Beratung · Prüfung · Service

Überörtliche Prüfung Informationstechnologie des Kreises Borken

Gemeindeprüfungsanstalt
Nordrhein-Westfalen

Heinrichstraße 1 · 44623 Herne
Postfach 101879 · 44608 Herne

Inhaltsverzeichnis

Überblick

Zur kommunalen IT-Landschaft in NRW

Nach unseren bisherigen Schätzungen werden in den kommunalen Körperschaften in NRW mehr als 500 Millionen Euro pro Jahr für den Einsatz von Informations- und Telekommunikationstechnologien aufgewendet.

Die Bedeutung der Informationstechnik für die Erfüllung der vielfältigen Aufgaben der öffentlichen Verwaltung steigt Jahr für Jahr an. Insgesamt sind viele Bereiche der Verwaltung ohne zuverlässige und auf die Bedürfnisse der Anwender ausgerichtete IT-Systeme heute nicht mehr vorstellbar. Datenschutz und die optimale Einbindung der IT in die Geschäftsprozesse[1] der Verwaltung sind zu zentralen Themen geworden.

Der Einsatz moderner und komplexer IT stellt sehr hohe Anforderungen. In dieser Hinsicht unterscheidet sich der IT-Service, der von einer Verwaltung in eigener Verantwortung erbracht wird, kaum von dem eines Gebietsrechenzentrums, etwa eines IT-Zweckverbandes.

Um den hohen Anforderungen an Qualität und Verfügbarkeit der IT in der öffentlichen Verwaltung gerecht zu werden, wandelt sich die kommunale IT-Organisation zunehmend von rein technikorientierten Funktionsbereichen zu „kundenorientierten Anbietern" von IT-Leistungen.

Die organisatorischen Lösungen, die wir in den Kommunen vorfinden, sind sehr vielfältig. Sie reichen von einer umfassenden Autonomie bis hin zur kompletten Auslagerung. In allen Fällen bleibt die Gesamtverantwortung für den Einsatz von IT jedoch bei der Behördenleitung.

[1] Geschäftsprozess: inhaltlich, abgeschlossene und sachlogische Folge von Aktivitäten, die der Erfüllung eines Oberziels dient.

Zur GPA NRW und zur Prüfung

Grundlagen

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

Bürger, Politik und Verwaltungsleitung erwarten gerade vom IT-Service als Betriebsaufgabe in Zeiten der Haushaltskonsolidierung zu Recht besondere Beiträge in Richtung Sparsamkeit und Wirtschaftlichkeit. Unsere Prüfung zeigt auf, ob hier Potenziale bestehen. Gleichzeitig wollen wir aber auch das Bewusstsein für Folgendes schärfen:

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

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

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

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

Prüfungsbericht

Adressat des Prüfungsberichtes ist die Steuerungsebene des Kreises.

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

- Aufwand
- Finanzwirtschaftliche Steuerung
- IT-Sicherheit
- Datenschutz
- Lizenzmanagement.

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

Bestimmte Ergebnisse unserer Untersuchung heben wir im Bericht in Form einer **Feststellung** hervor, die ermittelte Sachverhalte kurz zusammenfassend beschreibt. Diese Feststellungen können je nach Sachverhalt positive oder negative Wertaussagen enthalten. Zu negativen Feststellungen ist eine Rückäußerung der Verwaltung nur dann erforderlich, wenn im Bericht ausdrücklich um Stellungnahme gebeten wird.

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

Der Prüfbericht beginnt mit einer **Managementübersicht**. In der Folge werden die Prüfungsfelder der IT-Aufwendungen, der IT-Sicherheit und des Datenschutzes aufgearbeitet und dargestellt.

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.

In der als Anlage beigefügten Checkliste zur IT-Sicherheit ist im Detail ersichtlich, welches Spektrum unsere Prüfung in diesem Bereich umfasst und wie sich der Kreis Borken im interkommunalen Vergleich positioniert.

Methodik

Unser Prüfungsprozess vollzieht sich generell in drei Schritten:

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

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 und Leistungen - zu betrachten und zu bewerten.

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

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

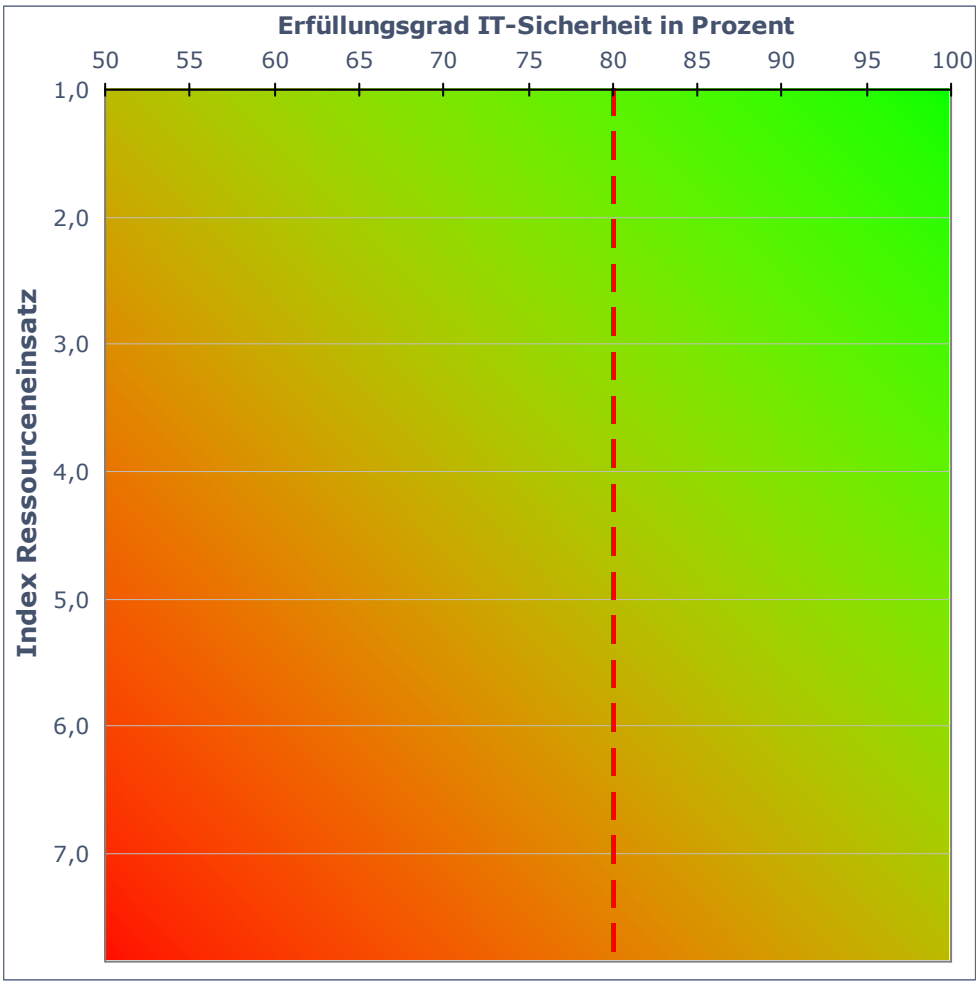
Der von uns gewählte Ansatz basiert auf der Grundannahme, dass die elektronische Verarbeitung von Informationen ein hohes, teilweise auch explizit definiertes[2] Maß an Sicherheit erfordert, um diese Daten vor Verlust, ungewollter Veränderung, unberechtigtem Zugriff durch Dritte und anderen Risiken zu 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 des Kreises Borken bereitzustellen und zu betreuen, mit dem geringsten Mitteleinsatz erfüllt wird.

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

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 den Kreis Borken 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.

Um die Ergebnisse der Prüfung interkommunal darzustellen und insbesondere auch in Relation zu setzen, bilden wir die erreichten Positionierungen sowohl hinsichtlich der Aufwendungen als auch hinsichtlich des Grades der Aufgabenerfüllung beim IT-Grundschutz in einer Matrixdarstellung ab:



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

Auf der Y-Achse wird die Position des geprüften Kreises unter dem Betrachtungsschwerpunkt des Ressourceneinsatzes abgebildet. Dazu wurde für die im Abschnitt „IT-Aufwendungen" behandelten Berichtskennzahlen

- IT-spezifische Aufwendungen je Arbeitsplatz mit IT-Ausstattung,
- IT-spezifische Aufwendungen je Einwohner

sowie den weiteren Analysekennzahlen

- Betreuungsquote,
- Bildschirmarbeitsplätze je 1.000 Einwohner und
- IT-Stellen je 100.000 Einwohner

die jeweilige Rangposition im interkommunalen Vergleich ermittelt und daraus ein Index für die Positionsbestimmung auf der Y-Achse errechnet. Diese Vorgehensweise ermöglicht es, die Unterschiede der Kennzahlenausprägung in der Gesamtheit annähernd proportional darzustellen.

Aus der erreichten Positionierung wird ersichtlich, in welchem Verhältnis das objektive Maß an IT-Sicherheit zu den eingesetzten Mitteln steht. Das individuelle Ergebnis der betrachteten Kreise ergibt zusammen mit den weiteren, anonymisierten Ergebnissen des aktuellen Vergleichs ein Abbild der kommunalen IT-Landschaft in Nordrhein-Westfalen.

Anhand dieser Darstellung versuchen wir zudem aufzuzeigen, in welchem Bereich (Ressourceneinsatz oder IT-Sicherheit) der größte Handlungsbedarf besteht.

Zur IT-Prüfung des Kreises Borken

Informationen zum Prüfungsablauf

Wir haben die Prüfung im Kreis Borken vom 20.07. bis 07.12.2010 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.

Soweit dies für die Analyse oder Darstellung von Sachverhalten erforderlich oder zweckmäßig ist, haben wir neben aktuellen Daten bei Bedarf auch Informationen aus Jahren vor dem vierjährigen Betrachtungszeitraum (2006 bis 2009) berücksichtigt.

Geprüft haben:

Alexander Ehrbar

Michael Neumann

Ulrich Sdunek

Wir haben das Prüfungsergebnis am 20.12.2010 im Rahmen eines Abschlussgesprächs erörtert.

Der Entwurf des Prüfberichts wurde übersandt.

Ausgangslage im Kreis Borken

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

Die zentrale Bereitstellung und Betreuung der IT ist im Kreis Borken aufbauorganisatorisch als Abteilung 10.3 (IT-Steuerung und Service) und Abteilung 10.4 (Technischer Betrieb) dem Fachdienst 10, Organisation und IT, angegliedert. Durch eine Umorganisation der früheren Fachdienste 16 (IT) und 17 (IT-Strategie und Organisation) im Frühjahr 2010 wurden Zuständigkeiten gebündelt, da ursprünglich fünf Organisationseinheiten für die Bereitstellung und Betreuung der IT verantwortlich waren.

Im Betrachtungsjahr 2009 waren der zentralen IT 16 Mitarbeiter zugeordnet.

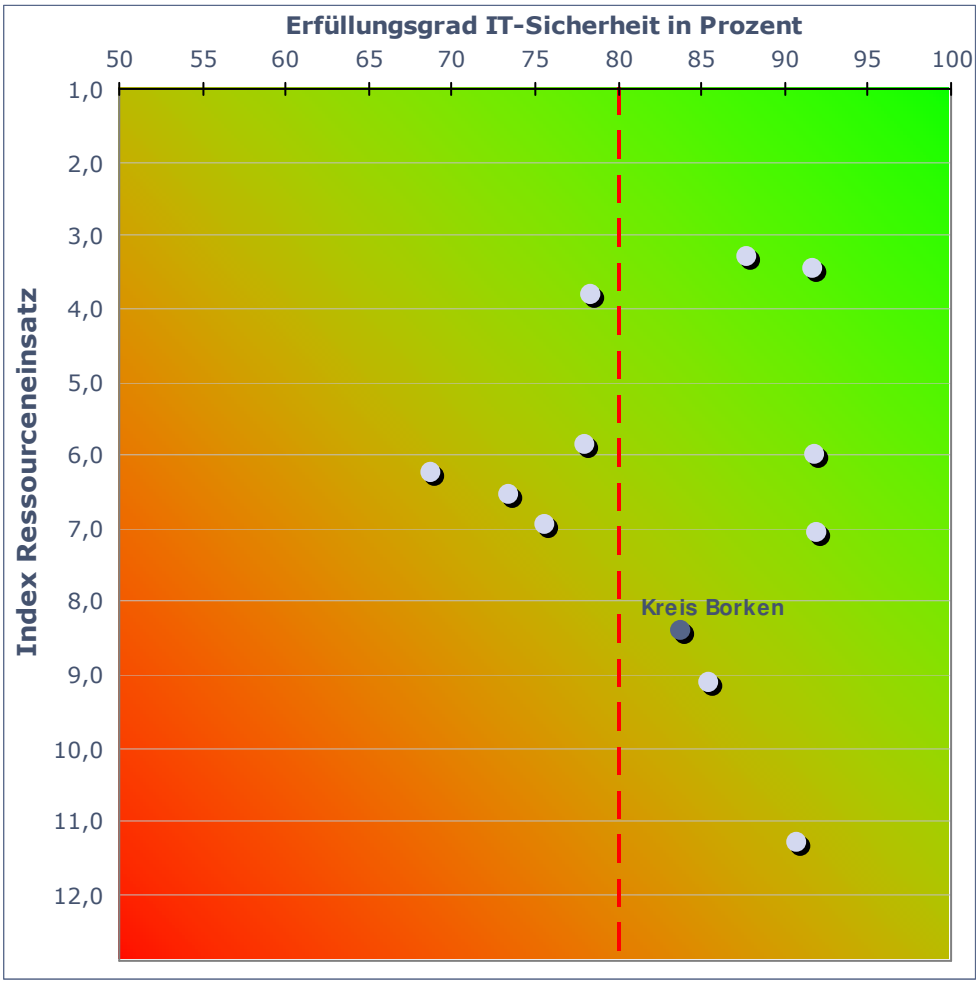
Der Kreis Borken betreibt seine IT weitgehend autonom und in eigener Verantwortung, nimmt aber als Drittkunde Leistungen des IT-Zweckverbandes KRZN in Kamp-Lintfort in Anspruch. Der Fachdienst 10 hat mit dem KRZN für die Verträge über die Bereitstellung von Fachanwendungen ein einheitliches Laufzeitende zum 31.12.2015 ausgehandelt; Zielsetzung ist es, zu diesem Zeitpunkt die Wirtschaftlichkeit der Leistungen zu überprüfen.

