Beratung · Prüfung · Service

Überörtliche Prüfung Informationstechnologie der Stadt Coesfeld vom 17.11.2009 bis 31.01.2010

Beratung · Prüfung · Service

GPA NRW

Überörtliche Prüfung Informationstechnologie der Stadt Coesfeld vom 17.11.2009 bis 31.01.2010

Inhaltsverzeichnis

Zur GPA NRW und zur Prüfung

Ziele und Inhalte unserer Prüfung

Mit unserer Prüfung wollen wir zu einem wirtschaftlichen, sachgerechten und rechtmäßigen Einsatz der Informationstechnologie (IT) 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 Entscheidung, die IT in den kommunalen Verwaltungen einer intensiven Betrachtung zu unterziehen, hat vielerlei gute Gründe. Die IT spielt gerade in Modernisierungsprozessen 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. Der Ressourcenaufwand ist häufig groß, so dass entsprechende Wirtschaftlichkeitspotenziale erwartet werden. Organisation und Steuerung bieten vielfältige Gestaltungsmöglichkeiten. In zahlreichen Fällen ist der Einsatz von IT oft die einzige Lösung, das einzige Organisationsmittel, um einen effizienten und effektiven Ablauf der Geschäftsprozesse gestalten zu können.

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

- Aufwand / Wirtschaftlichkeit
- Organisation und Steuerung
- Infrastruktur und Sicherheit
- Datenschutz.

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

Sukzessive werden wir diese Prüfung auf der Grundlage des § 105 der Gemeindeordnung NRW (GO NRW) bei allen Städten und Gemeinden sowie bei den Gemeindeverbänden durchführen.

Die Verantwortung für die Realisierung der oben genannten Ziele bleibt bei der Stadt Coesfeld. Wir sind der Auffassung, dass der hohe Ressourcenverbrauch und das erhebliche persönliche Haftungsrisiko die IT 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**.

Unser Prüfungsprozess vollzieht sich generell in drei 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 zur Kenntnis im Anhang beigefügt ist, kann entnommen werden, welches Spektrum unsere Prüfung in diesem Bereich umfasst.

Informationen zum Prüfungsablauf

Wir haben die Prüfung in der Stadt Coesfeld vom 17.11.2009 bis 31.01.2010 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
	Marcus Meyer-Meiners

Wir haben das Prüfungsergebnis mit

- der Leitung des Fachbereichs 10 sowie
- dem Leiter des IT-Teams

erörtert.

Der Entwurf des Prüfberichts wurde übersandt.

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[1] 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 Coesfeld bereitzustellen und zu betreuen, mit dem geringsten Mitteleinsatz - also in konsequenter Umsetzung des Minimalprinzips[2] - erfüllt wird.

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

[2] 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 Coesfeld 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 haben wir zusammengefasst, zu welcher Einschätzung wir in Bezug auf das Verhältnis von Aufwand und Leistungsqualität der IT in der Stadt Coesfeld 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.

Darstellung des Gesamtergebnisses

Zunächst bilden wir die von der Stadt Coesfeld erreichte Positionierung sowohl hinsichtlich der Aufwendungen als auch hinsichtlich des Grades der Aufgabenerfüllung beim IT-Grundschutz in einer so genannten Matrix ab.

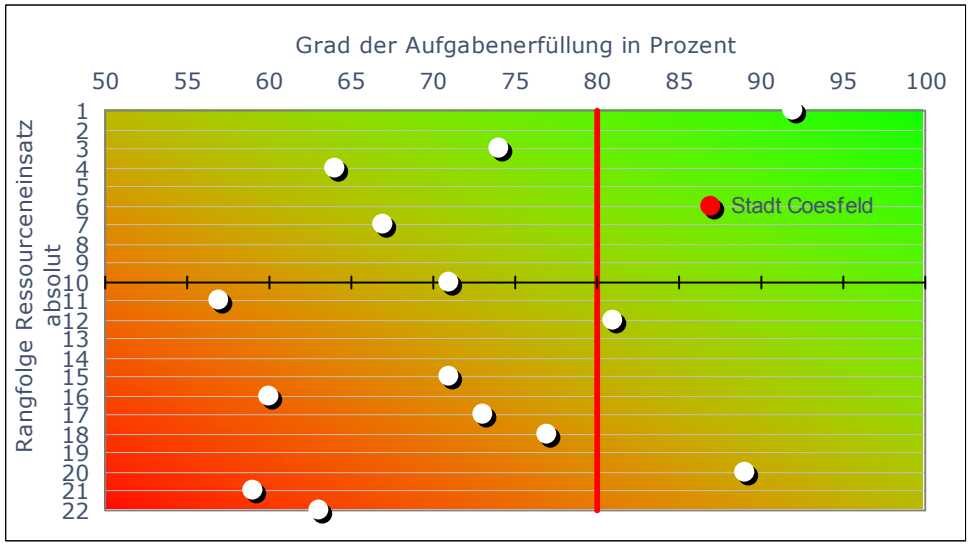
Ziel dieser Matrix ist die Darstellung des Verhältnisses zwischen eingesetzten Ressourcen und dem Grad der Aufgabenerfüllung. In der Matrixdarstellung wird auf der X-Achse der erreichte Grad der Aufgabenerfüllung abgebildet. Dieser ergibt sich aus den während der Prüfung angelegten Checklisten, welche als Anhang diesem Bericht beigefügt sind. Vor dem Hintergrund der Anforderungen des BSI-Grundschutz-Handbuchs erscheint ein Erfüllungsgrad bei der IT-Sicherheit von mindestens 80 Prozent erstrebenswert.

Auf der Y-Achse wird die Rangfolge der Kommune nach der betriebswirtschaftlichen Betrachtung abgebildet. Zur Ermittlung der Rangfolge wurden die im Abschnitt „IT-Aufwendungen" behandelten Berichtskennzahlen (*IT-Aufwendungen je Einwohner* und *IT-Aufwendungen je Bildschirmarbeitsplatz* (BSAP)*)* sowie weitere Analysekennzahlen (*Betreuungsquote, BSAP je 1.000 Einwohner* sowie *IT-Stellen je 100.000 Einwohner*) gewichtet und schließlich in eine interkommunale Rangfolge gebracht.

Aus der erreichten Positionierung lässt sich letztlich ablesen, welches objektive Maß an IT-Sicherheit mit den eingesetzten Mitteln erreicht wird. Dieses individuelle Ergebnis der betrachteten Kommune ergibt zusammen mit den weiteren, anonymisierten Ergebnissen des aktuellen Vergleichs ein Abbild der interkommunalen Landschaft (hier: mittlere, kreisangehörige Kommunen).

Wir versuchen anhand dieser Darstellung auch aufzuzeigen, welche Auswirkungen eine Erhöhung von Aufwendungen z. B. im Bereich der Sachaufwendungen zum Ausbau der IT-Sicherheit auf die Positionierung im interkommunalen Vergleich haben könnte. Daraus lassen sich letztlich konkrete Maßnahmen ableiten, welche zur Verwirklichung des Ziels „IT-Sicherheit bei angemessenen Aufwendungen" dienlich erscheinen.

Matrixdarstellung überörtliche Prüfung der IT - mittlere, kreisangehörige Kommunen



3

Bei der Gesamtbetrachtung der IT-Aufwendungen sowie des Grades der Aufgabenerfüllung erreicht die Stadt Coesfeld im interkommunalen Vergleich eine Spitzenposition. Die Positionierung zeigt, dass sie umfängliche IT-Standards zu angemessenen, vergleichsweise günstigen IT-Aufwendungen anbieten kann.

