dass die Stadt mehr Bildschirmarbeitsplätze einsetzt als die Mehrheit der Vergleichskommunen.

Betrachten wir in diesem Zusammenhang die Quote der Bildschirmarbeitsplätze je tausend Einwohner (BSAP/1000 EW), so bestätigt sich dieses Bild. Die Stadt Hilden erreicht hier eine recht hohe Quote von 7,8 BSAP/1000 EW; der Mittelwert der bisher geprüften Kommunen liegt bei rund 6,2 BSAP/1000 EW. Fünf Kommunen in diesem Vergleich setzen noch mehr Bildschirmarbeitsplätze je Einwohner ein. Den Minimalwert erreicht eine Stadt, die auf tausend Einwohner lediglich geringfügig mehr als 4,0 Arbeitsplätze mit IT-Ausstattung vorhält.

Wir verbinden mit der Nennung dieser Zahlenwerte keine Bewertung; sie dienen hier lediglich zur Erläuterung, aus welchen Gründen zwischen den von uns ermittelten Kennzahlen kein festes Größenverhältnis besteht. Bei einem angenommenen und auch allgemein feststellbaren Durchdringungsgrad von annähernd 100%[10] ist die Quote der Bildschirmarbeitsplätze je tausend Einwohner zwar ein wichtiger Indikator für die personalwirtschaftliche Gesamtsituation einer Kommunalverwaltung. Gleichwohl liegen selbst innerhalb des Segments der mittleren kreisangehörigen Städte die Einwohnerzahlen in einem recht breiten Spektrum; durch dieses Einwohnerspektrum bedingt sind die Unterschiede in den Strukturen und Aufgaben teilweise erheblich. Insofern ist es nachvollziehbar, dass die Stadt Hilden als eine der größten Städte

[10] Prämisse: In einer modernen Verwaltung liegt im Bereich der klassischen Büroarbeitsplätze – gleich in welchem Fachbereich – der Durchdringungsgrad bei annähernd 100%, d.h. praktisch jeder Arbeitsplatz verfügt über IT-Ausstattung.

innerhalb des in den Vergleich einbezogenen Segments eine auf tausend Einwohner bezogen eher große Verwaltung besitzt und dass die IT-Aufwendungen naturgemäß absolut, aber eben auch je Einwohner höher ausfallen als in deutlich kleineren Kommunen.

Vor diesem Hintergrund legen wir den Betrachtungsschwerpunkt auf die Frage, welchen Aufwendungen auf einen einzelnen Arbeitsplatz mit IT-Ausstattung entfallen und stellen fest, dass deren Höhe im interkommunalen Vergleich tendenziell niedrig ist. Dies gilt umso mehr, als wir das Leistungsniveau im Bereich des IT-Managements, hier insbesondere der betriebswirtschaftlichen Steuerung und der IT-Sicherheit in die Betrachtung einbeziehen und zu dem Ergebnis kommen, dass die Aufgabe IT in Hilden zwar nicht mit geringem, aber der Art der Aufgabenerfüllung durchaus angemessenem Aufwand wahrgenommen wird.

Feststellung

Die IT-Aufwendungen der Stadt Hilden liegen im interkommunalen Vergleich beim Einwohnerbezug deutlich über, beim Arbeitsplatzbezug dagegen unter dem Mittelwert.

Diese relativ starke Divergenz erklärt sich aufgrund der Tatsache, dass die Stadt im Vergleich der bisher geprüften Kommunen eine tendenziell hohe Zahl von Arbeitsplätzen mit IT-Ausstattung auf tausend Einwohner einsetzt.

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 stellen:

- Verfügt die Stadt Hilden 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 Hilden 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.

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

Im Rahmen der Prüfung sind uns die angeforderten Unterlagen und Informationen jeweils umgehend, vollständig und in umfassend nachvollziehbar aufbereiteter Form zur Verfügung gestellt worden.

Mit Umstellung des kommunalen Haushaltes auf die Systematik des Neuen Kommunalen Finanzmanagements (NKF) im Jahre 2007 wurden zwei getrennte Kostenstellen für den IT-Kernbereich und den Bereich Telekommunikation gebildet. Die eingerichtete Kontenstruktur ist differenziert und für Planungs- und Steuerungszwecke hinreichend aussagefähig. Die Stadt Hilden hat innerhalb der zentralen IT ein Controlling-Konzept implementiert, das hinsichtlich seiner fachlichen Ausgestaltung im Vergleich der bisher geprüften Kommunen derselben Größenklasse auf einem sehr hohen Niveau liegt.

Die interne Kostenverrechnung erfolgt auf Ebene der den Endanwendern bereitgestellten Hardware, d.h. im Wesentlichen der PCs und Notebooks, sowie der eingesetzten Fachanwendungen. In die Vollkostenrechnung fließen unter anderem Lizenz- und Wartungsgebühren, Sachkosten für die anteilige Servernutzung sowie Personalkostenanteile für IT-Management, technische Betreuung und Anwendungsbetreuung mit ein. Die für die Fachämter erbrachten IT-Leistungen werden quartalsweise abgerechnet.

Soweit es möglich und praktikabel ist, werden differenzierte Verrechnungsschlüssel bzw. Gewichtungsfaktoren zu Grunde gelegt, die Art und Umfang der Nutzung einer Software auf Anwenderebene berücksichtigen. So wird bei der Kostenverrechnung der großen Verfahren *INFOMA, evITA, MESO, EurOWiG* und *PROSOZ* bei den Arbeitsplätzen, die jeweils nahezu den gesamten Funktionalitätsumfang nutzen, ein wesentlich höherer Gewichtungsfaktor angesetzt als dort, wo sich die Softwarenutzung auf Leserechte beschränkt.

Im Ergebnis erreicht die IT in der Stadtverwaltung Hilden damit eine außerordentlich hohe Kostentransparenz und schafft damit eine entscheidende Voraussetzung, um aktiven Einfluss auf die Höhe der IT-Kosten zu nehmen.

Zudem existiert ein Kennzahlensystem, das ursprünglich interkommunalen Vergleichen innerhalb der kreisangehörigen Kommunen diente, deren praktische Relevanz aber aus unterschiedlichen Gründen abgenommen hat; inzwischen sind die Kennzahlen in der zentralen IT weiterentwickelt worden und werden vorrangig für interne Steuerungszwecke eingesetzt.