Im Bereich des Katasterwesens besteht eine öffentlich-rechtliche Kooperation mit dem Kreis Steinfurt, die historisch aus dem früher gemeinsam betriebenen Rechenzentrum KDZ Borken/Steinfurt hervorgegangen ist.

Managementübersicht

Mit dieser Managementübersicht wollen wir den für die Gesamtsteuerung in der Verwaltung Verantwortlichen einen konzentrierten Überblick über die wesentlichen Ergebnisse der Prüfung geben.

Gesamtergebnis in Matrixdarstellung



Die Matrixdarstellung zeigt, dass der Kreis Borken hinsichtlich der Relation des Ressourceneinsatzes zum Grad der Aufgabenerfüllung im Vergleich eine Position im unteren Mittelfeld einnimmt.

Der Erfüllungsgrad in der IT-Sicherheit liegt mit rund 84 Prozent über dem von uns empfohlenen Schwellenwert von 80 Prozent und entspricht fast genau dem Mittelwert der bisher geprüften Kreise. Negativ wirkt sich auf die Positionierung des Kreises Borken der im Vergleich relativ hohe Ressourceneinsatz aus. Die grafische Darstellung zeigt, dass ein

noch höheres Sicherheitsniveau von mehreren Kreisen mit einem teils erheblich günstigeren Ergebnis in der betriebswirtschaftlich orientierten Bewertung erreicht wird.

Die IT-Gesamtaufwendungen je Arbeitsplatz betragen 3.684 Euro und liegen damit oberhalb des interkommunalen Mittelwertes von 3.524 Euro. Die Aufwendungen je Einwohner im Kreisgebiet betragen 9,41 Euro und überschreiten damit den Mittelwert von 8,41 Euro um einen Euro; gleichwohl bleibt ein deutlicher Abstand zum Maximum von 10,94 Euro gewahrt.

Die Kennzahlenausprägung fällt bei der arbeitsplatzbezogenen Betrachtung weniger negativ aus, weil im Verhältnis zur Einwohnerzahl eine relativ große Zahl von Verwaltungsarbeitsplätzen mit IT-Ausstattung vorhanden ist; im Vergleich zu anderen Kreisen werden die Gesamtkosten also auf eine größere Verteilungsmenge verrechnet.

Eine eindeutige Ursache für die relativ ungünstige Positionierung ließ sich im Rahmen der Prüfung nicht identifizieren. So liegt die Stellenausstattung für die Wahrnehmung von IT-Aufgaben zwar über dem Durchschnitt, ist aber nicht allein für den insgesamt hohen Ressourceneinsatz ausschlaggebend. So ist auch auffallend, dass die Sachaufwendungen in dem vierjährigen Betrachtungszeitraum um annähernd 20 Prozent angestiegen sind. Eine derartige Entwicklung kann selbstverständlich sachlich begründbar und insofern gerechtfertigt sein, sollte aber dennoch Anlass geben, dem Sachkostenbereich besondere Aufmerksamkeit zu widmen.

Damit besteht letztlich im Bereich aller IT-Aufwandsarten mit einem nennenswerten Volumen Handlungsbedarf, Wege zu einer verbesserten Wirtschaftlichkeit zu finden. Dazu sind eigene, tiefer gehende Analysen erforderlich, in denen die spezifischen Anforderungen und Strukturen innerhalb der Kreisverwaltung Borken im Einzelnen berücksichtigt werden.

Im Rahmen der Prüfung haben wir feststellen können, dass der Kreis Borken bereits aktiv Möglichkeiten sucht, die Kostensituation positiv zu beeinflussen. Um die Wirtschaftlichkeit der gegenwärtig laufenden Softwareverträge mit dem KRZN zu gegebener Zeit unter Marktbedingungen neu bewerten zu können, hat der Fachdienst 10 beispielsweise die Laufzeit der Verträge auf einen einheitlichen Zeitpunkt synchronisiert. Diese Vorgehensweise können wir unter dem Blickwinkel der Herstellung einer Vergleichbarkeit des Angebotsmarktes nur begrüßen.

Auch die Zielsetzung des Kreises Borken, explizit auch im IT-Bereich ein zur aktiven Kostensteuerung eingesetztes Controllingkonzept zu implementieren, sehen wir als richtige Reaktion auf die festgestellte Situation an. In diesem Zusammenhang ist die erfolgte Umorganisation des IT-Bereichs ebenfalls positiv als Maßnahme zu bewerten, von der eine verbesserte Gesamtsteuerung zu erwarten ist.

Im Bereich des IT-Grundschutzes sehen wir Optimierungspotenziale zunächst in einer ergänzenden Absicherung der Infrastrukturräume oder gegebenenfalls in deren Verlegung. Die IT-Infrastruktur (Server, aktive Netzkomponenten, Tape Library Plattform) ist über drei Räume des Verwaltungsgebäudes Burloer Straße 93 verteilt. Der neu gestaltete Hauptserverraum im dritten Obergeschoss des Verwaltungsgebäudes weist beste Standards sowohl in der Anordnung und Unterbringung der dort vorgehaltenen Technik als auch der sicherheitstechnischen Gestaltung der Räumlichkeit auf. Die räumliche Unterbringung der Anlagenteile sowohl im zweiten Obergeschoss als auch im Bunkerraum, in dem Teile der Datensicherungstechnik untergebracht sind, sehen wir dagegen als risikobehaftet an. Räumlichkeiten, in denen IT-technische Anlagen untergebracht sind, sollten grundsätzlich gegen Gefahren durch Feuer oder Einbruch sowie Umgebungseinflüsse geschützt sein. Insbesondere sollte auch eine ausreichende Klimatisierung sichergestellt sein.

Hinsichtlich des IT-Sicherheitsmanagements bleibt festzuhalten, dass der Kreis Borken eine IT-Sicherheitsbeauftragte bestellt hat, die mit der Begleitung sicherheitsrelevanter Prozesse beauftragt ist. Auch wenn wir im Rahmen der Prüfung feststellen konnten, dass Bestandteile von IT-Sicherheitszielen bereits in Dienstanweisungen formuliert sind, halten wir es für geboten, eine IT-Sicherheitsleitlinie als generelles Dokument zu erlassen. Eine IT-Sicherheitsleitlinie eröffnet der in der Verantwortung stehenden Verwaltungsführung eine weitere Möglichkeit, kurz und übersichtlich das Bewusstsein für IT-Sicherheitsprozesse in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit, Transparenz und Revision von Daten zu schärfen und zur Sensibilität im Umgang mit dem Datenmaterial anzuhalten.

Zudem empfehlen wir, über das Betriebshandbuch hinaus Sicherungsmaßnahmen für Notfälle in einem Notfallhandbuch nach BSI-Standard zu beschreiben.

Im Bereich des Lizenzmanagements liegt der von uns festgestellte Erfüllungsgrad zwar unterhalb des Mittelwertes; dies lässt dennoch nicht auf einen dringlichen Handlungsbedarf schließen, da mit dem Microsoft Enterprise Agreement-Vertrag eine Vielzahl an möglichen Risiken, die

terprise Agreement-Vertrag eine Vielzahl an möglichen Risiken, die sich aus den Lizenzverträgen mit Microsoft und deren Nutzung ergeben könnten, wirksam abgedeckt werden. Gleichwohl sollte der Gesamtprozess des Lizenzmanagements beim Kreis Borken als ganzheitlicher Prozess ausgestaltet werden, der letztlich dazu beitragen wird, Rechtssicherheit und wirtschaftlichen Softwareeinsatz für die Gesamtheit der verwendeten Softwareprodukte sicherzustellen.

Ergebnisse im Einzelnen

IT-Aufwendungen

Inhalt und Ziel

Um den leistungsorientierten Einsatz der Ressourcen aufzuzeigen, ermitteln wir alle periodisch anfallenden Personal- und Sachaufwendungen. Über die Darstellung der Aufwandströme zeigen wir u. a. den Ressourcenverbrauch auf und ermöglichen so, eventuelle Kostentreiber zu identifizieren. Diese Vorgehensweise ermöglicht in tiefere Analysen einzusteigen und kann so eine Basis für einen wirtschaftlichen Einsatz der Ressourcen bereiten.

Bei der überörtlichen Prüfung der Informationstechnologie werden auch individuelle strukturelle und organisatorische Besonderheiten der betrachteten Verwaltungen berücksichtigt. Ein elementarer Bestandteil der Prüfung ist es, die gewonnenen Erkenntnisse in einen interkommunalen Vergleich einzustellen. Das breite Spektrum der Organisationsvarianten und konzeptionellen Ausrichtungen macht es daher erforderlich, dass wir, um eine vergleichbare Situation zu schaffen, einen „gemeinsamen Nenner" (z.B. Bildschirmarbeitsplätze, Einwohner) in den Kreisverwaltungen betrachten und darstellen.

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, Auf-

wand und Kosten wird damit zugunsten einer pragmatischen Lösung teilweise aufgehoben.

Wir bereinigen zudem die Aufwendungen, Stellenanteile und Anzahl der Arbeitsplatzrechner, die auf die Bereiche der Leistungsgewährung und Verwaltung der Aufgaben nach dem SGB II sowie auf den pädagogischen Bereich in den Schulen entfallen.

Maßgeblich ist, dass in allen geprüften Kreisen nach einheitlicher Methode vorgegangen wird, um die geforderte Datenvalidität und Aussagefähigkeit für den interkommunalen Vergleich zu erreichen. Dies ist durch die dargestellte Vorgehensweise gewährleistet.

Sachaufwendungen

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

Soweit 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 eine weitgehende Analogie zur Ergebnisrechnung des NKF aufweisen.

Neben Aufwendungen in der Kernverwaltung werden in der Prüfung der Kreise auch Aufwendungen mit IT-Bezug in den kommunalen Sondervermögen wie Eigenbetrieben oder eigenbetriebsähnlichen Einrichtungen einbezogen („Konzernsicht"). Insofern sind letztlich nicht die jeweilige Organisationsform bzw. der Auslagerungsgrad entscheidend, sondern inwieweit die umfassende kommunale Aufgabenwahrnehmung in der Gesamtsicht IT-Aufwendungen verursacht.

Im Rahmen des interkommunalen Vergleichs erfolgt grundsätzlich eine Bruttobetrachtung der im jeweiligen Kreis für die Bereitstellung von IT entstandenen Aufwendungen. Innere Verrechnungen oder Erstattungen werden im Rahmen des Vergleichs nicht berücksichtigt.

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[3]. Individuelle Personalkostenfaktoren wie etwa Dienstaltersstufen und Zuschläge beziehen wir im Rahmen der IT-Prüfung nicht in den interkommunalen Vergleich mit ein.