Aufgrund der vorgefundenen Situation und der geplanten weiteren Maßnahmen im IT-Bereich zählen wir die Stadt Coesfeld im aktuellen interkommunalen Vergleich zu den Benchmark-Kommunen.

Eine Erhöhung des prozentualen Grades der Aufgabenerfüllung ist bei entsprechendem Einsatz von Sachaufwendungen in einem gewissen Maße möglich, ohne dass die Stadt Coesfeld ihre derzeitige gute Position im interkommunalen Vergleich aufgeben müsste.

[3] Leere Rangpositionen werden von Prüfkommunen belegt, die mit in die Rangbildung einbezogen wurden, für die zum Zeitpunkt der Prüfung aber noch kein Erfüllungsgrad zur IT-Sicherheit ermittelt wurde.

Ergebnisse im Überblick

Die Stadt Coesfeld erreicht in der Betrachtung der IT-Aufwendungen aufgrund der – im interkommunalen Vergleich - unterdurchschnittlichen Aufwendungen im Bereich der Personal- und Sachaufwendungen im IT-Bereich Rang sechs.

Hinsichtlich der *IT Aufwendungen je Einwohner* erreicht die Stadt Coesfeld einen Wert von 20,81 Euro und liegt damit 1,86 Euro unter dem derzeitigen Mittelwert. Bezüglich der *IT-Aufwendungen je BSAP* erreicht die Stadt Coesfeld einen Wert von 3.345 Euro und unterschreitet damit den derzeitigen Mittelwert um 519 Euro.

Besonders positiv hervorzuheben sind die vorgefundenen Instrumente zur Finanzsteuerung, welche auch umfänglich auf das Produkt „Technikunterstützte Informationsverarbeitung" angewandt werden.

Neben der Inanspruchnahme von Leistungen des IT-Dienstleisters der Stadt Münster (citeq) betreibt die Stadt Coesfeld eine eigene IT-Infrastruktur. Dabei ist festzustellen, dass die vorhandene Infrastruktur sehr plausibel gestaltet ist und mit den vorgesehenen Infrastrukturanpassungen einen hohen Standard im interkommunalen Vergleich abbilden wird.

In diesem Zusammenhang begrüßen wir sehr die geplanten Aktivitäten zur Virtualisierung des Serverumfeldes, da dies eine elementare Basis für einen effezienteren und effektiveren Technikeinsatz darstellt.

In Hinblick auf die IT-Sicherheit erreicht die Stadt Coesfeld einen Erfüllungsgrad von 87 Prozent. Lediglich zwei Kommunen im aktuellen Vergleich erreichen einen höheren Grad an IT-Sicherheit, wobei eine dieser Kommunen wesentlich höhere Aufwendungen aufbringt.

Im Rahmen der IT-Sicherheitsprüfung werden Maßnahmen vorgeschlagen, deren Umsetzung größtenteils schon von der Stadt Coesfeld projektiert sind. Hierdurch wird zukünftig ein Erfüllungsgrad von über 90 Prozent erreichbar sein.

Die Umsetzung der Hinweise zum IT-Grundschutz kann u. U. mit einem Mehraufwand an Sach- und/oder Personalressourcen verbunden sein. Eine fiktive Erhöhung der Sachaufwendungen um jährlich 30.000 Euro (z. B. als Abschreibungsaufwand für die Einführung einer Virtualiserung-

sumgebung), würde den Erfüllungsgrad anheben, ohne dass die Rangfolge bei den IT-Aufwendungen sich negativ verändern würde.

Im Bereich des IT-Sicherheitsmanagements sind durch aufwandsneutrale, organisatorische Maßnahmen, wie z. B. das Erstellen einer Sicherheitsleitlinie und dem Einrichten einer Arbeitsgruppe „IT-Sicherheit" können weitere Optimierungspotenziale hinsichtlich des festgestellten Erfüllungsgrades realisiert werden.

Ergebnisse im Einzelnen

Ausgangslage in der kommunalen IT-Landschaft

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

Ausgangslage in Coesfeld

Die Stadt Coesfeld fällt in die Größenklasse der mittleren Kommunen; zum Stichtag 31.12.2008 hatte die Stadt 36.558 Einwohner.

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

Die zentrale Bereitstellung und Betreuung der IT ist in Coesfeld aufbauorganisatorisch als "IT-Team" dem Fachbereich 10 zugeordnet und damit dem Dezernat I angegliedert.

Die Stadt Coesfeld betreibt ihre IT in eigener Verantwortung. Daneben werden Services und Dienstleistungen des IT-Dienstleisters der Stadt Münster (citeq) in Anspruch.

Der zentralen IT sind vier Mitarbeiter zugeordnet. Wir werden nachfolgend detailliert darstellen, wie sich die Stellenanteile auf von uns definierte IT-Aufgabenbereiche verteilen.

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 im Bericht einheitlich von Aufwendungen sprechen, obwohl auch Ausgaben und Kostengrößen einfließen. Die in der betriebswirtschaftlichen Terminologie klare Trennung von Ausgaben, Aufwand und Kosten wird damit zugunsten einer pragmatischen Lösung teilweise aufgehoben.

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.

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:

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

Ergebnis der Jahresrechnung 2005/2006 Verwaltungshaushalt in Euro		
	2005	**2006**
Verbrauchsmaterial (Toner usw.) VHS	304	703
Verbrauchsmaterial (Toner usw.) Bücherei	1.072	740
Toner/Druckerpatronen AWW	228	510
Literatur, Zeitschriften	73	73
Wartungsverträge und Updates	44.011	47.188
Hardwarewartung	8.882	5.078
Reparatur und Wartung AWW		67
Elektronikversicherung	769	720
Nutzung von Leitungsdiensten Bücherei	20	20
Leitungsdienste versatel		1.411
Leistungen der citeq	244.357	318.847
Neuanschaffung und Unterhaltung von bewegl. Vernögen	16.662	3.321
Bürobedarf, Papier, Drucksachen	14.982	10.371
Verbrauchsmaterial, Netzanbindungen (Schulsek.)	8.750	8.750
Miete TK-Anlage	39.531	40742
Service, Dienstleistungen TK-Anlage	3.596	1.748
Summe	383.236	440.289

Ergebnis der Jahresrechnung 2005/2006 Vermögenshaushalt in Euro		
	2005	**2006**
Investitionen 0600.935.1000.6	84.340	29.889

Aufwendungen (AW) für IT 2007 – 2008 in Euro Jahresabschluss der Ergebnisrechnung		
	2007	**2008**
Verbrauchsmaterial (Toner usw.) VHS	352	349
Verbrauchsmaterial (Toner usw.) Bücherei	329	793
Handbücher		134
Toner, Druckerpatronen AWW	1.035	962
Literatur und Zeitschriften	81	81
Wartungsverträge und Updates	54.398	56.870
Hardwarewartung	4.223	4.204
Reparatur und Wartung in Fachbereichen	198	178
Elektronikversicherung	676	867
Nutzung von Leitungsdiensten (Bücherei)	20	20
Leitungsentgelte versatel	9.326	13.707
Leistungen der citeq	317.444	295.198
Druckerverbrauchsmaterial	11.844	14.484

Aufwendungen (AW) für IT 2007 – 2008 in Euro Jahresabschluss der Ergebnisrechnung		
	2007	**2008**
Aufwendungen IT	11.842	16.698
Verwaltungsrechner Schulen	8.750	8.750
Abschreibungen Hardware	8.698	23.859
Abschreibungen Software	3.033	4.480
Miete TK-Anlage	42.743	33.876
Service, Dienstleistungen TK-Anlage	839	632
Summe	475.830	476.141

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, damit individuelle Besonderheiten, die keinen Bezug zur Sachaufgabe haben, im interkommunalen Vergleich außer Betracht bleiben.