Lediglich die im NKF vorgesehene Definition von Zielen mit Steuerungsfunktion, deren Erfüllungsgrad also messbar sein muss, ist noch nicht umgesetzt. So ließe sich beispielsweise unter Einbeziehung individueller Anforderungen in Hilden das Ziel „wirtschaftlicher Einsatz von Hard- und Software" definieren und auf Basis des vorhandenen Kennzahlensystems messen und fortschreiben.

Feststellung

Die in der zentralen IT der Stadt Hilden implementierten betriebswirtschaftlichen Methoden liegen auf einem im kommunalen Vergleich dieser Größenklasse hohen Niveau; die damit erreichte

Kostentransparenz ist aus unserer Sicht vorbildlich.

Die Instrumente der Kostenrechnung werden fachlich sinnvoll und zielführend eingesetzt. Damit unterstützen sie die sachgerechte und wirtschaftliche Aufgabenerfüllung innerhalb der zentralen IT und leisten auf der Kostenebene einen nennenswerten Beitrag zur Gesamtsteuerung der Verwaltung.

Ein Kennzahlensystem ist vorhanden und in erster Linie zur internen Steuerung praxisrelevant, ferner dient es Vergleichen unter den Kommunen des Kreises Mettmann. Lediglich die im NKF vorgesehene Definition messbarer operativer Ziele ist in Hilden noch nicht umgesetzt.

Insgesamt ist damit ein überdurchschnittlich gut ausgestaltetes finanzwirtschaftliches Steuerungsinstrumentarium vorhanden.

Empfehlung

Die aus unserer Sicht guten und sinnvoll eingesetzten betriebswirtschaftlichen Instrumentarien im IT-Bereich sollten auch weiterhin gepflegt werden. Gegebenenfalls könnte, unter sorgfältiger Beachtung von Aufwand und Nutzen, eine bedarfsorientierte Erweiterung und Ergänzung angezeigt sein.

Die vorhandene Informationsqualität sollte intensiv mit der Zielsetzung einer aktiven Einflussnahme auf die Höhe der IT-Kosten genutzt werden.

Soweit – dies ließ sich im Rahmen der IT-Prüfung nicht thematisieren – in anderen Bereichen der Stadtverwaltung Hilden noch Entwicklungsbedarf hinsichtlich des Einsatzes betriebswirtschaftlicher Instrumentarien besteht, halten wir die Steuerung in der zentralen IT für einen geeigneten Orientierungsmaßstab für Methodeneinsatz und Steuerungsqualität.

IT-Sicherheit

Unser Prüfmodul IT-Sicherheit beschäftigt sich insbesondere mit den Bereichen Datensicherheit und soll darüber hinaus mögliche Risiken, die mit dem Betrieb der IT verbunden sind, identifizieren und aufzeigen. Im Rahmen dieses Moduls erfolgt eine summarische Gesamtbeurteilung. Ziel ist hierbei die Feststellung, ob den bestehenden Risiken in angemessenem und beherrschbarem Maße begegnet wird. Dabei spielt der Grad der technischen und organisatorischen Maßnahmen eine große Rolle, der in der geprüften Körperschaft eingeführt und umgesetzt wurde. Das Prüfmodul Datenschutz wird gesondert thematisiert.

Die Prüfungsaufgabe wird überwiegend unter Verwendung von Checklisten erledigt. Diese Checklisten wurden anhand anerkannter Kriterien des BSI[11] erarbeitet und sind in unterschiedliche Fragenkreise aufgeteilt.

Im Rahmen der Betrachtung der IT-Sicherheit werden im Detail die Bereiche

- IT-Infrastruktur
- IT-Anwendungen
- IT-Management

in den Blick genommen.

Die Betrachtung erfolgt im Dialog mit den Verantwortlichen für die IT-Organisationseinheiten.

Im kommunalen Raum sind verstärkt Tendenzen zu beobachten, die zu einer immer weiter ansteigenden Verselbstständigung von IT-Leistungen in den kommunalen Einrichtungen führen. Ohne dies in der Sache zu bewerten, steht jedoch eindeutig fest, dass Kommunen, die selbst Anbieter von IT-Leistungen für ihre Verwaltung sind, alle die mit der IT verbundenen Risiken auf ein beherrschbares Mindestmaß reduzieren müssen, sei es durch organisatorische und / oder durch technische Maßnahmen. Leider war aufgrund unserer bisherigen Erfahrungen jedoch festzustellen, dass gerade die Leitungsebene (Verwaltungsvorstand) oft nicht über bestehende Risiken bzw. Risikopotenziale informiert war. So-

[11] Bundesamt für Sicherheit in der Informationstechnik

mit ist es auch ein Ziel im Rahmen dieses Moduls, soweit erforderlich das Bewusstsein für bestehende Risiken zu stärken.

Allgemeine Sicherheitsanforderungen

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. Im Regelfall wird die Verantwortung auf den Fachbereich übertragen, der für die IT zuständig ist. Dazu sollte in den Körperschaften ein geeignetes Konzept vorliegen oder eingeführt werden, das den erforderlichen Grad an Informationssicherheit nachhaltig gewährleistet (Sicherheitskonzept).

Dieses Sicherheitskonzept soll eine Bewertung der Sicherheitsrisiken beinhalten, die aus dem Einsatz der IT resultieren. Daraus lassen sich dann technische und organisatorische Maßnahmen ableiten, um eine angemessene IT-Infrastruktur für die IT-Anwendungen zu gewährleisten sowie die ordnungsgemäße Abwicklung der IT-gestützten Geschäftsprozesse sicherzustellen.

IT-Systeme haben grundsätzlich die folgenden 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/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, HGB.

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. 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 nach folgenden Teilbereichen untergliedert:

- IT- Räumlichkeiten und IT- Infrastruktur- Aufbau
- Technische Ausstattung der Arbeitsplätze
- IT- Management (Konzepte und Dienstanweisungen)
- Backup und Archivierung
- Umsetzung Datenschutzgesetz.

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

Im Rahmen der Dokumentation des Prüfungsvorganges werden die Checklisten als Anlage zum Prüfbericht beigefügt.