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 der nachfolgenden Tabelle ist ersichtlich, welche Haushaltsergebnisse (hier: nur Sachaufwendungen) in die Kennzahlenbildung einfließen:

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

Aufwendungen für IT 2006 - 2009 in Euro Jahresabschluss der Ergebnisrechnung[4]				
	2006	**2007**	**2008**	**2009**
Kosten Rechenzentrum[5]	254.896	434.278	449.969	440.542
Abschreibungen	224.793	359.707	419.495	344.692
Miete/Leasing Arbeitsplatzausst. (Standard-PC, Monitor, Drucker)	270.088	284.655	300.759	288.852
Wartungsverträge und Updates	198.967	194.321	227.354	270.356
Dienstleistungen	127.322	106.826	157.092	215.506
Nutzung von Leitungsdiensten	182.512	182.254	174.492	87.813
Reparatur / Wartung	79.016	58.707	68.008	62.908
Verbrauchsmaterial	53.022	56.082	69.097	60.581
Pflege und Wartung ADV Fach-einheit 62	54.407	66.662	75.257	92.441
FE 62 - Erstattung an Kreis Steinfurt (Personalkostenanteil)	86.621	86.621	86.621	86.621
FE 62 - Erstattung an Kreis Steinfurt (Sachkostenanteil)	57.370	57.370	57.370	57.370
Sachaufwand Verwaltungsar-beitsplätze Kreisschulen	26.160	26.160	26.160	26.160
Wartung Telekommunikations-anlage (Hicom 300)	13.370	13.715	13.715	13.867
Anteil Inventarversicherung (für IT geschätzt)	2.021	2.025	2.186	2.188
Literatur und Zeitschriften	3.274	2.931	1.357	1.299
Summe	1.633.839	1.932.315	2.128.932	2.051.196

[4] Grundsätzlich werden die Sachaufwendungen aus dem jeweiligen Jahresabschluss der Ergebnisrechnung übertragen. Für die in der Tabelle enthaltenen Daten gilt dies nur eingeschränkt:

1. Für das Jahr 2009 lag zum Zeitpunkt der Datenerhebung noch kein testierter Jahresabschluss des Kreises Borken vor. Damit in die Ermittlung und Darstellung des Ressourcenverbrauchs valide Daten einfließen, wurden die Sachaufwendungen für das Jahr 2009 daher nicht wie für die Vorjahre aus dem Jahresabschluss übernommen, sondern über eine Auswertung der IT-spezifischen vorläufigen Buchungsdaten der Finanzbuchhaltung ermittelt.
2. Die IT-Sachaufwendungen aus dem Bereich des Katasterwesens und aus dem Bereich der Verwaltungsarbeitsarbeitsplätze in den kreiseigenen Schulen wurden aus Unterlagen ermittelt, die durch die jeweilige Facheinheit zur Verfügung gestellt worden sind.

[5] Bereinigt um Entgelte für Leistungen, die im Zusammenhang mit Aufgaben nach dem SGB II anfallen, vgl. auch Erläuterungen zu den Grundlagen der Datenerhebung, Seite 18.

Stellenausstattung und Personalaufwendungen für IT-Aufgaben

Wie im Abschnitt „Grundlagen der Datenerhebung" erläutert, fließen im Bereich der IT-Personalaufwendungen anstelle der tatsächlichen Haushaltsdaten Durchschnittswerte der KGSt 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 2009. 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	**14,75**	**937.895**
dezentrale Stellenanteile für originäre IT-Aufgaben Hier sind Stellenanteile erfasst, die außerhalb der zentralen IT Aufgaben aus den oben genannten Bereichen wahrnehmen.	**4,40**	**263.658**
Stellenanteile für originäre IT-Aufgaben (funktionale Ebene) gesamt	**19,15**	**1.201.553**
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.	**0,25**	**19.405**
Stellen in der zentralen IT (aufbauorganisatorische Ebene) gesamt	**15,00**	**957.300**

Für den Kreis Borken haben wir demnach innerhalb der zentralen IT-Abteilung 14,75 vollzeitverrechnete Stellenanteile ermittelt, die auf die Wahrnehmung originärer IT-Aufgaben entfallen.

Wir haben in der Mehrzahl der bisher geprüften Kreise und Gemeinden neben den Stellen in der zentralen IT weitere Stellenanteile für die dezentrale Erledigung von Aufgaben aus dem Bereich der Fachanwendungs- und Technikbetreuung identifiziert.

Durch den Kreis Borken wurden uns auf Basis einer eigener Untersuchung verwaltungsweit 4,40 dezentrale Stellenanteile für die Erledigung originärer IT-Aufgaben mitgeteilt. Die Bereitstellung und Betreuung von IT ist im Kreis Borken also in einer kombinierten Struktur zentraler und dezentraler Verantwortlichkeit organisiert.

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 Betreuung von PC-Arbeitsplätzen in einzelnen Organisationseinheiten oder die Wartung von Etagendruckern, entfallen.

Stellenausstattung des IT-Bereichs im interkommunalen Vergleich

Um die quantitative Stellenbemessung bewerten zu können, ermitteln wir die Betreuungsquote, also das Verhältnis der vollzeitverrechneten IT-Stellen[6] zu den betreuten Arbeitsplätzen mit IT-Ausstattung. Dieses Verhältnis bewegt sich bei den derzeit geprüften Städten in einem Spektrum von rund 1:32 bis 1:126.

Der Kreis Borken weist mit 51 betreuten Bildschirmarbeitsplätzen je IT-Stelle im Vergleich der bisher in dieser Prüfrunde von uns betrachteten Kreise eine deutlich unter dem mittleren Bereich liegende Betreuungsquote auf; das aktuelle arithmetische Mittel liegt bei etwa 1:79.

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

Beim interkommunalen Vergleich der Betreuungsquoten muss allerdings berücksichtigt werden, dass die Verwaltungen in sehr unterschiedlicher Ausprägung IT-Leistungen ausgelagert haben. In den bisher geprüften Kommunen und Kreisen 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.

Ein – wenngleich nur grober und rein monetärer – Indikator für den Auslagerungsgrad ist der relative Anteil der Entgelte, die für Rechenzentrumsleistungen anfallen, an den Gesamtaufwendungen der IT. Der Kreis Borken hat im Betrachtungsjahr 2009 als Drittkunde des KRZN in Kamp-Lintfort rund 440.000 Euro für die Bereitstellung von Fachanwendungen (*Wesen*) und den Betrieb der Datenleitung gezahlt; darin nicht enthalten sind die Entgelte für Leistungen, die im Zusammenhang mit SGB II-Leistungen anfallen (Fachanwendung „Prosoz"), da dieser Bereich in der Prüfung außer Betracht bleibt.

Der Betrag von 440.000 Euro bildet mit etwas weniger als 13 Prozent der IT-Gesamtaufwendungen einen der niedrigsten relativen Anteile unter den bisher geprüften Kreisen, die Rechenzentrumsleistungen in Anspruch nehmen. Im Durchschnitt entfällt rund ein Drittel[7] der IT-Aufwendungen auf solche Entgelte. Darin ist ein Anhaltspunkt dafür zu sehen, dass der Auslagerungsgrad im Kreis Borken eher niedrig ist und ein entsprechender Personalbedarf zur Aufgabenerledigung in eigener Verantwortung verbleibt. Insofern ist die festgestellte Betreuungsquote nach dieser Grobanalyse ein Wert, der nicht per se unangemessen hoch erscheint, aber unter organisatorischen und personalwirtschaftlichen Gesichtspunkten weiterhin aufmerksam beobachtet werden sollte.

[7] Diese Angabe bezieht sich nur auf Vergleichskreise mit einem nennenswerten Auslagerungsgrad an Gebietsrechenzentren, unabhängig vom Rechtsverhältnis (Zweckverbandsmitglied, Drittkunde usw.); Kreise, die ihre IT nahezu vollkommen autonom betreiben und deshalb keine oder nur marginale Aufwendungen für Rechenzentrumsentgelte aufweisen, sind hier nicht berücksichtigt. An dieser Stelle ebenfalls nicht mit einbezogen sind Kostenbeteiligungen oder -erstattungen zwischen Gebietskörperschaften, die im Rahmen öffentlich-rechtlicher Vereinbarungen im IT-Bereich interkommunal kooperieren.

Feststellung

Der Kreis Borken betreibt seine IT mit einem relativ geringen Grad an Auslagerung von Aufgaben an eine Datenzentrale. Die zentrale IT wird in der Anwendungsbetreuung in nennenswertem Umfang durch dezentrale Stellenanteile in den Fachbereichen unterstützt.

Die Betreuungsquote liegt deutlich unter dem Mittelwert; dies kann ein Indikator dafür sein, dass zumindest mittel- bis langfristig in der Stellenausstattung des IT-Bereichs Einsparpotenzial vorhanden sein könnte; ob ein solches Potenzial tatsächlich realisiert werden kann, muss jedoch anhand sachlicher, d.h. organisatorischer Kriterien durch den Kreis selbst beurteilt werden.

Interkommunaler Kennzahlenvergleich

Um eine Verzerrung und überproportionale Einflussnahme durch Schwankungen oder zufällig im Vergleichsjahr entstandene einmalige Zahlungsströme zu verhindern, berücksichtigen wir für die Kennzahlenbildung grundsätzlich das arithmetische Mittel aus dem vierjährigen Betrachtungszeitraum. Die Personalaufwendungen werden dagegen für das aktuellste Betrachtungsjahr ermittelt und um eine Sachkostenpauschale sowie Gemeinkostenzuschläge ergänzt.[8]

Die im vorherigen Kapitel für den Kreis Borken hergeleiteten Aufwendungen fließen demnach wie folgt in den Kennzahlenvergleich ein:

Grunddaten zur Kennzahlenbildung (Aufwendungen in Euro)	
IT-Sachaufwendungen (arithmetisches Mittel 4 Jahre)	1.936.571
Sachkostenpauschale nach KGSt-Empfehlung	103.410
Personalaufwendungen für originäre IT-Aufgaben (ermittelt nach KGSt-Pauschalen)	1.201.553
Gemeinkostenzuschlag nach KGSt-Empfehlung	240.311
Gesamtaufwendungen IT	**3.481.844**

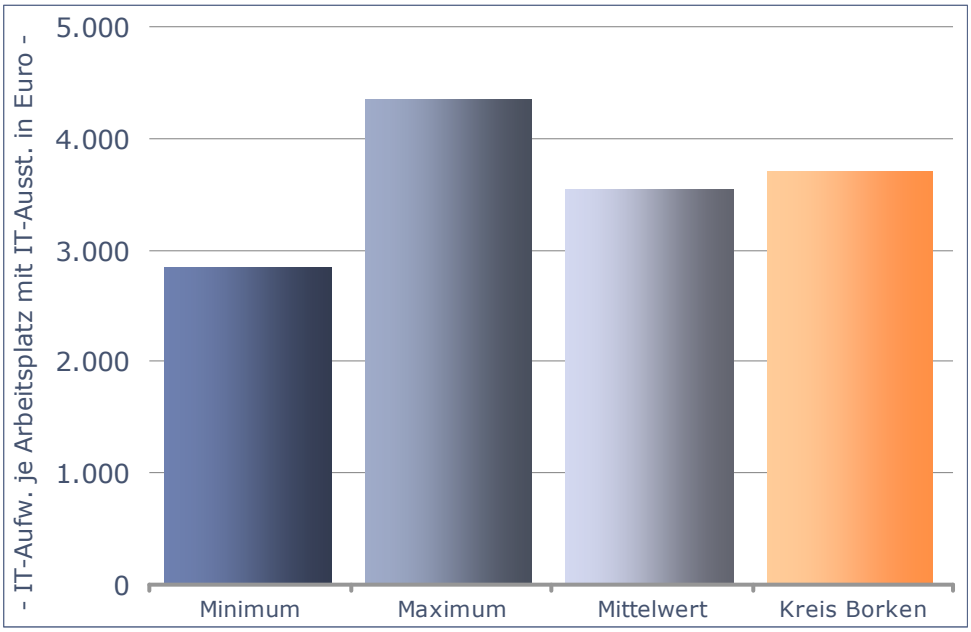
Als Bezugsgrößen legen wir neben den in den abgeschlossenen Prüfungen festgestellten Minimal- und Maximalwerten den einfachen Mittelwert als Orientierungsgröße zugrunde.

Zunächst stellen wir im Rahmen des interkommunalen Vergleichs der Kreise die IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung in den Mittelpunkt. Die daraus generierte Kennzahl liefert wichtige Informationen für Analysen im Rahmen interner Steuerungsprozesse.

Die Positionierung des Kreises Borken hinsichtlich seiner IT-Aufwendungen in der arbeitsplatzbezogenen Betrachtung zeigt die nachstehende Grafik.

[8] 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%.

IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung



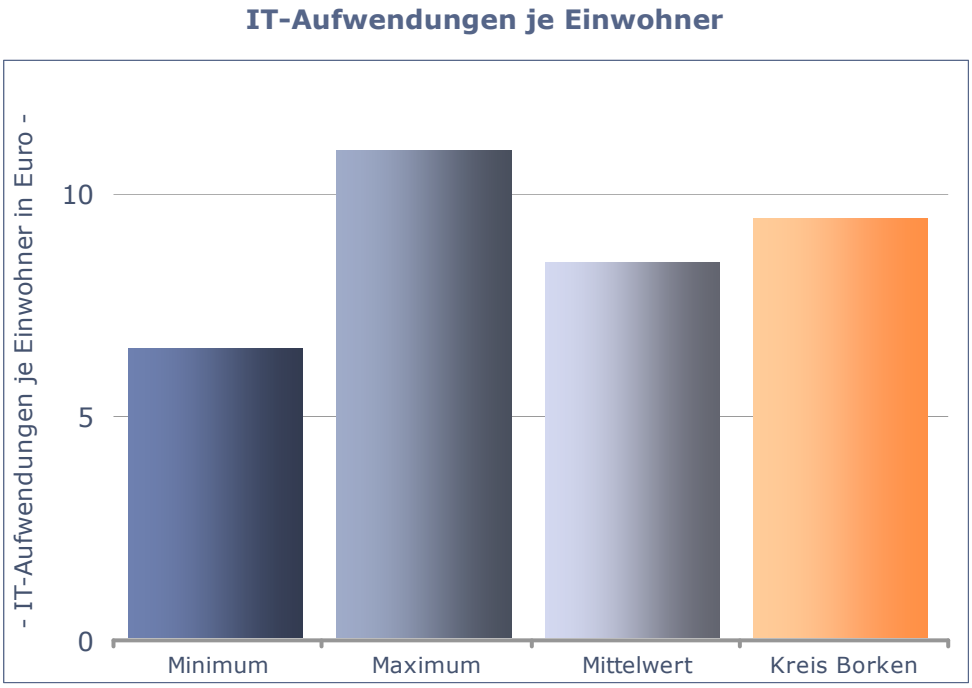
Bezugsgröße ist das arithmetische Mittel der Arbeitsplätze mit IT-Ausstattung im Betrachtungszeitraum in der Kernverwaltung und gegebenenfalls vorhandenen Sondervermögen.

IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung in Euro			
Minimum	Maximum	Mittelwert	**Kreis Borken**
2.825	4.334	3.524	**3.684**

Bei der auf Arbeitsplätze mit IT-Ausstattung bezogenen Kennzahl überschreitet der Kreis Borken den Mittelwert um 160 Euro, behält aber einen deutlichen Abstand zum Maximalwert bei. In absoluter Größenordnung ausgedrückt liegen die IT-Aufwendungen des Kreises Borken um rund 150.000 Euro jährlich über dem arithmetischen Mittel als statistischem Vergleichswert.

Ergänzend nehmen wir im Rahmen des interkommunalen Vergleichs eine Kennzahlenbildung mit Einwohnerbezug vor. Für eine Vielzahl der Aufgaben einer Kreisverwaltung sind die Einwohner des Kreisgebietes unmittelbare Adressaten, mindestens aber mittelbare Leistungsempfänger. 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.

Wie sich der Kreis Borken hinsichtlich seiner IT-Aufwendungen in der einwohnerbezogenen Betrachtung positioniert, zeigt die nachstehende Grafik.



Vergleichsbasis: 12 Kreise

IT-Aufwendungen je Einwohner in Euro			
Minimum	Maximum	Mittelwert	**Kreis Borken**
6,50	10,94	8,41	**9,41**

Bei der auf Einwohner bezogenen Kennzahl positioniert sich der Kreis Borken genau einen Euro über dem Mittelwert, bewahrt aber einen deutlichen Abstand zum Maximum.

Bei der Interpretation und Wertung der Kennzahlenausprägung muss beachtet werden, dass 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 hohe Anzahl positiv beeinflusst, weil die IT-Aufwendungen auf eine kleinere bzw. größere Verteilungsmenge fließen.

Im Vergleich wird deutlich, dass die Kennzahlen abhängig von der Bezugsgröße Einwohner bzw. Bildschirmarbeitsplatz im konkreten Fall des Kreises Borken ein leicht voneinander abweichendes Ergebnis liefern. Zwischen diesen Ergebnissen besteht keine Proportionalität, weil als rechnerischer Faktor die Anzahl der Bildschirmarbeitsplätze im Verhältnis zur Einwohnerzahl oder – anders ausgedrückt – die relative Größe der Verwaltung entscheidend ist. In der Relation, dies zeigt der Abstand der Werte des Kreises Borken zum jeweiligen Mittel- bzw. Maximalwert, fällt das Resultat beim Einwohnerbezug ungünstiger aus. Dies ist ein Indikator dafür, dass der Kreis mehr Bildschirmarbeitsplätze einsetzt als der Durchschnitt der Vergleichskreise.

Betrachten wir in diesem Zusammenhang die Quote der Bildschirmarbeitsplätze je tausend Einwohner (BSAP/1000 EW), so bestätigt sich dieses Bild. Der Kreis Borken erreicht hier eine etwas überdurchschnittliche Quote von 2,56 BSAP/1000 EW. Der Mittelwert der bisher geprüften Kreise liegt bei rund 2,4 BSAP/1000 EW.

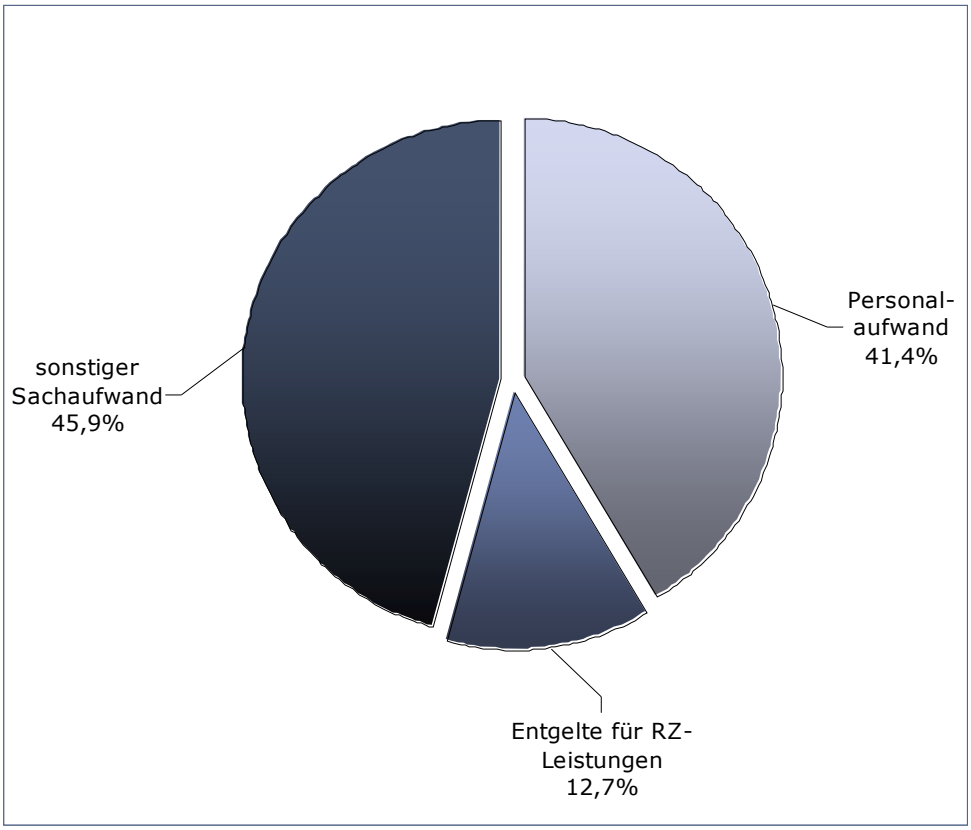
Wir verbinden mit der Nennung dieser Zahlenwerte keine Bewertung; sie dienen hier lediglich zur Erläuterung, aus welchen Gründen zwischen den von uns ermittelten Kennzahlen kein festes Größenverhältnis besteht. Bei einem angenommenen und auch allgemein feststellbaren Durchdringungsgrad von annähernd 100%[9] ist die Quote der Bildschirmarbeitsplätze je tausend Einwohner zwar ein wichtiger Indikator für die personalwirtschaftliche Gesamtsituation einer Verwaltung.

Gleichwohl tragen individuelle strukturelle Eigenschaften der geprüften Kreise dazu bei, dass sich teilweise nennenswerte Unterschiede in den Organisations- und Aufgabenstrukturen der Kreisverwaltungen ergeben. So können sich demografische und geografische Merkmale (etwa die Einwohnerzahl im Kreisgebiet insgesamt sowie in den kreisangehörigen Gemeinden; Flächenkreise mit vorrangig ländlicher Zersiedelung oder Kreise mit überwiegend städtischen Strukturen im kreisangehörigen Raum) mindestens mittelbar auf die personalwirtschaftliche Situation in der Verwaltung auswirken. Ob eine niedrige Quote an IT-Arbeitsplätzen je tausend Einwohner das Resultat eines effektiven und effizienten IT-Einsatzes als Mittel zur Aufgabenerfüllung ist, lässt sich wegen der Vielzahl von Einflussfaktoren mithin im Rahmen unserer Prüfung bis auf weiteres nicht ermitteln.

[9] 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.

Für die Kennzahl ‚IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung' stellen wir nachfolgend dar, wie sich die Gesamtaufwendungen zusammensetzen. Häufig lassen sich aus einer Grobanalyse Indikatoren herausarbeiten, in welchen Bereichen vorrangig Kostentreiber identifiziert werden können. Daher differenzieren wir je zunächst drei große Aufwandsblöcke, deren jeweiliger relativer Anteil an den Gesamtaufwendungen je Arbeitsplatz sich aus nachstehender Grafik ergibt.

Relative Anteile der IT-Aufwendungen je Arbeitsplatz



Relative Anteile der IT-Aufwendungen je Arbeitsplatz mit IT-Ausstattung			
Personal-aufwendungen	**Entgelte für RZ-Leistungen**	**sonstiger Sachaufwand**	**Summe**
41,4 Prozent	12,7 Prozent	45,9 Prozent	**100 Prozent**
1.525 Euro	466 Euro	1.692 Euro	**3.684 Euro**

Wie bereits ausgeführt ist der Anteil des Kreises Borken für Rechenzentrumsleistungen unter den Kreisen, die IT-Aufgaben an eine Datenzentrale ausgelagert haben, mit 12,7 Prozent recht niedrig.

Gleichwohl fällt bei einer differenzierten Betrachtung der Sachaufwendungen auf, dass die Zahlungen an das Rechenzentrum in den Jahren 2007 bis 2009 vor Abschreibungen, Miete bzw. Leasing und Wartungsverträgen/Updates die größte Position darstellen.[10]

Allgemeine betriebswirtschaftliche Erfahrungen belegen die Annahme, dass die Wahrscheinlichkeit hohe Einsparungspotenziale zu identifizieren bei den eingekauften Produkten mit den höchsten absoluten Preisen, d.h. im Bereich der so genannten A-Produkte, liegt. Zur ersten entsprechenden Orientierung haben wir die fünf Ausgabepositionen, für die die höchsten Entgelte anfallen, aufgelistet:

Die fünf größten Ausgabepositionen für Leistungen des KRZN	
Produktbezeichnung lt. Leistungsschein	**Entgelt Kreis Borken in Euro (2009)**
Prosoz[11]	157.908
Fahrerlaubnis	80.181
OK Vorfahrt	68.145
ADVIS	53.275
Einwohnerwesen	50.900

Um festzustellen, wie sich die gebildeten Aufwandsblöcke als Teilgröße der Kennzahl ‚Aufwendungen je Arbeitsplatz mit IT-Ausstattung' darstellen, sind wir wie folgt vorgegangen:

Die Personalaufwendungen und Sachaufwendungen[12] wurden separat und ohne Gemeinkostenzuschlag bzw. Sachkostenpauschale im interkommunalen Vergleich analysiert. Dabei zeigt sich, dass die Sachaufwendungen des Kreises Borken beim Arbeitsplatz- bzw. Einwohnerbezug deutlich bzw. nah unter dem Mittelwert liegen. Die genauen Werte sind den nachstehenden Tabellen zu entnehmen:

[10] Vgl. Tabelle auf Seite 21; lediglich im Jahr 2006 war mit den Miet- und Leasingentgelten eine andere Aufwandsart höher.

[11] In diese Auflistung haben wir die Anwendung Prosoz zur Verdeutlichung des Ausgabevolumens ausdrücklich einbezogen; bei der Ermittlung der Gesamtaufwendungen und in der Kennzahlenbildung wird der SGB II-Bereich allerdings nicht berücksichtigt, vgl. auch Erläuterungen auf Seite 18 sowie Fußnote 5 auf Seite 21.

[12] Hier: Sachaufwendungen gesamt einschließlich Entgelten für RZ-Leistungen.

IT-Sachaufwendungen (ohne Sachkostenpauschale) je Arbeitsplatz mit IT-Ausstattung in Euro			
Minimum	Maximum	Mittelwert	**Kreis Borken**
910	3.669	2.290	**2.049**

IT-Sachaufwendungen (ohne Sachkostenpauschale) je Einwohner in Euro			
Minimum	Maximum	Mittelwert	**Kreis Borken**
2,19	7,39	5,37	**5,24**

Dieses Resultat liefert zunächst keine belastbaren Anhaltspunkte dafür, dass nennenswerte Einsparpotenziale im Bereich der Sachaufwendungen vorliegen. Gleichwohl schließt eine Orientierung am Mittelwert im interkommunalen Vergleich nicht aus, dass in Teilbereichen eine höhere Wirtschaftlichkeit in der Aufgabenerfüllung erreichbar ist. Aus unserer Sicht sollte der Kreis Borken beispielsweise im Bereich der Sachaufwendungen weiterhin konsequent die Hardwarebeschaffung über Leasing in den Fokus einer Wirtschaftlichkeitsuntersuchung nehmen. Im Rahmen der Prüfung haben sich keine konkreten Anhaltspunkte für eine derzeit unwirtschaftliche Leasingvariante ergeben; aus grundsätzlichen Erwägungen halten wir es aber für geboten, den Kauf als ein denkbare Alternative in einen Vergleich einzubeziehen, wenn die aktuelle Leasinglaufzeit endet. Letztendlich sollte – selbstverständlich unter Beachtung der haushaltsrechtlichen Rahmenbedingungen – ausschließlich die Gesamtwirtschaftlichkeit den entscheidenden Maßstab im Alternativenvergleich darstellen.