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	**3,13**	**187.503**
dezentrale Stellenanteile für originäre IT-Aufgaben Hier sind Stellenanteile erfasst, die außerhalb der zentralen IT Aufgaben aus den oben genannten Bereichen wahrnehmen.	**0,69**	**36.773**
Stellenanteile für originäre IT-Aufgaben (funktionale Ebene) gesamt	**3,82**	**224.276**
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.	**0,17**	**9.892**
Stellen in der zentralen IT (aufbauorganisatorische Ebene) gesamt	**3,30**	**197.395**

Für die Stadt Coesfeld haben wir demnach innerhalb der zentralen IT-Abteilung 3,13 vollzeitverrechnete Stellenanteile ermittelt, die auf die Wahrnehmung originärer IT-Aufgaben entfallen.

Wir haben in der Mehrzahl der bisher geprüften mittleren kreisangehörigen Städte 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 Coesfeld wurden von Seiten des IT-Teams 0,69 dezentrale Stellenanteile für die Erledigung originärer IT-Aufgaben angegeben.

Die Dezentralität ist in diesem Falle jedoch nicht mit einer räumlichen Trennung verbunden. Die von der Stadt Coesfeld angegebenen dezentralen Anteile beziehen sich hauptsächlich auf die Betreuung des GIS. Diese Betreuung wird von einem Mitarbeiter des IT-Teams wahrgenommen, die Stellenanteile dafür werden jedoch vom Fachbereich 60 getra-

gen. Letztlich ist die Bereitstellung und Betreuung von IT in Coesfeld also konsequent zentralisiert ausgerichtet.

Letztlich ist es 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.

In diesem Zusammenhang ist sogenannte die Betreuungsquote interessant. Hierunter verstehen wir die Anzahl der BSAP, welche von seiten der IT betreut werden können.

Die Stadt Coesfeld weist mit 60 zu betreuenden BSAP eine im mittleren Bereich liegende Betreuungsquote der bisher in dieser Prüfrunde von uns betrachteten Städte auf. Derzeit liegt der interkommunale Mittelwert hier bei 62 zu betreuenden BSAP. Das Spektrum reicht dabei von lediglich 27 bis 102 zu betreuenden BSAP je vollzeitverrechneter IT-Stelle[5].

Beim interkommunalen Vergleich der Betreuungsquoten muss 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 detaillierte 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.

[5] Bei funktionaler Betrachtung; BSAP = 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.

Interkommunaler Kennzahlenvergleich

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

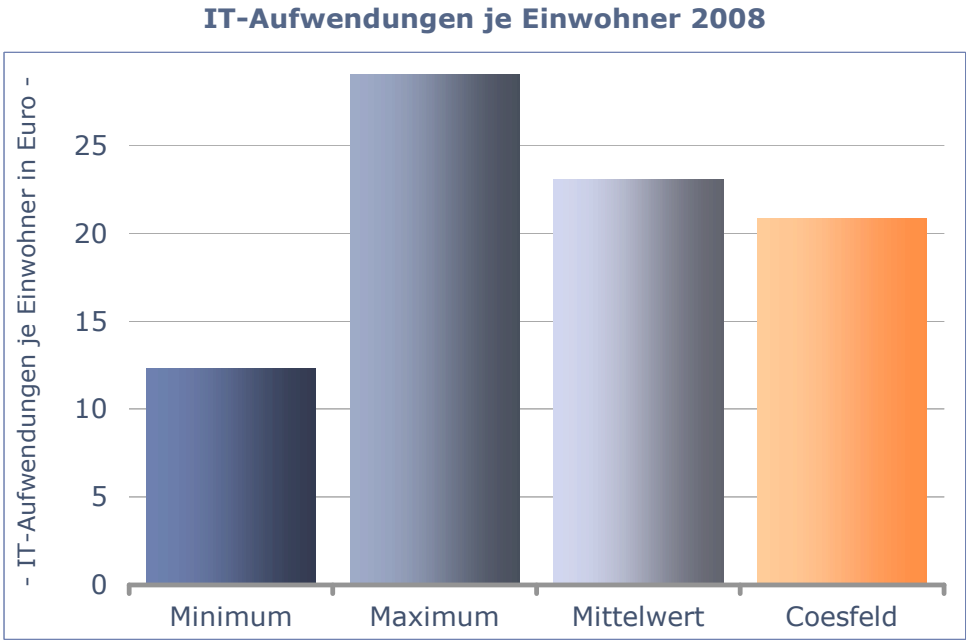
Grunddaten zur Kennzahlenbildung (Aufwendungen in Euro)	
IT-Sachaufwendungen (arithmetisches Mittel 4 Jahre)	472.431
Personalaufwendungen für originäre IT-Aufgaben (ermittelt nach KGSt-Pauschalen)	224.276
Sachkostenpauschale und Gemeinkostenzuschlag nach KGSt-Empfehlung	65.456
Gesamtaufwendungen IT	**762.163**

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 IT - 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.[6]

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

[6] 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: 25 Kommunen

IT-Aufwendungen je Einwohner in Euro			
Minimum	Maximum	Mittelwert	**Coesfeld**
12,29	29,02	22,67	**20,81**

Bei der auf Einwohner bezogenen Kennzahl positioniert sich die Stadt Coesfeld mit 1,86 Euro unter dem derzeitigen kommunalen Mittelwert. Bringt man alleine die IT-Aufwendungen in eine interkommunale Rangfolge, so erreicht die Stadt Coesfeld den sechsten Rang im Vergleich.

Hierbei ist jedoch zu bemerken, dass fünf der „günstigeren" Kommunen jedoch wesentlich weniger Leistungs- und Sicherheitsaspekte erfüllen, als die Stadt Coesfeld.

Diese Positionierung wird zum einen durch günstige Aufwendungen hinsichtlich des Personals erreicht. Hinsichtlich der Personalaufwendungen erreicht die Stadt Coesfeld ein Ergebnis, welches unter dem interkommunalen Mittelwert liegt.

IT-Personalaufwendungen je Einwohner in Euro			
Minimum	Maximum	Mittelwert	Coesfeld
3,53	11,07	6,48	6,12

Die Stadt Coesfeld muss 0,36 Euro weniger an Personalaufwand erbringen als der Schnitt der Vergleichskommunen. Dies läßt sich vor allem aus der Stellensituation im Bereich IT ableiten.

Zur besseren Darstellung des interkommunalen Vergleichs haben wir einen Bezug auf 100.000 Einwohner gesetzt.

IT-Stellen je 100.000 Einwohner			
Minimum	Maximum	Mittelwert	Coesfeld
6,08	18,07	11,14	10,42

Die Stadt Coesfeld weist letztlich 0,72 Stellen weniger im IT-Bereich aus, als der Schnitt der Kommunen im Vergleich, was sich entsprechend begünstigend auf die Personalaufwendungen im Rahmen der Betrachtung auswirkt.

Darüber hinaus wirken sich auch die der Gesamtkennzahl zugrunde zu legenden IT-Sachaufwendungen der Stadt Coesfeld positiv aus, wie ein interkommunaler Vergleich je Einwohner zeigt.

IT Sachaufwendungen je Einwohner je Einwohner in Euro			
Minimum	Maximum	Mittelwert	Coesfeld
8,47	19,10	14,77	12,90

Nach diesem Vergleich muss die Stadt Coesfeld 1,87 Euro weniger an IT-Sachaufwendungen aufbringen als das Mittel der Vergleichskommunen. Dieser Wert beeinflusst das oben dargestellte Gesamtergebnis der IT-Aufwendungen je Einwohner zusätzlich positiv.