Unterlagen und Ansprechpartner

Im Rahmen dieses Prüfmoduls lagen uns folgende Unterlagen vor:

- Allgemeine Dienstanweisung der Stadt Hilden
- Dienstanweisung für das Vergabewesen
- Dienstanweisung über die Organisation des Datenschutzes
- Dienstanweisung für den Einsatz der Informationstechnologie

- Dienstanweisung über die datenschutzmäßige Behandlung, Aufbewahrung und Beseitigung von Datenträgern
- Dienstanweisung zur Nutzung und Behandlung Elektronischer Post
- Dienstanweisung zur Nutzung der Internet-Dienste
- Dienstvereinbarung über die Einführung der alternierenden Tele-/Heimarbeit (aTH) bei der Stadt Hilden
- Datensicherungskonzept der Stadt Hilden
- IT- Sicherheitsleitlinie (Entwurfsfassung zu Beginn der Prüfung und beschlossene Fassung zum Prüfungsende)
- Netzwerkplan der Stadt Hilden
- Übersicht der SAN- Speicheraufteilung
- Darstellung Tape Libary (Bandlaufwerk).

Als Ansprechpartner standen uns folgende Personen zur Verfügung:

- Herr Kramer
- Frau Stein

Zentraler Ansprechpartner für die Prüfung war Herr Kramer.

Prüfungsmethode

Innerhalb dieses Prüfmoduls wurden die folgenden Prüfungsmethoden und -techniken - zum Teil im Stichprobenverfahren - eingesetzt:

- Interviews, systematisiert durch Checklisten
- Beobachtung von Verfahrensabläufen (Stichproben),
- Durchsicht von Unterlagen,
- Dokumentationsprüfung (Stichproben),

- Nachvollzug von Verfahrenabläufen (Stichproben)
- Analyse und ggf. Verwertung von Unterlagen Dritter
- Begehung der IT-Räume.

Fragenkreis „IT-Räume und Infrastrukturaufbau"

Zu diesem Fragenkreis haben wir folgende Teilbereiche betrachtet:

Serverraum, IT-Verkabelung, WLAN[12], Sicherheitsgateway (Firewall).

Der zentrale Serverraum der Stadt Hilden (Kellergeschoß) ist sehr funktional und unter Sicherheitsaspekten im interkommunalen Vergleich, auf einem auffallend hohen Niveau. Die Brandlöschvorrichtung (Gaslöschanlage) soll dabei nur als ein Beispiel hervorgehoben werden.

Die wichtigen Serversysteme sind, insbesondere unter Verwendung von Virtualisierungstechnologien, redundant ausgelegt. Außerdem ist eine Hochverfügbarkeitsumgebung über VMWare ESX und SAN- Technologie implementiert.

Auch die Netzwerkverteilung komplettiert diesen positiven Gesamteindruck.

Im Rahmen der Prüfung sind keine Sachverhalte identifiziert worden, die Empfehlungen führen.

[12] Wide Local Area Network

Fragenkreis „Technische Ausstattung der Arbeitsplätze/ Client-Umgebung“

Zu diesem Fragenkreis haben wir die Teilbereiche Allgemeine Client-Arbeitsplätze und mobile Arbeitmittel (Laptop/Notebooks) betrachtet.

Im Rahmen der Prüfung sind keine Sachverhalte identifiziert worden, die zu Empfehlungen führen.

Fragenkreis „IT-Management (Konzepte, Dienstanweisungen, Risikomanagement)“

Zu diesem Fragenkreis haben wir die Teilbereiche Sicherheitsmanagement, Sicherheitsorganisation, Notfallvorsorge, Personal, Virenschutz, Hard- und Softwaremanagement betrachtet.

Im Rahmen der Prüfung sind Sachverhalte identifiziert worden, die zu den nachfolgenden Empfehlungen führen.

Sicherheitsmanagement

Die sichere Verarbeitung von Informationen ist heutzutage für nahezu alle Behörden von existenzieller Bedeutung. Dabei reicht es für den Schutz der Informationen 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.

Feststellung

Bei der Stadt Hilden sind umfangreiche Maßnahmen im Rahmen eines Sicherheitsmanagements avisiert worden, insbesondere zur Implementierung von sicherheitsorganisatorischen Handlungen. Hierzu zählt u. a. die Einführung der Funktion eines Sicherheitsbeauftragten.

Leitlinie

Eine Sicherheitsleitlinie bestand zu Beginn der Prüfung in der Stadt Hilden im Entwurfsstatus und wurde im weiteren Verlauf der Prüfung vom Verwaltungsvorstand verabschiedet und mit Wirkung vom 15.10.2009 Kraft gesetzt.

Feststellung

Der vorliegenden Sicherheitsleitlinien stellen im Vergleich zu den bisher geprüften kreisangehörigen Kommunen ein sehr positives und nachamenwertes Beispiel dar. In diesem Zusammenhang ist die Orientierung am Grundschutzhandbuch des BSI der richtige Weg. Das Ziel, eine Arbeitsgruppe zum IT- Sicherheitsmanagement einzurichten, stellt ein sehr positives Beispiel für eine ämterübergreifende Zusammenarbeit zur Erreichung der Sicherheitsziele dar.

Organisationsstruktur für Informationssicherheit

Um einen IT-Sicherheitsprozess erfolgreich planen, umsetzen und aufrechterhalten zu können, muss eine geeignete Organisationsstruktur vorhanden sein. Es müssen also Rollen definiert sein, die die verschiedenen Aufgaben für die Erreichung der IT-Sicherheitsziele wahrnehmen. Außerdem müssen Personen benannt sein, die qualifiziert sind und denen ausreichend Ressourcen zur Verfügung stehen, um diese Rollen auszufüllen.

Die Art und Ausprägung einer IT-Sicherheitsorganisation hängt von der Größe, Beschaffenheit und Struktur der jeweiligen Institution ab. In jeder Institution sollte allerdings die Funktion des IT-Sicherheitsbeauftragten eingerichtet werden, der für alle IT-Sicherheitsbelange zuständig ist.

Bei der Stadt Hilden, ist im Rahmen der Verabschiedung und Einführung der Sicherheitsleitlinien, die Einrichtung der Funktion eines Sicherheitsbeauftragten vorgesehen.

Empfehlung

Wir empfehlen, die geplante Einführung eines Sicherheitsbeauftragten zügig umzusetzen.