Im Bereich der Personalaufwendungen wird der jeweilige Mittelwert sowohl beim Einwohner- als auch beim Arbeitsplatzbezug deutlich überschritten:

IT-Personalaufwendungen (ohne Gemeinkostenzuschlag) je Arbeitsplatz mit IT-Ausstattung in Euro			
Minimum	Maximum	Mittelwert	**Kreis Borken**
488	2.121	956	**1.271**

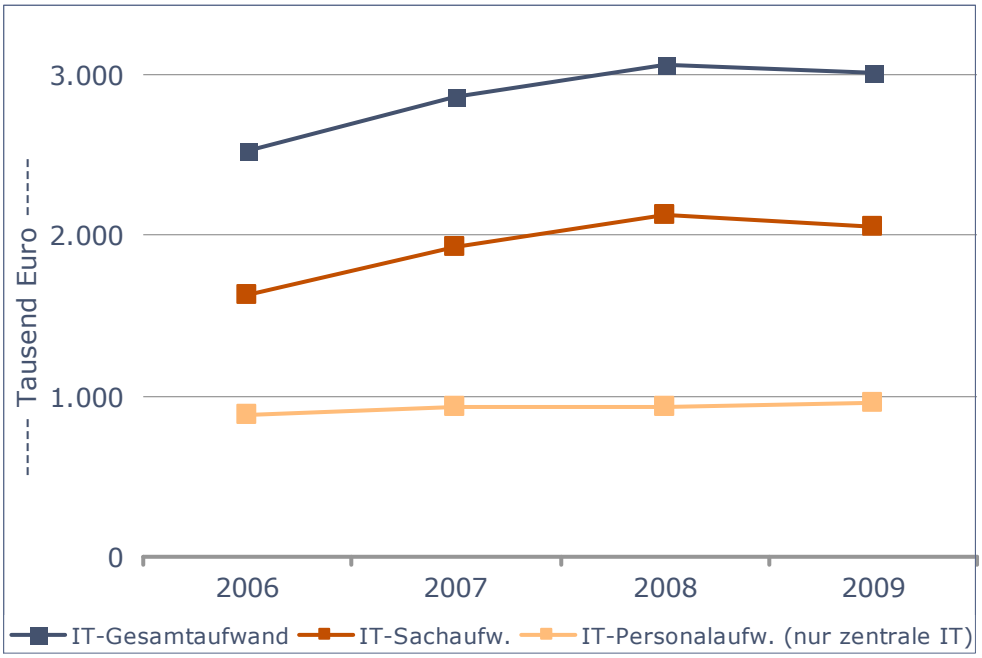
IT-Personalaufwendungen (ohne Gemeinkostenzuschlag) je Einwohner in Euro			
Minimum	Maximum	Mittelwert	**Kreis Borken**
0,77	5,75	2,35	**3,25**

In diesem Zusammenhang greifen wir noch einmal die bereits thematisierte Stellenausstattung des IT-Bereichs im interkommunalen Vergleich auf: Aus der Kombination der recht niedrigen Betreuungsquote und den über dem Mittelwert liegenden Personalaufwendungen lässt sich ableiten, dass dort die maßgebliche Ursache für die Positionierung des Kreises Borken hinsichtlich des Ressourceneinsatzes liegen könnte. Wie aber bereits ausgeführt können im Rahmen dieser Prüfung die spezifischen organisatorischen Kriterien nicht so betrachtet und bewertet werden, dass eine eindeutige Aussage zur Angemessenheit der Stellensituation im IT-Bereich ermöglicht wird.

Abschließend fokussieren wir die Betrachtung auf die Entwicklung der IT-Aufwendungen im Betrachtungszeitraum 2006 bis 2009 und differenzieren erneut nach Personal- und Sachaufwand. Aus nachstehender Grafik wird ersichtlich, dass bei relativ konstanten Personalkosten die Sachaufwendungen von 2006 bis 2009 um rund ein Viertel angestiegen sind. Die daraus resultierende Erhöhung der Gesamtaufwendungen beträgt rund 487.000 Euro, dies entspricht 19,3 Prozent.

Auch in dieser Analyse sind Pauschalen und Zuschläge nicht enthalten; die Personalaufwendungen beziehen sich nur auf die zentrale IT, da dezentrale Stellenanteile und darauf entfallende Kosten nur für das Jahr 2009 ermittelt wurden.

Entwicklung der IT-Aufwendungen von 2006 bis 2009



Zwar können solche Steigerungen durch unterschiedliche, sachliche begründbare Faktoren verursacht werden; der Anstieg fällt jedoch ins Auge und sollte Anlass für den Kreis Borken sein, die Entwicklung aufmerksam zu beobachten und einer aktiven Kostensteuerung zu unterwerfen.

Feststellung

Die IT-Aufwendungen des Kreises Borken überschreiten im interkommunalen Vergleich sowohl beim Einwohner- als auch beim Arbeitsplatzbezug den Mittelwert. Die Positionierung bei der arbeitsplatzbezogenen Kennzahl ist im direkten Vergleich besser; ein Einflussfaktor auf diese Tatsache ist die zahlenmäßig etwas überdurchschnittliche Ausstattung des Kreises Borken mit IT-Arbeitsplätzen auf tausend Einwohner.

Die differenzierte Betrachtung hat gezeigt, dass die eindeutige Identifizierung von „Kostentreibern", die als Ursache des relativ ungünstigen Ergebnisses in Frage kommen, nicht ohne weiteres möglich ist.

Empfehlung

Die Positionierung des Kreises Borken hinsichtlich des Ressourceneinsatzes löst in der Gesamtbetrachtung letztlich Handlungsbedarf aus, alle Aufwandsarten mit einem nennenswerten Volumen auf mögliche Einsparungspotenziale zu untersuchen.

Aus grundsätzlichen personalwirtschaftlichen Erwägungen sollte eine vergleichsweise niedrig ausfallende Betreuungsquote stets kritisch betrachtet werden, ohne jedoch den für eine hohe Qualität in der Aufgabenerfüllung erforderlichen Ressourcenbedarf unberücksichtigt zu lassen.

Zielsetzung sollte sein, mittel- bis langfristig objektive Grundlagen für die Beurteilung zu erhalten, ob und inwieweit die Stellensituation unter Berücksichtigung der spezifischen Anforderungen und Strukturen innerhalb der Kreisverwaltung Borken angemessen ist.

Gleiches gilt auch für die Sachaufwendungen, die zwar im interkommunalen Vergleich nicht auffällig hoch sind, deren erheblicher Anstieg in den letzten vier Jahren aber Anlass geben sollte, auch diesen Bereich im Hinblick auf eine wirtschaftliche Aufgabenerfüllung besondere Aufmerksamkeit zu widmen.

Finanzwirtschaftliche Steuerung im IT-Bereich

Inhalt und Ziel

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.

Eine wichtige Rolle spielt beispielsweise 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 Verwaltung nicht davon, diese Anteile zu ermitteln und den Möglichkeiten einer aktiven betriebswirtschaftlichen Steuerung zu unterwerfen.

Zur finanzwirtschaftlichen Steuerung im IT-Bereich lassen sich drei elementare Kernfragen formulieren:

- Verfügt der Kreis Borken 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 der Kreis Borken im Ergebnis aktiven Einfluss auf die Höhe seiner IT-Kosten nehmen?

Diese Fragestellungen gelten gleichermaßen für Kreise 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.

Analyseergebnisse

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

Damit echte finanzwirtschaftliche Steuerungsmöglichkeiten im IT-Bereich umgesetzt werden können, ist eine hohe Qualität der relevanten Informationen erforderlich. Mit Umstellung des kommunalen Haushaltes auf die Systematik des Neuen Kommunalen Finanzmanagements (NKF) zum 01.01.2006 wurde mit den Produkten 11.04.01 (IT-Betrieb) und 11.05.01 (IT-Strategie und Controlling) entsprechende Strukturen gebildet, die im Hinblick auf die angestrebten Steuerungsfunktionen aber noch nicht ausreichend ausgestaltet sind. Die im NKF-Haushalt vorgesehene Zieldefinition und Kennzahlenbildung ist erfolgt; in dem darauf basierenden Berichtswesen werden steuerungsrelevante Informationen quartalsweise aufbereitet und dargestellt.

Gerade für die Ziele mit Wirtschaftlichkeitsbezug können jedoch Erfüllungsgrade als entscheidender Maßstab für die Zielerreichung noch nicht so gemessen und dargestellt werden, dass sich daraus konkrete Maßnahmen zur Erhöhung der Wirtschaftlichkeit ableiten und steuern lassen. Soweit die Zieldefinitionen der Produkte 11.04.01 und 11.05.01 explizit auf wirtschaftliches Vorgehen ausgerichtet sind, sollten daher zur Messbarkeit bzw. Darstellung des Zielerreichungsgrades aussagefähigere Kennzahlen gebildet werden. Als Grundlage bieten sich z.B. die im vorliegenden Bericht verwendeten Kennzahlen für den interkommunalen Vergleich an. Damit lässt sich unter Einbeziehung individueller Anforderungen des Kreises das Ziel „wirtschaftlicher Einsatz von Hard- und Software" festlegen, messen und fortschreiben.

Unter aufbauorganisatorischen Aspekten war die Bündelung der IT-Aufgaben in einer verkleinerten Anzahl von Organisationseinheiten ein wichtiger Schritt auf dem Weg zu einer verbesserten Gesamtsteuerung.

Zur der Ausgestaltung des Controllingkonzeptes haben die Kämmerei des Kreis Borken und der Fachdienst 10 vereinbart, künftig Daten aus den IT-Buchungsstellen aus der Finanzsoftware automatisiert in die derzeit in Entwicklung befindliche Controllingstruktur zu übertragen. So

wird mit angemessenem Aufwand eine umfassende Informationsbasis für ein differenziertes und flexibles Kostencontrolling mit operativen Kennzahlen geschaffen.

Weiterhin ist geplant, künftig Projektkosten differenziert zu erfassen; im Sachkostenbereich wird so weit wie möglich eine Einzelkostenzuordnung angestrebt, Personalkostenanteile sollen über bewertete Zeitschätzungen in die Betrachtung einfließen.

Feststellung

In der Kreisverwaltung Borken wird gegenwärtig eine Controllingkonzeption für den IT-Bereich entwickelt. Ein großer Teil der für die aktive Steuerung der Wirtschaftlichkeit erforderlichen Strukturen sind bereits vorhanden oder konkret in Vorbereitung. Der Optimierungsbedarf, den wir im Bereich der finanzwirtschaftlichen Steuerung derzeit insbesondere noch in Bezug auf die oben formulierten Kernfragen sehen, war bereits erkannt; Lösungen werden gezielt angestrebt.

Wir bewerten die bereits angelaufenen bzw. geplanten Maßnahmen ausdrücklich positiv. Ein unter Abwägung von Aufwand und Nutzen und mit klarer Zielorientierung konzipiertes IT-Controlling wird aus unserer Sicht einen elementaren Beitrag zu einer erhöhten Wirtschaftlichkeit in der Aufgabenerfüllung leisten.

Empfehlung

Der Kreis Borken sollte die Maßnahmen zur Verbesserung der Steuerung mit der Zielsetzung einer erhöhten Wirtschaftlichkeit im IT-Bereich konsequent fortsetzen.

IT-Sicherheit

Inhalt und Ziel

Das Prüfmodul IT-Sicherheit beschäftigt sich insbesondere mit dem Bereich 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, der in der geprüften Körperschaft eingeführt und umgesetzt wurde, eine große Rolle.

Die Prüfungsaufgabe wird überwiegend unter Verwendung von Checklisten erledigt. Diese Checklisten wurden anhand anerkannter Kriterien des BSI[13] 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 Umsetzung der datenschutzrechtlichen Bestimmungen wird in einem gesonderten Kapitel thematisiert.

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 Maß-

[13] Bundesamt für Sicherheit in der Informationstechnik

nahmen. 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 folgende Sicherheitsanforderungen (=Basisziele) zu erfüllen:

- Verfügbarkeit

  Die Systeme müssen die geforderten Aufgaben zum verlangten Zeitpunkt in der angeforderten Weise erfüllen.

- Integrität

  Programme und Daten müssen vor Fälschung/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, und andererseits einen Überblick über die Standards zu erhalten, den die Kommunen diesbezüglich bereits erreicht haben. Es geht jedoch nicht darum, ein Szenario zu beschreiben, welche Maßnahmen möglich sind. Dies ist vielmehr eine Entscheidung der jeweiligen Organisation, mit welchen Mitteln das Mindestmaß an Sicherheitsanforderungen erreicht werden soll.