Feststellung

Die Stadt Coesfeld erreicht im interkommunalen Vergleich der IT-Aufwendungen je Einwohner einen Wert, welcher unter dem Mittel der Kommunen im Vergleich liegt.

Dieser Wert ist vor dem Hintergrund der vorgefundenen Leistungs- und Sicherheitsstruktur positiv hervorzuheben.

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.

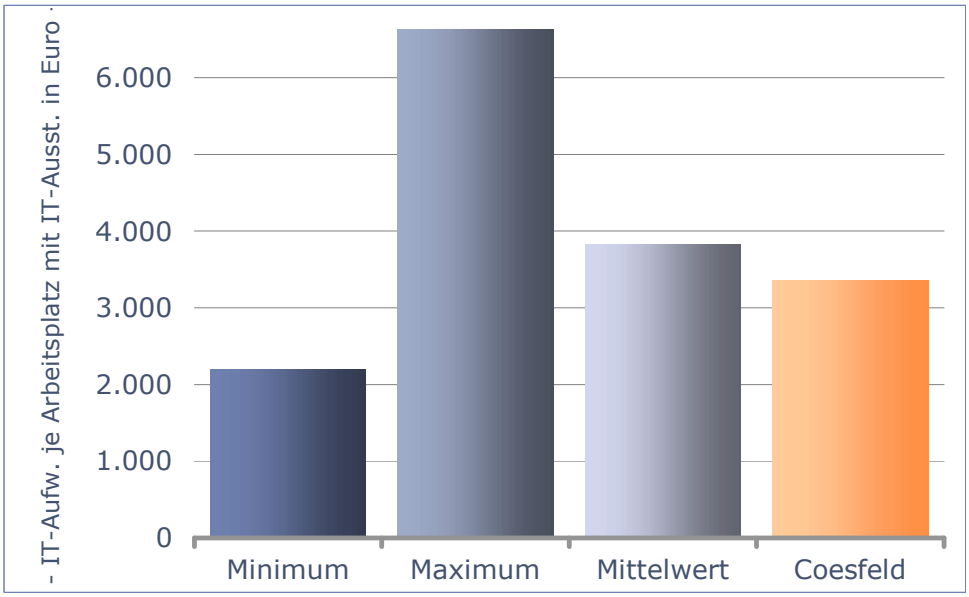
Bei der Interpretation und Wertung dieser Kennzahl muss jedoch beachtet werden, dass hier die Anzahl der BSAP im Verhältnis zu der Einwohnerzahl eine maßgebliche Rolle spielt. Die Positionierung im interkommunalen Vergleich wird durch eine – bezogen auf die Einwohner - niedrige Anzahl von BSAP negativ 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 Coesfeld 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 (= 227).

IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung in Euro			
Minimum	Maximum	Mittelwert	**Coesfeld**
2.196	6.630	3.873	**3.354**

Bei der auf Arbeitsplätze mit IT-Ausstattung bezogenen Kennzahl positioniert sich die Stadt Coesfeld mit 519 Euro unter dem derzeitigen interkommunalen Mittelwert.

Die günstigen IT-Gesamtaufwendungen bewirken letztlich auch bei Bezug auf den einzelnen BSAP eine Positionierung unterhalb des derzeitigen interkommunalen Mittelwertes.

Hinsichtlich der BSAP gilt dabei festzuhalten, dass die Stadt Coesfeld nicht mehr BSAP einsetzt, als die Kommunen im Vergleich.

Betrachten wir in diesem Zusammenhang nämlich die Quote der BSAP je tausend Einwohner (BSAP/1.000 EW), so bestätigt sich dieses Bild. Die Stadt Coesfeld erreicht hier eine am Mittelwert orientierte Quote von 6,21 BSAP/1.000 EW; der Mittelwert der bisher geprüften Kommunen liegt bei 6,32 BSAP/1.000 EW. Damit wird letztlich unterstrichen, dass die Stadt Coesfeld ihre BSAP günstiger betreiben kann, als das Mittel der Kommunen im Vergleich.

Die IT-Aufwendungen der Stadt Coesfeld liegen im interkommunalen Vergleich sowohl beim Einwohner- als auch beim Arbeitsplatzbezug unter dem Mittelwert. Im derzeitigen Vergleich erreicht die Stadt Coesfeld hinsichtlich der IT-Aufwendungen einen sehr guten sechsten Rang.

Die Betreuung der IT-Arbeitsplätze ist bei der Stadt Coesfeld ressourcenschonender als im Schnitt der Kommunen.

Finanzwirtschaftliche Steuerung im IT-Bereich

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

Dabei wurde deutlich, dass eine jederzeitige, auf einem System basierende Bereitstellung von Informationen in dem für interne Steuerungszwecke sinnvollen und wünschenswerten Umfang uneingeschränkt möglich ist.

Dies wurde unterstrichen durch den während der Prüfung bestehenden Kontakt zur Kämmerei und den von dieser Seite erfolgten inhaltlichen Unterstützungen.

Im Zusammenhang mit der Prüfung der IT sind neben der Transparenz der Haushaltsdaten, vor allem die von dort zur Verfügung gestellten „Sonderrichtlinien zur Ersterfassung und Erstbewertung bei der Stadt Coesfeld" hervorzuheben.

Diese umfassen differenzierte Aufstellungen zu Abschreibungen von Hardware, Software etc. und ermöglichen so, den Aufwand, welchen die IT bei der Stadt Coesfeld verursacht, zu ermitteln.

Diese Informationen sind neben inhaltlicher Qualität für eine wirksame Finanzsteuerung unerlässlich. Sie ermöglichen eine funktionierende Steuerung auf der finanzwirtschaftlichen Ebene, da spezifischen Kostenstrukturen erkennbar werden.

Feststellung

Die Stadt Coesfeld verfügt über Kosteninformationen bezüglich der IT, die eine Analyse und Darstellung der Kostenstrukturen ermöglichen.

Dabei lassen die Datenlage und -transparenz die Identifizierung der jeweiligen Kosten zu und ermöglichen einen aktiven Einfluß auf deren Höhe.

Nach Umstellung des kommunalen Haushaltes auf die Systematik des Neuen Kommunalen Finanzmanagements (NKF) im Jahre 2007 wurde das ein Produkt „Technikunterstützte Informationsverarbeitung“ (10.09) gebildet und im Hinblick auf konkrete Steuerungsfunktionen ausgestaltet.

Hierzu wurden sowohl allgemeine Ziele als auch Wirkungsziele formuliert und mit meßbaren Kennzahlen („IT-Wert je BSAP im interkommunalen Vergleich“) verknüpft.

Feststellung

Entsprechend der Zielsetzung des NKF, Produkte über Ziele und Kennzahlen zu steuern, wurden auch für den Bereich IT sowohl Produktziele benannt als auch Leistungsmengen, Kosten- und Zielkennzahlen aufgestellt, welche miteinander in Beziehung stehen.

Diese konsequente Ausgestaltung ist insgesamt positiv hervorzuheben.

IT-Sicherheit

Das Prüfmodul IT-Sicherheit beschäftigt sich insbesondere mit den Bereichen Datensicherheit und Datenschutz 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.

Die Prüfungsaufgabe wird überwiegend unter Verwendung von Checklisten erledigt. Diese Checklisten wurden anhand anerkannter Kriterien des BSI[7] 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
- Umsetzung Datenschutzgesetz

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

[7] Bundesamt für Sicherheit in der Informationstechnik

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. Somit 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. 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, 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 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.

Dort wo die Prüfung zu Empfehlungen und Feststellungen führt, sind entsprechende Ausführen in den Prüfbericht aufgenommen worden.