Die Aufgaben des IT-Sicherheitsbeauftragten sind unter anderem:

- den IT-Sicherheitsprozess zu steuern und zu koordinieren,
- die Erstellung von IT-System-Sicherheitsrichtlinien zu initiieren und zu koordinieren,
- die Erstellung des IT-Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte zu koordinieren,
- den Realisierungsplan für die IT-Sicherheitsmaßnahmen zu erstellen und deren Realisierung zu initiieren und zu überprüfen,
- der Leitungsebene zu berichten,
- sicherheitsrelevante Projekte zu koordinieren und den Informationsfluss zwischen Bereichs-IT-, IT-Projekt- sowie IT-System-Sicherheitsbeauftragten sicherzustellen,
- sicherheitsrelevante Zwischenfälle zu untersuchen sowie
- Sensibilisierungs- und Schulungsmaßnahmen zu IT-Sicherheit zu initiieren und zu steuern.

Der IT-Sicherheitsbeauftragte muss bei allen Projekten mit IT-Bezug beteiligt werden, damit sichergestellt ist, dass sicherheitsrelevante Aspekte ausreichend beachtet werden. Dazu gehören z. B. die Beschaffung von IT-Systemen oder die Gestaltung von IT-gestützten Geschäftsprozessen.

Um den direkten Zugang zur Behördenleitung (Bürgermeister der Stadt Hilden) sicherzustellen, ist es empfehlenswert, diese Rolle als Stabsstelle einzurichten. In kleinen Organisationen kann die Funktion des IT-Sicherheitsbeauftragten auch von einem qualifizierten Mitarbeiter neben anderen Aufgaben wahrgenommen werden. Maßgeblich ist, dass dem IT-Sicherheitsbeauftragten ausreichend Zeit zur sachge-

rechten Erfüllung seiner Aufgaben zugebilligt wird. Vor allem bei der erstmaligen Einrichtung des IT-Sicherheitsprozesses müssen hierfür auch hinreichende zeitliche Ressourcen eingeplant werden. Ebenfalls wichtig bei der Planung der IT-Sicherheitsorganisation ist die Benennung eines qualifizierten Vertreters des IT-Sicherheitsbeauftragten.

Management-Berichte zur IT-Sicherheit

Damit die oberste Leitungsebene einer Behörde (Verwaltungsvorstand) die richtigen Entscheidungen treffen kann, um IT-Sicherheit auf einem angemessenen Niveau zu gewährleisten, benötigt sie die dafür notwendigen Informationen.

> **Empfehlung**
>
> Soweit bei der Stadt Hilden noch kein IT-Sicherheitsbeauftragter bestellt ist, sollten Berichte zur IT-Sicherheit vom IT-Team erstellt werden, um der Verwaltungsleitung alle Informationen für eine Risikobewertung transparent zu machen und eine Basis für notwendige Entscheidungen zu liefern.

Grundsätzlich ist das Erstellen von Management-Berichten zur IT-Sicherheit eine originäre Aufgabe des IT-Sicherheitsbeauftragten. Da dieser bei der Stadt Hilden noch nicht vorhanden ist, sollte dennoch sichergestellt werden, dass der Verwaltungsvorstand über alle Angelegenheiten zum Thema IT-Sicherheit informiert ist, um anhand dieser Informationen eine Risikoabschätzung durchführen und ggf. Maßnahmen initiieren zu können. Da die Gesamtverantwortung der Sicherheit in der Datenverarbeitung bei der Behördenleitung liegt, sind derartige Berichte eigentlich unverzichtbar und sollten daher auch von der Leitung eingefordert werden.

Ein Managementbericht IT-Sicherheit sollte aufzeigen:

- inwieweit die Vorgaben des IT-Sicherheitskonzepts in der Behörde bereits abgedeckt sind,
- an welchen Stellen noch Lücken - und damit Restrisiken - bestehen,
- ob und welche IT-Sicherheitsvorfälle aufgetreten sind,
- welche Schäden entstanden sind und welche Schäden verhindert werden konnten,
- welche Ergebnisse interne Überprüfungen und Audits erbracht haben,
- inwieweit das IT-Sicherheitsniveau den Sicherheitsanforderungen und der Bedrohungslage der Institution genügt,
- ob sich Rahmenbedingungen geändert haben, so dass weitere Maßnahmen erforderlich sind,
- ob die Aktivitäten im Rahmen der IT-Sicherheit Erfolg hatten,
- ob sich die IT-Sicherheitsmaßnahmen zur Erreichung der IT-Sicherheitsziele als geeignet erwiesen haben oder ob Maßnahmen geändert oder ergänzt werden müssen,
- welche Rückmeldungen es von Kunden, Geschäftspartnern, Mitarbeitern oder der Öffentlichkeit zu IT-Sicherheitsaspekten gab,
- welche Ressourcen für IT-Sicherheit aufgewendet wurden,
- ob und wie die Entscheidungen der letzten Managementbewertung umgesetzt wurden und ob die Aktivitäten im Rahmen der IT-Sicherheit Erfolg hatten.

Dokumentation des Sicherheitsprozesses

Im Sinne des IT- Grundschutzes, lässt sich ein angemessenes Sicherheitsniveau nur dann erreichen, wenn eine verständliche, angemessene, aktuelle und konsistente Dokumentation des IT-Sicherheitsprozesses vorhanden ist.

Empfehlung

Der Ablauf des IT-Sicherheitsprozesses sowie wichtige Entscheidungen und die Arbeitsergebnisse in den einzelnen Phasen sollten dokumentiert werden.

Eine solche Dokumentation ist eine wesentliche Grundlage für die Aufrechterhaltung der IT-Sicherheit und damit entscheidende Voraussetzung für die effiziente Weiterentwicklung des Prozesses. Sie hilft dabei, die Ursachen von Störungen und fehlgeleiteten Abläufen zu finden und zu beseitigen. Wichtig ist dabei, dass nicht nur die jeweils aktuelle Version der betreffenden Unterlagen griffbereit gehalten wird, sondern auch eine zentrale Archivierung der Vorgängerversionen vorgenommen wird. Erst hierdurch ist eine kontinuierliche Rückverfolgung der Entwicklung im Bereich IT-Sicherheit, bei der die getroffenen Entscheidungen nachvollziehbar werden, gewährleistet.

Schulungen zu IT- Sicherheitsmaßnahmen

Wie sich an vielen konkreten Beispielen und auch den Schadensstatistiken von Elektronik-Versicherern zusammenfassen lässt, resultieren IT-Schäden oft schlicht aus der Unkenntnis elementarer Sicherheitsmaßnahmen. Um dies zu verhindern, sollte grundsätzlich jeder einzelne Mitarbeiter im sorgfältigen Umgang mit der IT unterwiesen werden. Nur durch die Vermittlung der notwendigen Kenntnisse kann ein Verständnis für die erforderlichen IT-Sicherheitsmaßnahmen geweckt werden.