Die Betrachtung ist nach folgenden Teilbereichen untergliedert:

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

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

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

Unterlagen und Ansprechpartner

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

- Dienstanweisung IT vom 28.06.2006
- Sicherheitsrichtlinie für die mobile Nutzung von IT-Systemen
- Erklärung für die Nutzung des Internet (Benutzerrichtlinie) der Kreisverwaltung Borken als Ergänzung der Dienstanweisung für die technikunterstützte Informationsverarbeitung beim Kreis Borken
- Geschäftsanweisung für die Benutzung und Behandlung externer elektronischer Post (eMail) bei der Kreisverwaltung Borken vom 31.08.1999
- Dienstvereinbarung für die Einführung und Anwendung einer Telekommunikationsanlage
- IT-Betriebshandbuch der Kreisverwaltung Borken (Stand 03/2006)
- Virtualisierungsanalyse vom 11.08.2009
- Bericht Security Scan des internen Netzes vom 15.02.2010
- Technische und organisatorische Beschreibung (Planung 2010) der Serverräume
- Beschreibung der Gateway-Struktur
- Auflistung der Server (physisch/virtuell)
- Beschreibung der Datensicherungsumgebung für den Kreis Borken vom 19.03.2010
- Information Lifecycle Management vom 08.06.2009
- Netzplan 06/2010.

Als Ansprechpartner stand uns der Leiter des technischen Betriebes im Fachdienst 10 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
- Beobachten von Verfahrensabläufen (Stichproben)
- Durchsicht von Unterlagen
- Dokumentationsprüfung (Stichproben)
- Nachvollzug von Verfahrensabläufen (Stichproben)
- Analyse und gegebenenfalls Verwertung von Unterlagen Dritter
- Begehung der IT-Räume (soweit vorhanden).

Fragenkreis „IT-Räume und Infrastrukturaufbau“

Zu diesem Fragenkreis haben wir folgende Teilbereiche betrachtet:

Serverraum, IT-Verkabelung, WLAN[14], Sicherheitsgateway (Firewall).

Die IT-Infrastruktur (Server, aktive Netzkomponenten, Tape Library Plattform) ist über drei Räume des Verwaltungsgebäudes Burloer Straße 93 verteilt. Im Rahmen der Begehung haben wir in Bezug auf die Ausprägung der Sicherheitsanforderungen an die Raum umschließenden Elemente sehr unterschiedlich zu bewertende Situationen vorgefunden.

Zunächst einmal ist festzuhalten, dass der Hauptserverraum (Raum 2346) im dritten Obergeschoss des Verwaltungsgebäudes beste technische Standards sowohl in der Anordnung und Unterbringung der dort vorgehaltenen Technik als auch der sicherheitstechnischen Gestaltung der Räumlichkeit aufweist. Der Serverraum ist gut geplant und funktional angelegt und verfügt nicht nur über die erforderliche Brand- und Rauchschutztür sowie eine Gefahrenmeldeanlage, sondern insbesondere durch den Betrieb einer Gaslöschanlage über einen hervorragenden primären und sekundären Brandschutz. Aufgeteilte Stromkreise, redundant ausgelegte Klimatisierung und ein Fernanzeigesystem, das Wasseraustritte, Temperaturüberschreitungen sowie Störungen der USV-Anlagen meldet, tragen dazu bei, die Betriebssicherheit wesentlich zu erhöhen. Auch das betriebene Netzwerk komplettiert diesen positiven Gesamteindruck.

Soweit die IT-Räume und Infrastruktur betreffende Sicherheitsrisiken anzusprechen sind, liegen diese sicherlich nicht im Bereich des Hauptserverraumes (Raum 2346) oder des physischen Netzes. Mängel im räumlichen Umfeld waren sowohl beim Serverraum im zweiten Obergeschoss (Raum 2260) als auch im Bunkerraum, in dem Teile der Datensicherungstechnik untergebracht sind, festzustellen. So verfügt der Bunkerraum über keine Klimatisierung. Schon bei der Begehung der Räumlichkeiten wurde die Raumtemperatur im Bunkerraum ohne konkrete Messung als außergewöhnlich hoch empfunden.

Räumlichkeiten, in denen IT-technische Anlagen untergebracht sind, sollten grundsätzlich gegen Gefahrenpotenziale durch Feuer oder Einbruch sowie Umgebungseinflüsse geschützt sein.

[14] Wireless Local Area Network

Empfehlung

Wir empfehlen, die räumliche Unterbringung der Server im Raum 2260 sowie des Datensicherungssystems im Bunkerraum des Verwaltungsgebäudes zu überdenken und ggf. auf besser geeignete Standorte zurückzugreifen.

Als besonders positiv schätzen wir ein, dass der Kreis Borken die interne Netzstruktur im Rahmen eines Security Scan hat prüfen lassen. Sicherheitsmängel wurden in einem Maßnahmenkatalog zusammengefasst und mit entsprechenden Prioritäten belegt. Die Abstellung der Mängel erfolgt sukzessive.

Weitere, im Rahmen der Prüfung identifizierte Sachverhalte führen zu folgenden Empfehlungen.

Serverraum (Raum 2260 und Bunkerraum)

Brandlasten

Bei der Begehung der Serverraumes im zweiten Obergeschoss sowie des Bunkerraumes sind Brandlasten aufgefallen. Insbesondere handelt es sich um Verpackungsmaterialien, Möbelteile, Papierlagerung, eine hölzerne Deckenkonstruktion und einen leicht entflammbaren Teppich im Raum 2260.

Empfehlung

Um den sicheren Betrieb unter Gesichtspunkten des Brandschutzes zu gewährleisten, sollten in den Räumlichkeiten der technischen Infrastruktur Brandlasten möglichst vermieden werden.

Verwendung von Sicherheitstüren und - fenstern

Die Konzeption eines Serverraums sieht einen abgeschlossenen Sicherheitsbereich vor. Er sollte möglichst gut zu sichernde Zugangstü-

ren haben, die vor Gefährdungen durch Umgebungseinflüsse, insbesondere aber gegen Feuer und Einbruch schützen.

Der zweite Serverraum (Raum 2260) des Kreises Borken befindet sich im zweiten Obergeschoss des Verwaltungsgebäudes Burloer Straße 93. Er verfügt über drei Zugänge - über das angrenzende Büro (Raum 2258) sowie über den für die Öffentlichkeit zugänglichen Flur (Zugang 2260 und 2262) und ist nur durch Holztüren gesichert, die üblicherweise in nicht schützenswerten Gebäudebereichen verbaut werden. Die Türen sind zwar alarmgesichert, verfügen aber über keinerlei Feuer- oder mechanischen Einbruchsschutz. Sie bieten daher keine ausreichende Sicherung gegen gewaltsames Eindringen oder den Übergriff von Feuer aus angrenzenden Bereichen. So könnte beispielsweise ein Brandherd, der im Nebenbüro oder Flur entstanden ist, ungehindert auf den Serverraum übergreifen. Eine Feuergefahr vom Flur aus ist nicht unwahrscheinlich, da dieser mit einem Teppichboden ausgelegt ist. Auch die Alarmsicherung der Serverraumtüren stellt nur eine sekundäre Präventionsmaßnahme dar. Allein eine bautechnische Härtung der Serverraumzugänge trägt dazu bei, Schäden durch Diebstahl und Vandalismus so weit wie möglich vorzubeugen.

Die über ein Flachdach gut zugänglichen Serverraumfenster (Raum 2260) sind nicht gegen Glasbruch geschützt, vom Rahmen her nicht gehärtet und auch nicht in das Alarmsystem eingebunden. Aus feuer- bzw. sicherheitstechnischer Betrachtung heraus stellen sie ein beträchtliches Risiko dar. Die Fensterrahmen sind aus Holz gefertigt und mit keinerlei Sicherheitsbeschlägen versehen, die die Zugangszeit im Falle eines Einbruchs verzögern könnten.

Sicherheitstüren und –fenster bieten gegenüber normalen Bürotüren und Fenstern Vorteile:

- In der Norm DIN EN 1627 „Fenster, Türen, Abschlüsse- Einbruchhemmung – Anforderungen, Klassifizierung" sind die Bauelemente in Widerstandsklassen (WK) eingeordnet worden. Türen gemäß der Klassifizierung WK1 bis WK4 bieten aufgrund ihrer Stabilität einen höheren Schutz gegen Einbruch.

- Als selbstschließende, feuerhemmende und gegebenenfalls rauchdichte Tür (z. B. FH-Tür T30, nach DIN 18082 „Feuerschutzanschlüsse") verzögern sie die Ausbreitung eines Brandes.

- Sie schützen in der Ausführung als selbstschließende Rauchschutztür (DIN 18095-1 „Türen, Rauchschutztüren; Begriffe und

Anforderungen") vor der Ausbreitung von Brandrauch. Brandrauch ist so feinkörnig, dass er problemlos durch Druckausgleichs- und Lüftungsöffnungen von Festplatten dringt. Für die geringen Flughöhen von Festplattenleseköpfen ist er aber immer noch viel zu groß und verursacht dort enorme Schäden.

Empfehlung

Der zweite Serverraum des Kreises Borken (Raum 2260) sollte gegen Feuer, Einbruch und Vandalismus besser geschützt werden. Wir empfehlen, in Zusammenarbeit mit dem vorbeugenden Brandschutz der Feuerwehr, der kriminalpolizeilichen Beratung und dem technischen Baubereich Lösungen zu erarbeiten, die Türen, Fenster, angrenzende Büroraume und Umgebungswände einbeziehen, soweit nicht über eine Verlagerung der technischen Anlagen nachgedacht wird. Insbesondere sollte der Raum nicht als Lagerraum genutzt werden.

Im Rahmen dieser Untersuchung sollte auch die Tür des Hauptserverraumes hinsichtlich des Einbruchsschutzes begutachtet werden.

Abgeschlossene Türen

Die Tür des Serverraums im zweiten Obergeschoss (Raum 2260) ist nicht abgeschlossen. Nicht nur die Türen unbesetzter Räume, sondern in besonderem Maße die Türen von Serverräumen oder Räumen anderweitiger IT-technischer Infrastruktur sollten stets verschlossen sein. Dadurch wird verhindert, dass Unbefugte Zugriff auf darin befindliche Unterlagen und IT-Einrichtungen erhalten.

Empfehlung

Insbesondere in Anbetracht dessen, dass die Räumlichkeiten der IT öffentlich zugänglich sind, empfehlen wir, die Tür zum Serverraum (Raum 2260) stets abgeschlossen zu halten und darüber hinaus den Zugang nur auf den zugelassenen Personenkreis zu beschränken.

Wasser führende Leitungen

In Räumen oder Bereichen, in denen sich IT-Geräte mit zentraler Funktion (z. B. Server oder Netzwerkkomponenten) befinden, sollten Wasser führende Leitungen aller Art vermieden werden. Die einzigen Wasser führenden Leitungen sollten, wenn unbedingt erforderlich, Kühlwasser-, Löschwasserleitungen und Heizungsrohre sein. Sind Wasser führende Leitungen unvermeidbar, müssen Vorkehrungen getroffen werden, um einen Wasseraustritt möglichst frühzeitig zu erkennen und die negativen Auswirkungen zu minimieren.

Im Serverraum (Raum 2260) sind Heizkörper installiert.

Empfehlung

Der Kreis Borken sollte prüfen, inwieweit es bautechnisch möglich ist, die Heizkörper vom Wasser führenden Kreislauf abzutrennen, damit das beschriebene Gefahrenpotenzial vermieden wird. Sollte dies nicht möglich sein, erscheint zumindest die Einbindung des Risikos eines Wasseraustritts in ein Fernanzeigesystem geboten.

Not-Aus-Schalter

Für den Serverraum ist kein Not-Aus-Schalter vorhanden. Bei Räumen, in denen elektrische Geräte in der Weise betrieben werden, dass z. B. durch deren Abwärme, hohe Gerätedichte oder Vorhandensein zusätzlicher Brandlasten ein erhöhtes Brandrisiko besteht, ist die Installation eines Not-Aus-Schalters sinnvoll. Dies sind z. B. gerade Server- oder Technikräume. Da zur Betätigung des Not-Aus-Schalters allerdings Personal erforderlich ist, kommt er jedoch nur in solchen Bereichen in Frage, in denen ständig oder meistens Personen anwesend sind. In nicht oder nur sporadisch besetzten Bereichen ist eine Notabschaltung durch eine Brandfrühesterkennung wesentlich effektiver. Dies sollte bei der Betrachtung, ob die Installation einer Notabschaltung sinnvoll ist, beachtet werden.

Mit Betätigung des Not-Aus-Schalters wird dem Brand eine wesentliche Energiequelle genommen, was bei kleinen Bränden zu deren Verlöschen führen kann. Zumindest ist aber die Gefahr durch elektrische Spannungen beim Löschen des Feuers beseitigt.