Unterlagen und Ansprechpartner

Im Rahmen der Prüfung lagen uns u.a. folgende Unterlagen vor:

- Dienstanweisung für den Einsatz der technikunterstützten Informationsverarbeitung
- Liste der Fachanwendungen und der dezentralen Ansprechpartner
- Dienstvereinbarung zur Telearbeit bei der Stadt Coesfeld
- Dienstanweisung für die Benutzung und Behandlung externer elektronischer Post
- Serverübersichten
- IT- Notfallhandbuch der Stadt Coesfeld
- Netzwerkplan
- Portbelegungsplan
- Darstellung der WAN / LAN- Verbindungen

Als Ansprechpartner standen uns der Leiter des Fachbereichs „IT" sowie alle Mitarbeiter des IT-Bereichs zur Verfügung.

Vorgehen im Rahmen der Prüfung der IT-Sicherheitsanforderungen

Die folgenden Prüfungsmethoden und -techniken wurden - 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[8], Sicherheitsgateway (Firewall).

Der Serverraum im technischen Rathaus in Coesfeld macht insgesamt einen sehr strukturierten und funktionalen Eindruck. Die Gesamtkonzeption des Serverraumes ist im interkommunalen Vergleich positiv zu sehen und ist als überdurchschnittlich einzustufen. Der zentrale Serverraum der Stadt Coesfeld befindet sich im Kellerbereich des Rathauses, ein weiterer Serverraum befindet sich in einem abgetrennten Teil der Räumlichkeiten der Stadtkasse. Die Serverräume befinden sich in einen guten Zustand und sind, insbesondere der Hauptserverraum im Keller, durch verschiedene Maßnahmen gegen unbefugte Zutritte geschützt. Besonders zu erwähnen ist hier die Videoüberwachungen dieser Räumlichkeiten per Webcam. Darüber hinaus sind Maßnahmen des vorbeugenden Brandschutzes positiv zu erwähnen, insondere die Gaslöschanlage im Hauptserverraum und das Racksystem mit Kühlung und Löscheinrichtung im Serverraum der Stadtkasse.

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

Serverraum

Wasserführende Leitungen

In Räumen oder Bereichen, in denen sich IT-Geräte mit zentralen Funktionen (z. B. Server) befinden, sollten Wasser führende Leitungen aller Art vermieden werden. Sind Wasser führende Leitungen unvermeidbar, müssen Vorkehrungen getroffen werden, einen Wasseraustritt möglichst frühzeitig zu erkennen bzw. die negativen Auswirkungen zu minimieren.

[8] Wide Local Area Network

Im Hauptserverraum der Stadt Coesfeld sind Wasserführende Leitungen (Heizungsanlage) vorhanden, die den Serverraum durchqueren.

Feststellung

Um den durch Wasser führende Leitungen entstehenden zusätzlichen Risiken angemessen zu begegnen, hat die Stadt Coesfeld Wasseraustrittsmelder installiert. Soweit Wasser führende Leitungen nicht vermeidbar sind, ist dies eine sehr begrüßenswerte Maßnahme.

Soweit Wasseraustrittsmeldesysteme installiert sind ist darauf zu achten, dass diese ihre Schutzfunktion auch bei Stromausfall behalten.

Empfehlung

Darüber hinaus sollten die Wasser führenden Leitungen regelmäßig auf Undichtigkeit untersucht werden (Früherkennung von Leckagen); das Ergebnis dieser Überprüfung sollte dokumentiert werden.

Technische und organisatorische Vorgaben für die Serverräume

Ein Serverraum sollte als geschlossener Sicherheitsbereich konzipiert sein. Dieser sollte möglichst gut zu sichernde Zugangstüren und Fenster haben, da alle Zutrittsmöglichkeiten überwacht werden müssen. Der Zutritt sollte durch hochwertige Zutrittskontrollmechanismen geschützt werden.

Diese generellen Anforderungen gelten für alle Räume, in denen Serverkomponenten zum Einsatz kommen. Ein Serverraum ist ein sicherheitsrelevanter Bereich, daher sollten dort nur die Administratoren der dort aufgestellten IT-Systeme Zutritt haben. Durch eine darauf abgestimmte Zutrittsregelung muss für eigene Mitarbeiter und wichtiger noch für nur zeitweilig Beschäftigte, z. B. zu Wartungsarbeiten tätige, sichergestellt werden, dass sie keinen Zugriff auf Systeme außerhalb ihres Tätigkeitsbereiches erhalten.

IT-Systeme, die von Externen betreut werden, sollten in separaten Räumen aufgestellt werden. Es ist außerdem zu überlegen, IT-Systeme mit unterschiedlichem Schutzbedarf oder aus verschiedenen Bereichen in getrennten Serverräumen aufzustellen, um den Kreis der Zutrittsberechtigten klein zu halten.

In einem Serverraum sollten sich auf keinen Fall Geräte oder Ausrüstung befinden, die den Zutritt für einen großen Benutzerkreis erforderlich machen, also z. B. Fax-Geräte oder Fotokopierer. Brennbare Materialen wie Druckerpapier sollten ebenfalls nicht in einem Serverraum gelagert werden.

Empfehlung

Es sollten generelle Regelungen, z.B. im Rahmen einer Dienstanweisung oder durch Erstellen von verbindlichen Leitlinien getroffen werden, um dem Schutzbedarf der Serverräume im obigen Sinne einen organisatorischen Rahmen zu geben.

Redundanzen im Serverumfeld

Grundsätzlich sind die von der Stadt Coesfeld betriebenen Server nicht redundant ausgelegt. Prinzipiell ist auch die doppelte Ausstattung mit Servern für den Fall von Serverausfällen nicht erforderlich, aber soweit für bestimmte Aufgaben oder Verfahren Verfügbarkeitsanforderungen an die IT gestellt werden, kann auch dies erforderlich sein. Eine redundante Auslegung vermeidet Arbeitsausfälle im Verwaltungsbetrieb, die ansonsten mehrere Tage andauern können (Minimierung von Ausfallrisiken).

Soweit hier Dienstleistungen und Fachverfahren des Rechenzentrums der Stadt Münster (citeq) genutzt werden, ist durch die dort vorgehaltene Hochverfügbarkeitsumgebung gewährleistet, dass Ausfälle minimiert und Schäden auf ein geringst mögliches Maß reduziert werden.

In Gesamtzusammenhang ist hinsichtlich der Risikominimierung positiv anzumerken, dass die Stadt Coesfeld eine Virtualisierungsumgebung plant. Dies ermöglicht die Realisierung einer höheren Ausfallsicherheit.

Feststellung

Die Implementierung von Virtualisierungstechnologien bei der Stadt Coesfeld ist ein wichtiger Schritt, um die Ausfallsicherheit der Server- Systeme zu erhöhen und bei konsequenter Umsetzung auch Einspareffekte zu erzielen. Der geplante Aufbau der Virtualisierungsumgebung ist in diesem Zusammenhang sehr positiv zu sehen

Redundanzen im Speicherumfeld

Die Stadt Coesfeld betreibt ihr Serverumfeld derzeit noch nach dem Prinzip der dedizierten Server mit verteiltem Festplattenspeicher, d.h. dass die Datenhaltung generell auf zahlreichen Servern verteilt erfolgt und von dort auch im Rahmen der Datensicherung auf Datenbänder gesichert wird. Dies ist generell nicht nachteilig, allerdings bedeutet dies im Regelfall, dass der auf zahlreiche Server verteilte Datenspeicher nicht in gleicher Weise wirtschaftlich verwaltet werden kann, wie dies in zentralen Speichersystemen möglich ist. Darüber hinaus sind auch hinsichtlich der Datensicherung bei zentralen Speichersystemen Wirtschaftlichkeitsaspekte gegeben.