Nicht nur für das IT-Personal sollte eine derartige Unterweisung obligatorisch sein.

Empfehlung

Für die Mitarbeiter sollte eine Grundeinweisung zum Thema IT-Sicherheit erfolgen, um hier zusätzliche Kompetenzen zu grundsätzlichen Risiken und aktuelle Gefährdungslagen aufzubauen.

In diesem Zusammenhang ist sehr positiv anzumerken, dass ein Vortrag zum Thema IT-Sicherheit durch den IT- Leiter im Rahmen einer Sitzung auf Amts- und Abteilungsleiterebene vorgesehen ist, um auf aktuelle Sicherheitsaspekte aufmerksam zu machen und das Bewusstsein für Gefährdungslagen zu schärfen

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. Ein Konzept zur Notfallvorsorge besteht in Hilden derzeit noch nicht, ist aber nach Angaben der IT kurzfristig geplant.

> **Empfehlung**
>
> Es sollte ein Notfallvorsorgekonzept bzw. ein Notfallhandbuch für die IT erstellt werden.

Für die Erstellung eines Notfallvorsorgekonzepts, das letztlich in einem Notfallhandbuch münden soll, sind eine Reihe von Maßnahmen umzusetzen, beginnend mit einer strategischen Planung über die Einbeziehung der relevanten Geschäftsprozesse bis hin zu konkreten Maßnahmen für die IT-Systeme, die diesen Prozessen zugeordnet sind.

Das Notfallhandbuch muss an die spezifische IT-Situation der Behörde angepasst sein. In Form detaillierter Übersichten sind die verantwortlichen und handelnden Personen, die zu treffenden Entscheidungen, die Sofortmaßnahmen bei Feststellung eines Notfalls und die Handlungsanweisungen für spezielle Ereignisse festzuschreiben. Es beschreibt die präventiven Maßnahmen sowie die Maßnahmen zur Schadenstabilisierung und zur Wiederherstellung der IT-Systeme; letztendlich auch Ersatzbeschaffungsmaßnahmen.

Das Notfallhandbuch muss im Notfall schnell erreichbar und transportabel sein. Bei ausschließlich elektronischer Speicherung des Dokumentes oder wenn es in einer werkzeuggestützten Form vorliegt, ist die Bereitstellung eines oder mehrerer Notfall-Notebooks erforderlich.

Von besonderer Bedeutung ist die Durchführung von Notfallübungen, um die Umsetzung der im Notfallhandbuch aufgeführten Maßnahmen einzuüben und deren Effizienz zu steigern.

Feststellung

Nach Angaben der IT werden in Hilden Notfallübungen und –prozeduren bereits regelmäßig durchgeführt.

Da diese Übungen den normalen Betriebsablauf stören können, sollte die Häufigkeit an der Gefährdungslage orientiert sein, jedoch sollten die entsprechenden Notfallübungen zumindest einmal jährlich stattfinden. Soweit erforderlich sind Schulungsmaßnahmen der Mitarbeiter durchzuführen (Erste Hilfe, Brandbekämpfung etc.).

Empfehlung

Die Ergebnisse einer Notfallübung sollten dokumentiert werden.

Im Rahmen der Notfallvorsorge besteht zwischen der Stadt Hilden und der Stadt Monheim am Rhein eine Absprache auf der Basis einer interkommunalen Zusammenarbeit, die für den Eintritt von Notfallereignissen eine gegenseitige Hilfestellung bei der Errichtung einer Notfall- Infrastruktur zum Gegenstand hat.

Virenschutz

Virenschutzkonzept

Um für eine gesamte Organisation einen effektiven Computer-Virenschutz zu erreichen, sind abgestimmte und angemessene Schutzmaßnahmen auszuwählen und umzusetzen. Dies setzt eine konzeptionelle Vorgehensweise voraus, um sämtliche betroffenen IT-Systeme mit geeigneten Maßnahmen zu versehen und durch Aktualisierung den notwendigen Schutz aufrechtzuerhalten.

Feststellung

Bei der Stadt Hilden werden technische Maßnahmen durchgeführt, um einen ausreichenden Mindestschutz vor Computerviren sicherzustellen. Ein Virenschutzkonzept gibt es derzeit bei der Stadt Hilden noch nicht.

Ziel eines Virenschutzkonzeptes ist es, geeignete Maßnahmen zum Schutz vor Schadprogrammen zusammenzustellen. Es soll hier gewährleistet werden, dass das Auftreten von Computer-Viren verhindert oder so früh wie möglich erkannt wird.

Empfehlung

Wir empfehlen, ein dediziertes Virenschutzkonzept zu erstellen. Dabei können die Regelungen, die bereits in den vorhandenen Dienstanweisungen vorhanden sind, zusammengeführt werden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hält bei Bedarf ein Muster für den Inhalt eines Virenschutzkonzeptes vor.

Fragenkreis „Backup und Archivierung“

Im Rahmen der Prüfung sind keine Sachverhalte identifiziert worden, die zu Empfehlungen führen.

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 ein Datenschutzbeauftragter mit Stellvertreter ordnungsgemäß bestellt worden ist und ob ein Verfahrensverzeichnis im Sinne des § 8 DSG NRW geführt wird.

Gegenstand der Prüfung sind nicht eventuelle Verstöße gegen die materiell-rechtlichen Bestimmungen des Datenschutzes. Allerdings vertreten wir die Auffassung, dass in Kommunen, die unter Verletzung gesetzlicher Bestimmungen keinen Datenschutzbeauftragten ernannt haben, das Risiko der Missachtung materiell-rechtlicher Datenschutzbestimmungen wegen einer fehlenden behördeninternen Kontrollinstanz erheblich erhöht ist. Mit dem formalen Akt der Bestellung sind aus unserer Sicht elementare Voraussetzungen für die Beachtung und Einhaltung des Datenschutzes geschaffen.

Pflicht zur Bestellung eines Datenschutzbeauftragten

§ 32a DSG NRW verpflichtet öffentliche Stellen, die personenbezogene Daten verarbeiten – mithin auch die die Städte und Gemeinden – zur Bestellung eines behördlichen Datenschutzbeauftragten und eines Stellvertreters. 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.