Zu beachten ist auch, dass lokale unterbrechungsfreie Stromversorgungen (USV-Anlagen) nach Ausschalten der externen Stromversorgung die Stromversorgung selbsttätig übernehmen und die angeschlossenen Geräte unter Spannung bleiben. Daher ist bei der Installation eines Not-Aus-Schalters zu beachten, dass auch die USV abgeschaltet und nicht nur von der externen Stromversorgung getrennt wird.

Der Not-Aus-Schalter kann innerhalb des Raumes neben der Eingangstür (mit Hinweis außen an der Tür) oder außerhalb des Raumes neben der Tür angebracht werden; dies sollte im Einzellfall mit einem Sachverständigen besprochen werden. Für die Lage ist allerdings zu bedenken, dass dieser Not-Aus-Schalter auch ohne Gefahr versehentlich oder absichtlich (Sabotage) betätigt werden kann. Daher ist der Not-Aus-Schalter mit einer Abdeckung gegen versehentliche Betätigung zu schützen.

Empfehlung

Soweit der Kreis Borken keine Verlagerung der technischen Anlage in Betracht zieht, sollte die Installation eines Not-Aus-Schalters für den zweiten Serverraum (Raum 2260) sowie den Bunkerraum geprüft und ggf. umgesetzt werden.

Zutrittsregelung und Zugangskontrolle

Der Kreis Borken hat Vorkehrungen getroffen, den Zutritt zum Hauptserverraum nur auf einen befugten Personenkreis zu begrenzen. Insbesondere sind die codierten Schlüssel nur im Bedarfsfall über den Leiter des IT-Betriebes erhältlich. Der Zutritt wird aber nicht dokumentiert.

Empfehlung

Soweit die technische Realisierung mit einem vertretbaren Aufwand verbunden ist, empfehlen wir, den Zutritt zu den Serverräumen über ein elektronisches Zugangssystem zu sichern, das gleichzeitig den Schließmechanismus der Tür als auch die Zutrittsdokumentation abdeckt.

Soweit Dritte in Begleitung eines IT- Bediensteten die Räumlichkeiten betreten, sollte dies manuell protokolliert werden.

Sicherheitsgateway (Firewall)

Grundstruktur des Sicherheitsgateways

Beim Kreis Borken wird derzeit ein Sicherheitsgateway betrieben, dessen Kernkompetenz aus einer redundant ausgelegten Checkpoint Firewall besteht. Die Empfehlung des BSI geht derzeit dahin, eine mehrstufige Firewall-Struktur zu etablieren, da getrennte, sich ergänzende Systeme den Vorteil haben, aufgrund unterschiedlicher Stärken ein höheres Sicherheitsniveau zu bieten. Einzelne Systeme haben den Nachteil, dass potenzielle Angreifer nur die Sicherheitsmechanismen eines einzigen Systems überwinden müssen, um das Sicherheitsgateway zu kompromitieren.

Empfehlung

Wir empfehlen, die Grundstrukturen des Sicherheitsgateways zu überdenken, um den gestiegenen Sicherheitsanforderungen in der externen Kommunikation gerecht zu werden.

Fragenkreis „Technische Ausstattung der Arbeitsplätze/ Client-Umgebung"

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

Im Rahmen der Prüfung sind über die Formulierungen in der Checkliste hinaus keine Sachverhalte identifiziert worden, die zu einer Empfehlung 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. 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.

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.

Im Rahmen der Prüfung konnten wir feststellen, dass der Kreis Borken Bestandteile von IT-Sicherheitszielen durchaus schon in der Dienstanweisung IT, der Sicherheitsrichtlinie für die mobile Nutzung von IT-Systemen, der Benutzerrichtlinie Internet und der Geschäftsanweisung für die Benutzung und Behandlung externer elektronischer Post (eMail) aufgenommen und schriftlich festgehalten hat. So wurden Grundsätze für den Einsatz von Informationstechniken, Verantwortlichkeiten, Betrieb und Nutzung der IT-Systeme, Nutzungsverbote, Nutzung von Internet und E-Mail-Diensten verbindlich geregelt. Ein generelles Dokument mit Leitliniencharakter, das die Positionierung der in der Verantwortung stehenden obersten Leitungsebene zum Stellenwert der IT-Sicherheit zum Ausdruck bringt, existiert derzeit noch nicht. Über diese Ausführungen in der Dienstanweisung sowie den vorgenannten Richtlinien hinaus sehen wir in dem Erlass einer IT-Sicherheitsleitlinie eine weitere Möglichkeit der Verwaltungsführung, kurz und übersichtlich das Bewusstsein für IT-Sicherheitsprozesse in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit, Transparenz und Revision von Daten zu schärfen und zur Sensibilität im Umgang mit dem Datenmaterial anzuhalten.

Einer der Grundpfeiler zur Erreichung eines angemessenen Sicherheitsniveaus ist, dass die Leitungsebene hinter den Sicherheitszielen steht und ihre Verantwortung für Informationssicherheit deutlich macht. Letztendlich geht es darum, über die Leitlinie verantwortungsbewussten Umgang mit Daten vorzuleben und auf diesem Wege in einer besonderen Form die IT-Sicherheitsziele in die Mitarbeiterschaft zu tragen. Die

Dienstanweisung IT sowie die weiteren Richtlinien stellen in diesem Zusammenhang ein wertvolles und unerlässliches Werkzeug, eingebettet in weitere, nachfolgend beschriebene IT-Sicherheitsmaßnahmen dar.

Besonders positiv schätzen wir es ein, dass schon heute die Nutzung der Informationstechnik betreffende Dienstanweisungen, Richtlinien und Nutzungshinweise für die Mitarbeiterschaft stets verfügbar ins Intranet eingestellt 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.

Nach Dienstanweisung IT vom 28.06.2006 – Ziffer 1.4 - liegt die Verantwortung für die Planung der IT-Sicherheitskonzepte bei der IT-Sicherheitsbeauftragten (Stabstelle IT Strategie und Controlling). Zwischenzeitlich wurden die Aufgabenbereiche Organisation, IT-Betrieb und IT-Strategie und Controlling zum 01.04.2010 neu organisiert. Vorgenannte Aufgaben sind dem Fachdienst 10 - Organisation und IT - zugewiesen worden. Der Bereich IT-Sicherheit verblieb bei der Behördlichen Datenschutzbeauftragten. Eine Stellvertretungsregelung für die IT-Sicherheitsbeauftragte besteht nicht.

Feststellung

Wir halten positiv fest, dass der Kreis Borken eine IT-Sicherheitsbeauftragte benannt hat und auf diesem Wege die Begleitung des IT-Sicherheitsprozesses wahrnehmen lässt. Die

Stellvertreterfunktion ist nicht besetzt. Darüber hinaus sind die Aufgaben der IT-Sicherheit und des behördlichen Datenschutzes auf einer Stelle zusammengefasst.

Empfehlung

Wir empfehlen dem Kreis Borken über die Einrichtung einer Stellvertreterfunktion nachzudenken, die ggf. die Umsetzung des IT-Sicherheitsprozesses in geeigneter Weise begleiten könnte. Denkbar wäre auch, den IT-Sicherheitsprozess im Rahmen einer Arbeitsgruppe zu unterstützen.

Erstellung eines IT-Sicherheitskonzeptes

Ein IT-Sicherheitskonzept ist erforderlich, damit die in der IT-Sicherheitsleitlinie vorgegebenen IT-Sicherheitsziele und Sicherheitsstrategien verfolgt und dazu passende Maßnahmen geplant, umgesetzt und aktualisiert werden können.

Empfehlung

Wir empfehlen, ein IT-Sicherheitskonzept nach den Standardvorgaben des BSI zu entwickeln.

In einem IT-Sicherheitskonzept nach BSI-Standard werden dazu folgende Teilschritte unterschieden:

- Auswahl einer Methode zur Risikobewertung
- Klassifikation von Risiken beziehungsweise Schäden
- Risikobewertung
- Entwicklung einer Strategie zur Behandlung von Risiken

- Auswahl von Sicherheitsmaßnahmen.

Ein IT-Sicherheitskonzept enthält demnach u. a. eine

- *Schutzbedarfsanalyse* zur Identifizierung und Bewertung der kritischen IT-Anwendungen, IT-Systeme und Räume,
- *IT-Grundschutzanalyse* mit einer Ermittlung der notwendigen Sicherheitsmaßnahmen sowie Ermittlung des aktuellen Umsetzungsgrades von Sicherheitsmaßnahmen (Basis-Sicherheitscheck),
- *Realisierungsplanung* zur Umsetzung der konsolidierten und priorisierten Sicherheitsmaßnahmen.

Management-Berichte zur IT-Sicherheit

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

> **Empfehlung**
>
> Es sollten regelmäßige Berichte zur IT-Sicherheit von der IT-Sicherheitsbeauftragten erstellt werden, um der Verwaltungsleitung alle Informationen für eine Risikobewertung transparent zu machen und eine Basis für notwendige Entscheidungen zu liefern.

Nach dem Sachvortrag des Kreises Borken ist ein Managementbericht im Rahmen des Security Scan des Netzwerkes im Februar 2010 erstellt worden. Die Einrichtung eines regelmäßigen Berichtswesens halten wir für unerlässlich, da über diesen Weg ein fortlaufender Informationsaustausch die Sensibilität für Sicherheitsprozesse gewährleistet.

Ein Management-Bericht zur IT-Sicherheit sollte aufzeigen,

- inwieweit die Vorgaben des IT-Sicherheitskonzeptes 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.

Notfallvorsorge

Notfallhandbuch und Verantwortlichkeit

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.

Der Kreis Borken verfügt über ein Betriebshandbuch, dass bereits heute schon wichtige Informationen liefert, die in einer Notfallsituation eine wertvolle Arbeitshilfe darstellen können. So werden IT Prozesse, IT Komponenten und Anwendungen, das Clientmanagement sowie Vertragsübersichten nachvollziehbar abgebildet und dokumentiert. Auch wenn es sich bei den vorgelegten Unterlagen überwiegend um Beschreibungen handelt, die den laufenden Betrieb regeln, tragen sie sicherlich dazu bei, einer Notfallsituation unter Beteiligung der zur Verfügung stehenden Mitarbeiterinnen und Mitarbeiter des Fachdienstes 10 Organisation und IT in einem gewissen Umfang zu begegnen. In einer Notfallsituation müssen aber auch Dritte in die Lage versetzt werden können, eine funktionsfähige IT unter dem Blickwinkel der Wiederbeschaffungsmöglichkeiten, der internen und externen Ausweichmöglichkeiten, eines eingeschränkten IT-Betriebes und der Datensicherung wieder herzustellen.

Empfehlung

Wir empfehlen, über das Betriebshandbuch hinaus Sicherungsmaßnahmen für Notfälle in einem Notfallhandbuch nach BSI-Standard festzuhalten.

Unsere Empfehlung zielt darauf ab, die bereits heute vorliegende Dokumentation und weitere Notfallmaßnahmen zu ordnen, im Sinne der BSI-Vorgaben zu vervollständigen und griffbereit vorzuhalten. Hierzu will der Kreis Borken das elektronische Notfallhandbuch der Firma SECOM einsetzen. Diesen Schritt begrüßen wir.

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.

Empfehlung

Darüber hinaus empfehlen wir auch, für die autorisierte und rechtzeitige Einleitung von Notfallmaßnahmen einen Notfallverantwortlichen förmlich zu benennen.

Der Notfall-Verantwortliche sollte sowohl die Entscheidung treffen dürfen, ob ein Notfall eingetreten ist, als auch autorisiert sein, die notwendigen Notfallmaßnahmen einzuleiten. Sollte das SECOM Notfallhandbuch zum Einsatz kommen, werden vorgenannte Festlegungen dort getroffen.

Eingeschränkter IT-Betrieb und Übersicht über Verfügbarkeitsanforderungen

> **Empfehlung**
>
> Der Kreis Borken sollte festlegen, welche IT-Anwendungen mit welcher Priorität im Notfall eingeschränkt betrieben werden müssen.

Für den Fall, dass Teile des IT-Systems ausfallen, ist zu untersuchen, ob ein eingeschränkter IT-Betrieb notwendig und möglich ist. Ziel sollte hier sein, bei einem - durch einen Notfall bedingten - eingeschränkten IT-Betrieb möglichst viele IT-Anwendungen betreiben zu können.

Dabei muss für den eingeschränkten IT-Betrieb festgelegt werden, welche IT-Anwendungen mit welcher Priorität betrieben werden bzw. verfügbar sein müssen. Dies ist mit der Verwaltungsleitung und ggf. auch mit den Fachbereichen abzustimmen und sollte schriftlich fixiert werden.

Wir halten es für unerlässlich, Verfügbarkeitsanforderungen festzulegen und mit den Fachdiensten zu vereinbaren. Es geht darum, die tolerierbaren Ausfallzeiten für Serversysteme oder Anwendungen zu bestimmen, da dies nicht nur eine elementare Planungsgrundlage für den weiteren Ausbau der IT-Infrastruktur darstellt, sondern auch die Festlegung der Notfallvorsorgemaßnahmen entscheidend beeinflusst.