Der größte Vorteil einer zentralen Datenhaltung wird jedoch dadurch erzielt, dass neben einem effizienten und effektiven Aufbau eines redundanten Speicherumfeldes auch die Grundlage für eine Hochverfügbarkeitsumgebung geschaffen werden kann.

Feststellung

Die Stadt Coesfeld plant die Implementierung eines zentralen Speichersystems (SAN); dies ist unter verschiedenen Aspekten sehr zu begrüßen und lässt in Verbindung mit dem geplanten Aufbau einer Servervirtualisierung den Aufbau einer sehr wirtschaftlichen und hoch verfügbaren Server- und Speicherinfrastruktur zu. Dies wird sich dann auch positiv auf die Verfügbarkeiten der Server und der damit bereit gestellten Anwendungen im Rahmen der Notfallvorsorge und Notfallbehandlung positiv auswirken.

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 Notfallvorsorge hat die Stadt Coesfeld ein vorbildliches Vorsorgekonzept, abgebildet in einem sehr umfänglichen Notfallhandbuch, vorliegen. Die Erstellung des Notfallkonzeptes erfolgte im Anschluss an eine Empfehlung im Rahmen der überörtlichen Prüfung 2006. Bisher konnte in der interkommunalen Betrachtung keine vergleichbare Notfallvorsorge festgestellt werden, und lässt hinsichtlich der erforderlichen Bemühungen, einen angemessenen Grundschutz für den IT- Betrieb zu erreichen, keine Wünsche offen.

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 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-Sicherheits-management bezeichnet.

Leitlinie

Empfehlung

Die Leitaussagen zur IT-Sicherheitsstrategie sollten in einer IT-Sicherheitsleitlinie zusammengefasst werden, um die zu verfolgenden IT-Sicherheitsziele und das angestrebte IT-Sicherheitsniveau für alle Mitarbeiterinnen und Mitarbeiter zu dokumentieren.

Mit der IT-Sicherheitsleitlinie bekennt sich die Behördenleitung sichtbar zu ihrer Verantwortung für IT-Sicherheit.

Die IT-Sicherheitsleitlinie sollte kurz und übersichtlich sein, dabei aber mindestens die folgenden Aspekte enthalten:

- Der Stellenwert der IT-Sicherheit und die Bedeutung der IT für die Institution müssen dargestellt werden.
- Die IT-Sicherheitsziele und der Bezug der IT-Sicherheitsziele zu den Behördenzielen und Aufgaben der Institution müssen dabei erläutert werden.
- Die Kernelemente der IT-Sicherheitsstrategie sollten genannt werden.

- Die Leitungsebene muss allen Mitarbeitern aufzeigen, dass die IT-Sicherheitsleitlinie von ihr getragen und durchgesetzt wird. Ebenso muss es Leitaussagen zur Erfolgskontrolle geben.

- Die für die Umsetzung des IT-Sicherheitsprozesses etablierte Organisationsstruktur muss beschrieben werden.

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.

Empfehlung

Es wird die Benennung eines IT-Sicherheitsbeauftragten empfohlen.

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 zur 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.

Die Funktion des IT-Sicherheitsbeauftragten kann von einer qualifizierten Mitarbeiterin oder einem qualifizierten Mitarbeiter neben anderen Aufgaben wahrgenommen werden. Maßgeblich ist, dass dem IT-Sicherheitsbeauftragten ausreichend Zeit zur sachgerechten 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 Coesfeld 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 Coesfeld 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 gegebenenfalls 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

> **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.

Fragenkreis „Backup und Archivierung"

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

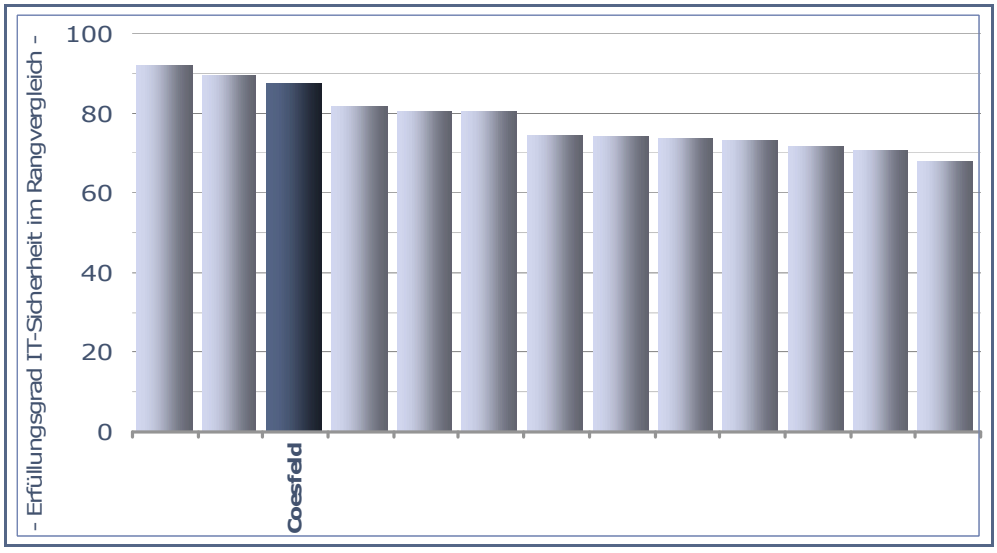
Erfüllungsgrad IT- Sicherheit

Im Interkommunalen Vergleich der umgesetzten Maßnahmen zum Erreichen eines Mindeststandards an IT- Sicherheit[9] erzielt die Stadt Coesfeld derzeit Rang 3 von bisher 23 gewerteten Prüfungsergebnissen. Der mit dieser Prüfung festgestellte Gesamterfüllungsgrad beträgt für Coesfeld 87,3 Prozent, der kommunale Mittelwert liegt derzeit bei 72,9 Prozent.

Die in der Gesamtbetrachtung erreichte Positionierung ist einerseits ein sehr gutes Ergebnis für Coesfeld und andererseits im interkommunalen Vergleich eines der besten Ergebnisse überhaupt. Darüber hinaus sind in Coesfeld bereits verschiedene Maßnahmen in der Planung (Hochverfügbarkeitsumgebung, Virtualisierung, IT- Sicherheitsmanagement), die in den kommenden Jahren perspektivisch zu einem Erfüllungsgrad von deutlich über 90 Prozent führen werden.

In diesem Zusammenhang ist auch darauf hinzuweisen, dass der bisher höchste Erfüllungsgrad im interkommunalen Vergleich bei 92 Prozent liegt.

Interkommunale Rangfolge IT-Sicherheit



[9] Auszug aus dem Maßnahmenkatalog des BSI, siehe Anlage zum Prüfbericht

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 Coesfeld ordnungsgemäß personell besetzt; ein Stellvertreter ist bestellt.

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

Die von der Stadt Coesfeld zur automatisierten Verarbeitung personenbezogener Daten eingesetzten Verfahren sind derzeit noch nicht gemäß den Anforderungen des § 8 Abs. 1 Nr. 1 bis 11 DSG NRW hinreichend dokumentiert.

Die Stadt hat jedoch Maßnahmen getroffen, um ein den gesetzlichen Bestimmungen entsprechendes Verzeichnis zu erstellen.