Feststellung

Die Funktion des Datenschutzbeauftragten ist in der Stadt Hilden ordnungsgemäß personell besetzt; ein Stellvertreter ist bestellt.

Die Stadt hat von der Möglichkeit nach § 32a Abs. 1 Satz 3 DSG NRW Gebrauch gemacht und einen gemeinsamen Datenschutzbeauftragten mit einer anderen öffentlichen Stelle, hier: dem Kreis

Mettmann bestellt. Der stellvertretende Datenschutzbeauftragte ist Mitarbeiter der Stadtverwaltung Hilden.

Verfahrensverzeichnis

Die Führung des Verfahrensverzeichnisses ist im Rahmen der Aufgaben des Datenschutzbeauftragten von besonderem Gewicht. Es handelt sich um die im § 8 DSG NRW gesetzlich vorgeschriebene Dokumentation aller automatisierten Verfahren, also sämtlicher Programme oder Programmteile, 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

Von der Stadt Hilden wird ein Verfahrensverzeichnis gemäß § 8 DSG NRW geführt. In das Verzeichnis wurde im Rahmen der Prüfung stichprobenweise Einsicht genommen.

Die Feststellung, ob das Verzeichnis in dem Sinne vollständig ist, dass sämtliche zur automatisierten Verarbeitung personenbezogener Daten eingesetzten Verfahren ordnungsgemäß erfasst sind, war nicht Gegenstand der Prüfung.

Zwar umfasst das Verzeichnis den in § 8 DSG NRW vorgeschriebenen Informationsgehalt, wurde aber seit mehreren Jahren nicht mehr fortgeschrieben.

Die Stadt hat in Zusammenarbeit mit dem Datenschutzbeauftragten Maßnahmen getroffen, um in absehbarer Zeit ein aktualisiertes, den gegenwärtigen Stand der eingesetzten Verfahren dokumentierendes Verzeichnis zu erstellen.

Empfehlung

Die Stadt Hilden sollte die Aktivitäten zur Aktualisierung bzw. Vervollständigung des Verfahrensverzeichnisses mit Priorität fortsetzen.

Nachsatz

Auf das weitere Verfahren nach § 105 Abs. 5 GO NRW weisen wir hin.

Eine Weiterverfolgung der getroffenen Feststellungen obliegt dem Landrat als untere staatliche Verwaltungsbehörde sowie als Bewilligungsbehörde in eigener Kompetenz.

Herne, den 15.12.2009

Präsident der Gemeindeprüfungsanstalt

Nordrhein-Westfalen

Im Auftrag

Michael Kuzniarek

GPA NRW

Überörtliche Prüfung Informationstechnologie
- Erhebungsbogen IT-Sicherheit -

Name der Kommune:
Stadt Hilden

Gesprächstermin:
08.09.2009

Prüfer:
AE

Gesprächspartner in der Kommune:
Herr Kramer

Fragenkreis: IT-Räume und Infrastrukturaufbau

Serverraum

Baustein Serverraum:
von 21 Maßnahmen 20x JA, 0x NEIN, 0x teilweise, 1x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Angepasste Aufteilung der Stromkreise	ja	
Handfeuerlöscher	ja	
Verwendung von Sicherheitstüren und -fenstern	ja	
Geschlossene Fenster und Türen	ja	
Gefahrenmeldeanlage/Brandmelder	ja	
Abgeschlossene Türen	ja	
Vermeidung von wasserführenden Leitungen	ja	
Überspannungsschutz	ja	
Not-Aus-Schalter	entfällt	
Klimatisierung	ja	
Lokale unterbrechungsfreie Stromversorgung	ja	
Fernanzeige von Störungen	ja	
Redundanzen in der technischen Infrastruktur (ohne Storage)	ja	
Technische und organisatorische Vorgaben für Serverräume	ja	
Brandschutz von Patchfeldern	ja	
Zutrittsregelung und -kontrolle	ja	
Rauchverbot	ja	
Verwendung von hochverfügbaren Architekturen	ja	
Anschluss an SAN, NAS, DAS	ja	
Storage System redundant	ja	
Wird eine Servervirtualisierung eingesetzt?	ja	

IT-Verkabelung

Baustein IT-Verkabelung:
von 12 Maßnahmen 11x JA, 0x NEIN, 0x teilweise, 1x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Welche Verkabelungsart kommt zum Einsatz?	ja	
Netz-Topologie	ja	
Erneuerung der IT-Verkabelung	ja	
Redundanzen für die Primärverkabelung	ja	
Redundanzen für die Gebäudeverkabelung	ja	
Brandabschottung von Trassen	ja	
Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht	ja	
Ausreichende Trassendimensionierung	ja	
Materielle Sicherung von Leitungen und Verteilern	ja	
Dimensionierung und Nutzung von Schranksystemen	ja	
Neutrale Dokumentation in den Verteilern	entfällt	
Laufende Fortschreibung und Revision der Netzdokumentation	ja	

Sicherheitsgateway

Baustein Sicherheitsgateway:
von 19 Maßnahmen 17x JA, 0x NEIN, 0x teilweise, 2x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Outsourcing des Sicherheitsgateway		☐ Sicherheitsgateway ausgelagert, keine unmittelbare Prüfung erfolgt
Entwicklung eines Konzepts für Sicherheitsgateways	ja	
Auswahl geeigneter Grundstrukturen für Sicherheitsgateways	ja	
Content Filter im Einsatz	ja	
Proxy Server im Einsatz	ja	
Gateway redundant	ja	
Schulung der Administratoren des Sicherheitsgateways	ja	
Protokollierung der Sicherheitsgateway-Aktivitäten	ja	
Integration von Proxy-Servern in das Sicherheitsgateway	ja	
Integration von VPN-Komponenten in ein Sicherheitsgateway	ja	
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	ja	
Integration eines E-Mailservers in ein Sicherheitsgateway	ja	
Integration eines Datenbank-Servers in ein Sicherheitsgateway	ja	
Integration eines DNS-Servers in ein Sicherheitsgateway	ja	
Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway	entfällt	
Notfallvorsorge bei Sicherheitsgateways	ja	

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 5x JA, 0x NEIN, 0x teilweise, 4x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Existiert bei Notebooks Homogenität?	ja	
Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz	entfällt	
Einsatz von Diebstahl-Sicherungen	entfällt	
Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung	ja	
Regelmäßiger Einsatz eines Anti-Viren-Programms	ja	

Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme	entfällt	
Sichere Kommunikation von unterwegs	ja	
Sicherer Anschluss von Notebooks an lokale Netze	ja	
Datensicherung bei mobiler Nutzung des IT-Systems	entfällt	

Allgemeiner Client

Baustein Allgemeiner Client:
von 14 Maßnahmen 12x JA, 0x NEIN, 0x teilweise, 2x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Existiert ein homogenes Umfeld bei den Client PC? Hardware	ja	
Existiert ein homogenes Umfeld bei den Client PC? Software	ja	
Austauschzyklen ?	ja	
Wie alt sind die Geräte?		max. 4 Jahre
Wird ein Systemmanagement eingesetzt?	ja	
Wird Remote Desktop genutzt?	ja	
Herausgabe einer PC-Richtlinie	entfällt	
Dokumentation der Systemkonfiguration	ja	
Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	ja	
Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz	ja	
Geregelte Außerbetriebnahme eines Clients	ja	
Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung	ja	
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 4x JA, 2x NEIN, 1x teilweise, 1x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Erstellung einer Leitlinie zur Informationssicherheit	ja	
Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	nein	
Erstellung eines Sicherheitskonzepts	ja	
Management-Berichte zur Informationssicherheit	teilw.	
Dokumentation des Sicherheitsprozesses	nein	
Festlegung der Sicherheitsziele und -strategie	ja	
Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	ja	
Erstellung von zielgruppengerechten Sicherheitsrichtlinien	entfällt	

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	
Vergabe von Zutrittsberechtigungen	ja	
Vergabe von Zugangsberechtigungen	ja	
Vergabe von Zugriffsrechten	ja	
Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln	ja	
Schlüsselverwaltung	ja	
Kontrollgänge	teilw.	

Sicherheit Personal

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

Maßnahmen	erfüllt?	Bemerkungen
Geregelte Einarbeitung/Einweisung neuer Mitarbeiter	ja	
Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen	ja	
Schulung vor Programmnutzung	ja	
Schulung zu IT-Sicherheitsmaßnahmen	teilw.	
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 7x JA, 7x NEIN, 0x teilweise, 1x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Erstellung einer Übersicht über Verfügbarkeitsanforderungen	nein	
Notfall-Definition, Notfall-Verantwortlicher	nein	
Erstellung eines Notfall-Handbuches	nein	
Dokumentation der Kapazitätsanforderungen der IT-Anwendungen	ja	
Definition des eingeschränkten IT-Betriebs	nein	
Untersuchung interner und externer Ausweichmöglichkeiten	ja	
Regelung der Verantwortung im Notfall	nein	
Alarmierungsplan	nein	
Notfall-Pläne für ausgewählte Schadensereignisse	nein	
Erstellung eines Wiederanlaufplans	ja	
Durchführung von Notfallübungen	ja	
Erstellung eines Datensicherungsplans	ja	
Ersatzbeschaffungsplan	entfällt	
Abschließen von Versicherungen	ja	
Redundante Kommunikationsverbindungen	ja	

Hard- und Softwaremanagement

Baustein Hard- und Softwaremanagement:
von 9 Maßnahmen 8x JA, 0x NEIN, 1x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Regelung des Passwortgebrauchs	ja	
Hinterlegen des Passwortes	teilw.	
Dokumentation der Systemkonfiguration	ja	
Regelung für die Einrichtung von Benutzern / Benutzergruppen	ja	
Dokumentation der zugelassenen Benutzer und Rechteprofile	ja	
Dokumentation der Veränderungen an einem bestehenden System	ja	
Informationsbeschaffung über Sicherheitslücken des Systems	ja	
Software-Abnahme- und Freigabe-Verfahren	ja	
Kontrolle der Protokolldateien	ja	

Virenschutz

Baustein Virenschutz:
von 4 Maßnahmen 2x JA, 1x NEIN, 0x teilweise, 1x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Erstellung eines Computer-Virenschutzkonzepts	nein	
Aktualisierung der eingesetzten Computer-Viren-Suchprogramme	ja	
Regelmäßiger Einsatz eines Anti-Viren-Programms	ja	
Verhaltensregeln bei Auftreten eines Computer-Virus	entfällt	