Empfehlung

Die Stadt Coesfeld sollte die Aktivitäten zur 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 23.02.2010

Präsident der Gemeindeprüfungsanstalt

Nordrhein-Westfalen

Im Auftrag

Michael Kuzniarek

Überörtliche Prüfung Informationstechnologie
- Erhebungsbogen IT-Sicherheit -

Name der Kommune:
Stadt Coesfeld

Gesprächstermin:
17.11.2009

Prüfer:
AE

Gesprächspartner in der Kommune:
Herr Eising, Herr Volmer, Herr Eink

Fragenkreis: IT-Räume und Infrastrukturaufbau

Serverraum

Baustein Serverraum:
von 21 Maßnahmen 13x JA, 4x NEIN, 3x teilweise, 1x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Angepasste Aufteilung der Stromkreise	ja	
Handfeuerlöscher	ja	vor den Serverräumen sind Feulerlöscher griffbereit installiert; die Feuerlöscher sind aktuell gewartet
Verwendung von Sicherheitstüren und -fenstern	ja	der Serverraum im Keller ist durch eine Sicherheitstür (Stahl) abgesichert; Fenster sind nicht vorhanden; der Serveraum im Kassenbereich ist verschlossen (Glas/Stahl- Kombination), Die Fenster sind verschlossen und von außen nicht unmittelbar zugänglich
Geschlossene Fenster und Türen	ja	s.o.
Gefahrenmeldeanlage/Brandmelder	ja	Brandmeldesystem mit Anbindung an die Feuerwache
Abgeschlossene Türen	ja	
Vermeidung von wasserführenden Leitungen	teilw.	im Serverraum im Keller ist eine wasserführende Leitung (Heizung) vorhden; zu Absicherung ist ein Wassermeldessystem mit SMS und Email- Meldung installiert; im Serverraum in der Stadtkasse ist ein Wasseraustrittsschutz für die Klimaanlage installiert
Überspannungsschutz	ja	
Not-Aus-Schalter	entfällt	im Serverraum im Keller ist eine Gaslöschanlage installiert, außerdem wird im Notfall eine autmatische Abschaltung der Server vorgenommen; der Serverraum im Kassenbereich verfügt über ein Serverrack mit Löscheinrichtung (Firma Rittal)
Klimatisierung	ja	
Lokale unterbrechungsfreie Stromversorgung	ja	mehrere USV- Geräte der Firma APC
Fernanzeige von Störungen	ja	per Mail uind SMS
Redundanzen in der technischen Infrastruktur (ohne Storage)	ja	Dateien werden regelmäßig repliziert, so dass im Schadenfall z.B. ein weiterer Fileserver die erforderlichen Daten zur Verfügung stellen kann; künftig ist eine Virtualisierungsumgebung geplant
Technische und organisatorische Vorgaben für Serverräume	nein	
Brandschutz von Patchfeldern	teilw.	im Serveraum im Keller durch Gasanlage geschützt, im Kassenbereich geschützt, soweit im Racksystem untergebracht
Zutrittsregelung und -kontrolle	ja	es sind Webcams mit Bewegungssensoren installiert, wodurch eine Kontrolle erfolgen kann, Zutritt haben lediglich die Mitarbeiter der IT und die Hausmeister; Zutrittsregelung erfolgt über "Schlüsselgewalt"
Rauchverbot	ja	
Verwendung von hochverfügbaren Architekturen	nein	Für 2011 f ist eine Virtualsierungsumgebung und der Einsatz eines SAN vorgesehen
Anschluss an SAN, NAS, DAS	teilw.	SAN- System soll eingeführt werden, bis dahin liegen die Daten auf den dezidierten Servern und werden von dort gesichert und gespiegelt
Storage System redundant	nein	
Wird eine Servervirtualisierung eingesetzt?	nein	

IT-Verkabelung

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

Maßnahmen	erfüllt?	Bemerkungen
Welche Verkabelungsart kommt zum Einsatz?	ja	Ehternet CAT5 Standard und LWL- Leitungen für die Anbindung der Außenstellen
Netz-Topologie	ja	Standard erfüllt
Erneuerung der IT-Verkabelung	ja	fortlaufend, zuletzt 1998
Redundanzen für die Primärverkabelung	ja	
Redundanzen für die Gebäudeverkabelung	ja	Die Switche sind zusätzlich über USV abgesichert
Brandabschottung von Trassen	ja	soweit erkennbar
Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht	ja	s.o.

Ausreichende Trassendimensionierung	ja	
Materielle Sicherung von Leitungen und Verteilern	ja	
Dimensionierung und Nutzung von Schranksystemen	teilw.	im Serverraum im Keller sind die Seversystem noch nicht als Racksysteme implementiert, dies ist jedoch in Planung
Neutrale Dokumentation in den Verteilern	ja	
Laufende Fortschreibung und Revision der Netzdokumentation	ja	Netzdokumentation liegt elektronisch vor und wird aktuell gepfelgt

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
Proxy Server 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 Proxy-Servern 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 9x JA, 0x NEIN, 0x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Existiert bei Notebooks Homogenität?	ja	es werden überwiegend HP Notebooks oder FU/SI- Notebooks eingesetzt

Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz	ja	
Einsatz von Diebstahl-Sicherungen	ja	soweit sinnvoll und erforderlich
Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung	ja	es besteht eine IT- Dienstanweisung, die generellle Regelungen beinhaltet
Regelmäßiger Einsatz eines Anti-Viren-Programms	ja	McAffee (ePolicie-Registrator)
Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme	ja	EFS
Sichere Kommunikation von unterwegs	ja	über RSA und Citrix - Einwahl (Gateways der Citeq)
Sicherer Anschluss von Notebooks an lokale Netze	ja	
Datensicherung bei mobiler Nutzung des IT-Systems	ja	

Allgemeiner Client

Baustein Allgemeiner Client:
von 14 Maßnahmen 11x JA, 1x NEIN, 2x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Existiert ein homogenes Umfeld bei den Client PC? Hardware	ja	
Existiert ein homogenes Umfeld bei den Client PC? Software	ja	es wird Xpprof und Vista eingesetzt; neue Rechner sollten Windows 7 ausgestattet werden
Austauschzyklen ?	nein	bis zu 7 Jahren
Wie alt sind die Geräte?		s.o.
Wird ein Systemmanagement eingesetzt?	ja	
Wird Remote Desktop genutzt?	ja	
Herausgabe einer PC-Richtlinie	teilw.	es bestehten generelle Regelungen in der Dienstanweisung TUI
Dokumentation der Systemkonfiguration	ja	es wird ein Inventarisierungstool eingesetzt
Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	ja	es wird ein WSUS- Server eingesetzt
Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz	teilw.	Teilaspekte werden im Rahmen der Notfallvorsorge abgehandelt
Geregelte Außerbetriebnahme eines Clients	ja	Festplatten werden phys. Zerstört
Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung	ja	
Regelmäßiger Einsatz eines Anti-Viren-Programms	ja	
Einrichten einer Referenzinstallation für Clients	ja	
Regelmäßige Datensicherung	ja	auf den Clients erfolgt keine lokale Datenhaltung

Fragenkreis: IT-Management

Sicherheitsmanagement

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

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

Sicherheitsorganisation

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

Maßnahmen	erfüllt?	Bemerkungen
Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz	ja	
Vergabe von Zutrittsberechtigungen	ja	

Vergabe von Zugangsberechtigungen	**ja**	es besteht ein abgestimmtes Verfahren mit dem Personalteam
Vergabe von Zugriffsrechten	**ja**	s.o.
Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln	**ja**	
Schlüsselverwaltung	**ja**	
Kontrollgänge	**ja**	bei Bedarf bei den Clients, im Serverbreich täglich

Sicherheit Personal

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

Maßnahmen	erfüllt?	Bemerkungen
Geregelte Einarbeitung/Einweisung neuer Mitarbeiter	**ja**	
Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen	**ja**	
Schulung vor Programmnutzung	**ja**	
Schulung zu IT-Sicherheitsmaßnahmen	**ja**	mit einem Sicherheitsprogramm "Behörden- Sicherheitstraining BITS" des StGB
Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern	**ja**	es besteht ein abgestimmtes Verfahren mit dem Personalteam
Schulung des Wartungs- und Administrationspersonals	**ja**	Schulungen sind bei Bedarf jederzeit möglich
Personaleinsatz und -qualifizierung	**ja**	
Vertraulichkeitsvereinbarungen	**ja**	

Notfallvorsorgekonzept

Baustein Notfallvorsorgekonzept:
von 15 Maßnahmen 15x JA, 0x NEIN, 0x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Erstellung einer Übersicht über Verfügbarkeitsanforderungen	**ja**	
Notfall-Definition, Notfall-Verantwortlicher	**ja**	
Erstellung eines Notfall-Handbuches	**ja**	das Notfallhandbuch wurde ich Nachgang der Prüfung 2005 erstellt; hieru wurde die Software der Firma Seccon eingesetzt
Dokumentation der Kapazitätsanforderungen der IT-Anwendungen	**ja**	
Definition des eingeschränkten IT-Betriebs	**ja**	geht aus dem Notfall- Handbuch hervor
Untersuchung interner und externer Ausweichmöglichkeiten	**ja**	
Regelung der Verantwortung im Notfall	**ja**	
Alarmierungsplan	**ja**	
Notfall-Pläne für ausgewählte Schadensereignisse	**ja**	
Erstellung eines Wiederanlaufplans	**ja**	
Durchführung von Notfallübungen	**ja**	
Erstellung eines Datensicherungsplans	**ja**	
Ersatzbeschaffungsplan	**ja**	
Abschließen von Versicherungen	**ja**	
Redundante Kommunikationsverbindungen	**ja**	Der Router zur Datenzentrale ist hardwareseitig nicht redundant ausgelegt, kann aber kurzfristig durch die Citeq ersetzt werden

Hard- und Softwaremanagement

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

Maßnahmen	erfüllt?	Bemerkungen
Regelung des Passwortgebrauchs	**ja**	
Hinterlegen des Passwortes	**ja**	Verwaltung der Passwörter per Software; Replikat auf CD in Tresor eingelagert
Dokumentation der Systemkonfiguration	**ja**	im Rahmen des Notfallhandbuches
Regelung für die Einrichtung von Benutzern / Benutzergruppen	**ja**	s.o. (abgesprochenes Verfahren mit dem Personalteam)
Dokumentation der zugelassenen Benutzer und Rechteprofile	**ja**	insbesondere über die Funktionen der Domänenverwaltung
Dokumentation der Veränderungen an einem bestehenden System	**ja**	im Rahmen des Notfallhandbuches und der Inventardatenbank
Informationsbeschaffung über Sicherheitslücken des Systems	**ja**	über Fachzeitschriften, Newsletter des BSI, etc.
Software-Abnahme- und Freigabe-Verfahren	**ja**	Bei Softwareeinkauf von Drittanbietern wird auf eine angemssene Referenz Wert gelegt
Kontrolle der Protokolldateien	**ja**	im Rahmen der Überwachung der Serverfunktionalitäten; es wird auch eine Software für die Überwachung eingesetzt (Total Network Monitor)

Virenschutz

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

Maßnahmen	erfüllt?	Bemerkungen

Erstellung eines Computer-Virenschutzkonzepts	**ja**	es wird das Virenschutzkonzept der Citeq angewendet
Aktualisierung der eingesetzten Computer-Viren-Suchprogramme	**ja**	
Regelmäßiger Einsatz eines Anti-Viren-Programms	**ja**	
Verhaltensregeln bei Auftreten eines Computer-Virus	**ja**	

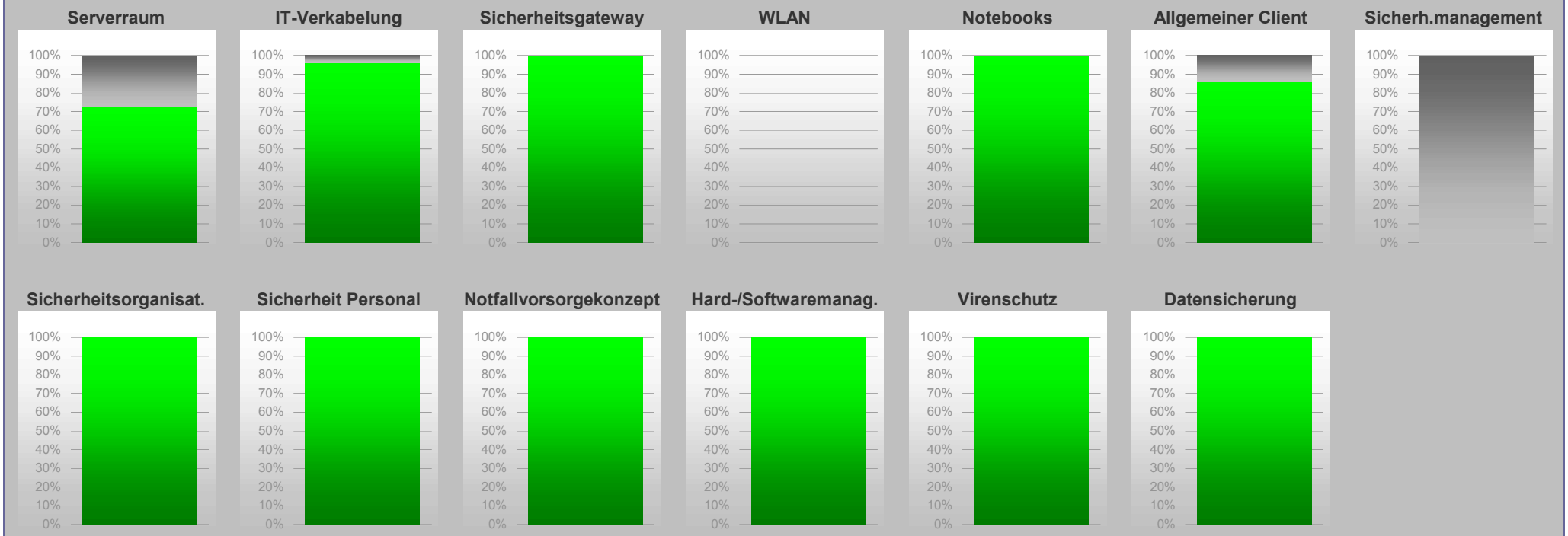
Fragenkreis: Backup und Archivierung

Datensicherung

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

Maßnahmen	erfüllt?	Bemerkungen
Verpflichtung der Mitarbeiter zur Datensicherung	entfällt	Datensicherung ist auf den lokalen Datenträger nicht zulässig, bei den Notebooks erfolgt eine automatische Datensicherung, sobald eine Anmeldung im LAN erfolgt
Beschaffung eines geeigneten Datensicherungssystems	**ja**	
Geeignete Aufbewahrung der Backup-Datenträger	**ja**	Die Tages- und Wochenbänder werden in einem Stahlschrank aufbewahrt, die Monatssicherung sind im Tresor der Stadtkasse verwahrt
Sicherungskopie der eingesetzten Software	**ja**	
Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen	**ja**	
Regelmäßige Datensicherung	**ja**	tägliche Vollsicherung
Entwicklung eines Datensicherungskonzepts	**ja**	Festlegungen sind im Rahmen der Notfallvorsorge getroffen worden
Dokumentation der Datensicherung	**ja**	es werden Log- Files erzeugt un din einem sep. Ordner aufbewahrt
Übungen zur Datenrekonstruktion	**ja**	

Überörtliche Prüfung Informationstechnologie
- Detail-Erfüllungsgrade Stadt Coesfeld -



Anlage 2 zum Prüfbericht Informationstechnologie

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