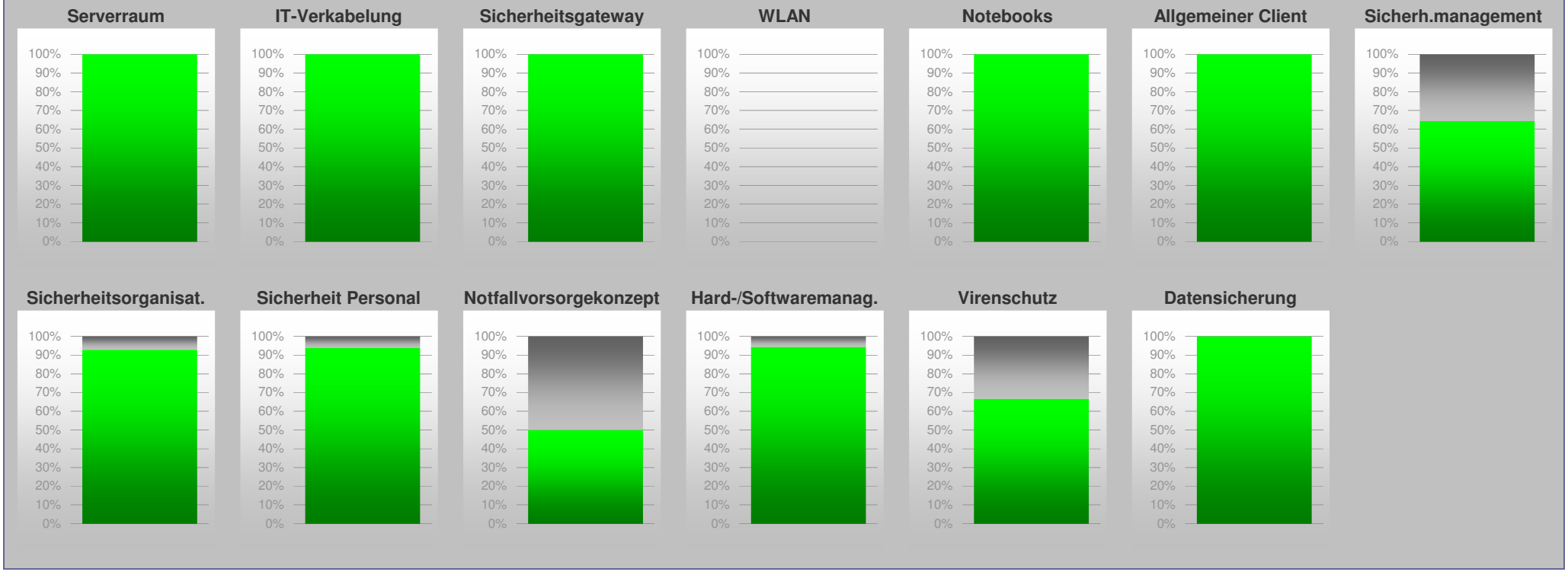
Fragenkreis: Backup und Archivierung

Datensicherung

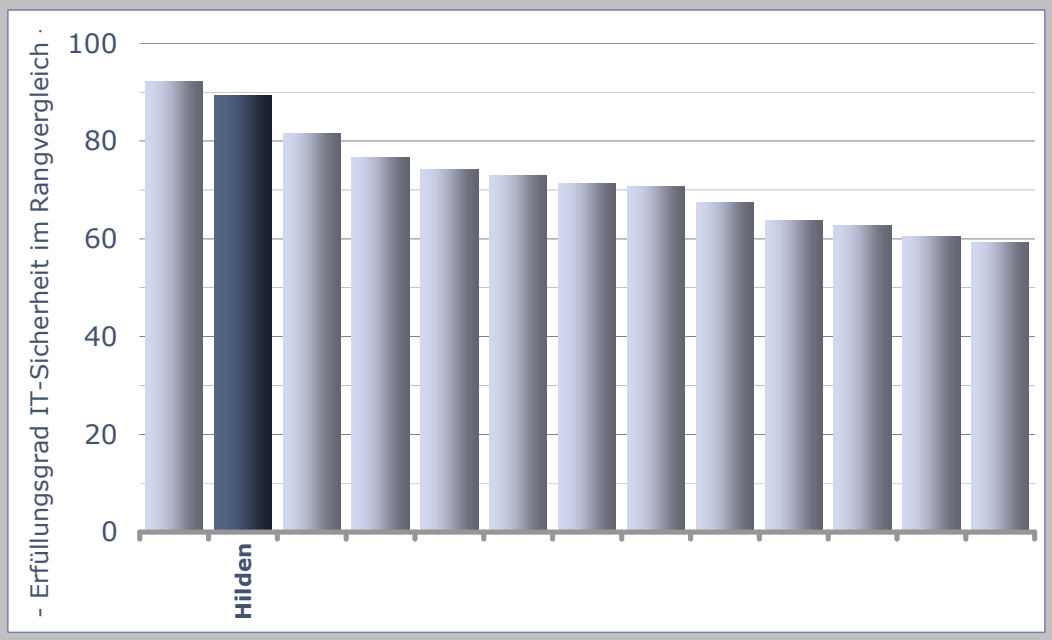
Baustein Datensicherung:
von 9 Maßnahmen 8x JA, 0x NEIN, 0x teilweise, 1x entfällt

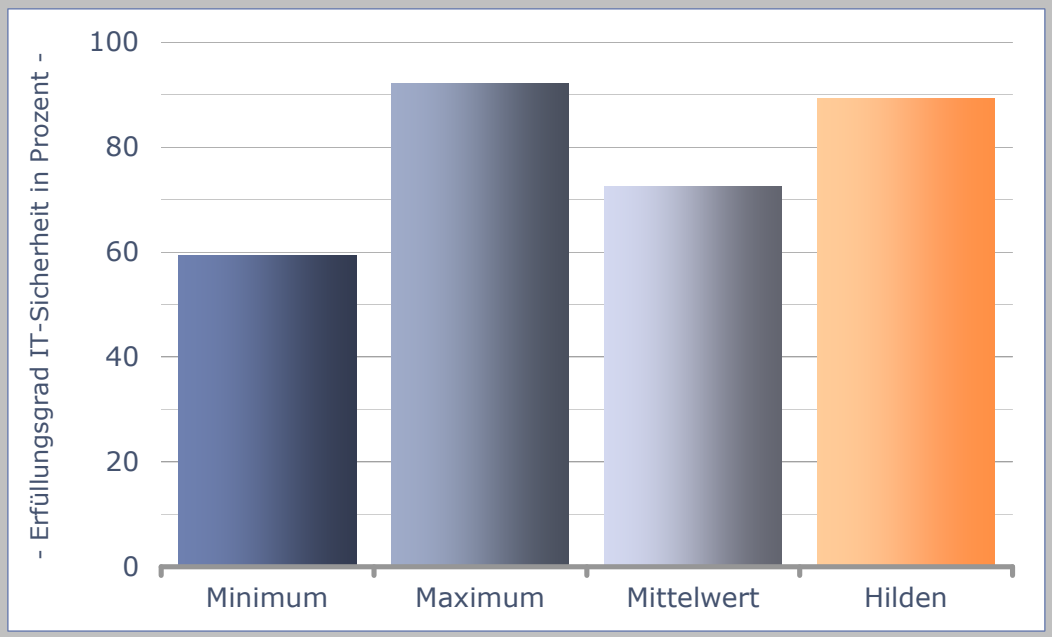
Maßnahmen	erfüllt?	Bemerkungen
Verpflichtung der Mitarbeiter zur Datensicherung	entfällt	
Beschaffung eines geeigneten Datensicherungssystems	ja	
Geeignete Aufbewahrung der Backup-Datenträger	ja	
Sicherungskopie der eingesetzten Software	ja	
Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen	ja	
Regelmäßige Datensicherung	ja	
Entwicklung eines Datensicherungskonzepts	ja	
Dokumentation der Datensicherung	ja	
Übungen zur Datenrekonstruktion	ja	

Überörtliche Prüfung Informationstechnologie
- Detail-Erfüllungsgrade Stadt Hilden -



Überörtliche Prüfung Informationstechnologie
- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -





GPA NRW
Heinrichstraße 1 · 44623 Herne
Postfach 101879 · 44608 Herne
Telefon (02323) 1480-0
Fax (02323) 1480-333
info@gpa.nrw.de
www.gpa.nrw.de

Gemeindeprüfungsanstalt
Nordrhein-Westfalen