Notfallpläne für ausgewählte Schadensereignisse

> **Empfehlung**
>
> Es sollten Notfallpläne erstellt werden, die speziell auf die Belange der IT beim Kreis Borken ausgerichtet sind.

Notfallpläne beinhalten dabei Handlungsanweisungen und Verhaltensregeln für bestimmte Schadensereignisse. Hierbei handelt es sich um Er-

eignisse, die diejenigen Teile des IT-Systems gefährden, die von existentieller Bedeutung sind. Ein Notfall-Plan ist auf die möglichst schnelle Wiederherstellung der Verfügbarkeit auszurichten.

Ein Notfallplan muss auch das Zusammenwirken eines schädigenden Ereignisses und der getroffenen Notfall-Maßnahme berücksichtigen. Beispielsweise kann durch den Einsatz einer Sprinkleranlage ein Brand bekämpft werden. Jedoch können durch den Wassereinsatz wiederum auch neue Gefährdungen entstehen, z. B. für die Stromversorgung oder für Datenträgerarchive.

Notfallpläne sind je nach Umfeldgegebenheiten für folgende Ereignisse aufzustellen[15]:

- Brand,
- Wassereinbruch,
- Stromausfall,
- Ausfall der Klimaanlage,
- Explosion,
- Ausfall der Datenfernübertragungseinrichtung sowie
- Sabotage.

Wiederanlaufpläne und Notfallübungen

Im Zusammenhang mit den Verfügbarkeitsanforderungen und der Definition des eingeschränkten IT-Betriebs sollten auch Wiederanlaufpläne erstellt werden. Die hierfür erforderlichen Schritte sind ebenfalls in das Notfallhandbuch mit aufzunehmen. Hierbei kann es sich um folgende Aktivitäten handeln:

- Aufbau und Installation der notwendigen Hardware Komponenten
- Einspielen und Konfigurieren der Systemsoftware

[15] gem. Maßnahmenkatalog des BSI

- Einspielen der Anwendungssoftware
- Bereitstellen der notwendigen Daten einschließlich Konfigurationsdateien
- Wiederanlauf
- Revisionssichere Protokollierung.

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

Empfehlung

Beim Kreis Borken sollten Wiederanlaufpläne erstellt und in ein Notfallhandbuch mit aufgenommen werden. Diese Maßnahmen sollten regelmäßig anhand von Notfallübungen überprüft werden.

Fragenkreis „Backup und Archivierung"

Basisierend auf einer IBM Tivoli-Storage-Manager (ITSM) Lösung und dem Tool Backup Eagle von der Fa. Schmitz RZ Consult hat der Kreis Borken eine integrierte, unternehmensweite Datensicherungslösung geschaffen.

Die Originaldaten auf den kreisweiten Servern werden entsprechend ihrer Klassifizierung in verschiedenen Zeitabständen zunächst auf das ITSM-Primärsystem im Hauptserverraum 2346 und zusätzlich täglich auf das ITSM-Backupsystem im Schutzkeller auf LTO4-Bänder geschrieben.

ITSM-Primär- und ITSM-Backup-System befinden sich zwar in unterschiedlichen Brandabschnitten des Verwaltungsgebäudes, der Schutzkeller ist im besichtigten Zustand für die Vorhaltung von IT-Technik jedoch nur bedingt geeignet. Eine feuerfeste Aufbewahrung der Bandsicherungen in einem feuerschutzzertifizierten Datensicherungsschrank erfolgt nicht.

Der Kreis Borken hat bewusst aus Kostengründen und unter Berücksichtigung der Wahrscheinlichkeit einer gleichzeitigen Zerstörung beider ITSM-Systeme und des größten anzunehmenden Unfalls auf eine Auslagerung des gesamten ITSM-Backup-Systems an einen entfernten Standort verzichtet. Dennoch scheint unterschwellig eine gewisse Verunsicherung in Bezug auf die Datensicherungskonzeption und hier insbesondere die Auslagerung von Sicherungsbändern vorzuherrschen, da der Kreis Borken in seinem Vermerk zur Datensicherungsumgebung vom 19.03.2010 formuliert hat: „Aufgrund der teilweise herausragenden Bedeutung und des großen Wertes der gespeicherten Daten des Fachbereichs 62 werden die besonders schützenswerten Daten des Fachbereichs 62 zusätzlich neben der allgemeinen Datensicherung an einen externen Standort ausgelagert." Offensichtlich wird an dieser Stelle ein Restrisiko doch nicht ausgeschlossen.

In diesem Zusammenhang stellt sich auch die Frage, ob weitere, beim Kreis Borken gehostete wesentliche Verfahren und Datenbanken, wie z. B. das Finanzverfahren, das Baugenehmigungsverfahren, das Gesundheitsinformationssystem oder das Dokumentenmanagement als weniger schutzwürdig einzuschätzen sind.

Empfehlung

Wir empfehlen das Datensicherungskonzept in Bezug auf die Unterbringung der ITSM-Systeme und Erstellung und Lagerung von Sicherungsdatenträgern zu überdenken.

Datenschutz

Inhalt und Ziel

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 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 im Kreis Borken 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 vom Kreis Borken zur automatisierten Verarbeitung personenbezogener Daten eingesetzten Verfahren waren zum Zeitpunkt der Prüfung noch nicht hinreichend dokumentiert. Die im vorhandenen Verzeichnis enthaltenen Angaben sind unvollständig und erfüllen nicht die Anforderungen des § 8 Abs. 1 Nr. 1 bis 11 DSG NRW.

Der Kreis hat Maßnahmen getroffen, um in absehbarer Zeit ein den gesetzlichen Bestimmungen entsprechendes Verzeichnis zu erstellen. Die Strukturen für eine systematische Erstellung des Verzeichnisses sind vorhanden, im Intranet sind entsprechende Formulare mit umfassenden Erläuterungen verfügbar. Die Fachdienste wurden durch den Landrat aufgefordert, der Datenschutzbeauftragten bis zum 31.12.2010 die zur vollständigen Dokumentation der Verfahren erforderlichen Informationen zur Verfügung zu stellen.

Lizenzmanagement

Inhalt und Ziel

Aufgrund des hohen Durchdringungsgrades, den die Informationstechnologie in den letzten 15 Jahren in der öffentlichen Verwaltung erreicht hat, existiert heute kaum noch ein Behördenprozess, der nicht durch Software unterstützt wird. Zahlreiche Organisationen, darunter auch nicht selten öffentliche Körperschaften, haben jedoch keinen Überblick, welche Software, wo und wie oft eingesetzt wird und ob die Softwarenutzung ausreichend durch Lizenzen gedeckt ist. Die Unkenntnis entbindet jedoch nicht von der Verantwortung, lizenzrechtliche Bestimmungen einzuhalten, um mögliche rechtliche Konsequenzen abzuwenden.

Statistische Zahlen, die durch die Business Software Alliance (BSA)[16] erhoben wurden, zeigen auf, dass jede dritte Softwareinstallation nicht korrekt lizenziert im Einsatz ist.

Neben den rechtlichen Aspekten trägt eine effektive Lizenzverwaltung auch zu mehr Wirtschaftlichkeit bei. So binden einerseits ungenutzte Lizenzen unnötig Kapital, andererseits führen geschickt ausgewählte Lizenzmodelle zu Einsparpotentialen.

Namhafte Beratungsunternehmen [17]gehen derzeit davon aus, dass mit einem funktionierenden Lizenzmanagement eine Kostenreduktion von bis zu 30 Prozent mittel- bis langfristig realisiert werden kann.

Der Begriff „Lizenzmanagement" setzt sich aus „Lizenz" (die Erlaubnis) und Management (an der Hand führen) zusammen und steht für das Verwalten und Managen von Softwarelizenzen (auch Softwareassets genannt). Das Lizenzmanagement beschreibt Prozesse für den legalen und wirtschaftlichen Umgang mit Software und deren Lizenzbestimmungen.

Das Prüfmodul Lizenzmanagement ist zunächst als systemische Prüfung konzipiert und beschäftigt sich insbesondere mit der Frage, inwieweit die öffentlichen Körperschaften bereits ein aktives Lizenzmanagement

[16] Die Business Software Alliance (BSA) ist eine Non-Profit-Organisation zur Unterstützung der Ziele der Softwarebranche und ihrer Hardwarepartner. Sie ist die führende Organisation im Bereich der Förderung einer sicheren und gesetzestreuen digitalen Welt. Der Verband ist in über 80 Ländern aktiv, darunter auch in Deutschland.

17 Aus Wettbewerbsgründen findet keine namentliche Benennung statt.

betreiben. Neben der Erfassung der aktuellen Situation im Bereich des behördlichen Lizenzmanagement verfolgt die Prüfung auch das Ziel, Prozesse zur Entwicklung eines angemessenen Lizenzmanagements in Gang zu setzen, falls dies bisher noch nicht oder nicht ausreichend der Fall war. In dieser Hinsicht spielen Aufklärung und Transparenz eine wesentliche Rolle.

Die Prüfung ist durch die Verwendung von Checklisten systematisiert. Diese Checklisten werden gemeinsam mit den IT-Verantwortlichen vor Ort im Rahmen eines Interviews besprochen. Im Rahmen des Prüfungsumfanges ist nicht vorgesehen, die Ergebnisse in den Interviews zu überprüfen; dies kann nur in Einzelfällen als Stichprobe erfolgen. Vielmehr sollen im Rahmen des Interviews Chancen und Risiken gemeinsam erörtert werden. Dort wo die Prüfung zu Empfehlungen und Feststellungen führt, sind entsprechende Ausführungen in den Prüfbericht aufgenommen worden.

Lizenzmanagement beim Kreis Borken

Die Aufgabe des Lizenzmanagements wird derzeit beim Kreis Borken innerhalb des IT- Teams wahrgenommen. Dies ist jedoch in materieller Hinsicht zu verstehen, eine formale Bestellung als Lizenzmanager oder die konkrete Ausweisung von Stellenmerkmalen in der Stellenbeschreibung liegt dabei nicht vor. Die Aufgaben des Softwaremanagements werden vielmehr als nicht näher bezeichneten Part des Aufgabenanteils für die IT- Verwaltung eingestuft. Insofern sind auch für die Bewältigung dieser Aufgabe keine konkreten Zeitanteile eingeplant.

> **Empfehlung**
>
> Die Aufgabe des Lizenzmanagements sollte zumindest in die Stellenbeschreibung explizit mit aufgenommen und mit Zeitanteilen versehen werden. Es bietet sich auch an, zur Erfüllung des Lizenzmanagements Zielvereinbarungen zu formulieren, um hier für die Aufgabenerledigung eine gewisse Verbindlichkeit zu erzielen.

Organisatorische Grundlage für ein funktionierendes Lizenzmanagement ist das Vorhalten von Zeitanteilen für die zu bewältigende Aufgabe. Andernfalls wird das Lizenzmanagement bei zeitlichen Engpässen, die aufgrund des reaktiven Charakters des Tagesgeschäftes in der IT häufig vorkommen, regelmäßig zu kurz kommen.

Derzeit werden beim Kreis Borken bereits Übersichten geführt, die einen Überblick über eingesetzte und vorhandene Lizenzen dem Grunde nach ermöglicht. Allerdings sind diese Übersichten nicht ständig aktuell, da bei dem verwendeten Programm, das zur Softwareverteilung eingesetzt wird, aus Kostengründen ein verfügbares Lizenzmodul mit automatisierter Lizenzverwaltung noch nicht angeschafft wurde.

Softwareübersichten, die nicht ständig aktualisiert vorliegen und auch nur mittels erheblichen manuellem Aufwand erstellt werden, können folgende Nachteile mit sich bringen:

- Risiko von Unterlizenzierungen (rechtliche Problemstellung)
- Risiko von Überlizenzierungen (Effizienznachteile)
- Nichterkennen von freien Lizenzen (Effizienznachteile).

Hinsichtlich der Verwaltung der beim Kreis Borken eingesetzte Lizenzen der Firma Microsoft besteht jedoch derzeit kein erkennbarer unmittelbarer Handlungsbedarf, da sich der Kreis hier für den Abschluss eines sogenannten „Enterprise- Agreement"- Vertrages (Konzernvertrag) entschieden hat. Microsoft Enterprise Agreement ist ein Volumenlizenzvertrag für mittelgroße bis große Unternehmen und Organisationen, die mindestens 250 Desktop-PCs einsetzen und sich für eine standardisierte IT-Plattform auf der Basis von Microsoft Produkten entscheiden. Ziel dieser Vertragsvariante ist u.a. das Verringern des administrativen Aufwands und der Kosten, um den legalen Einsatz von Microsoft Standardprodukten sicherzustellen. Zudem wird die Budgetierung der Software-Kosten für den Vertragsnehmer deutlich vereinfacht. Insgesamt ergeben sich für den Kreis Borken folgende nennenswerte Vorteile:

- Einfache Bestellung und Verwaltung der Lizenzen
- Einfache Software- Budgetierung
- Gewähr, dass Lizenzbestimmungen stets eingehalten werden

- Einfache "Nach-Lizenzierung" zusätzlicher PCs
- stets aktueller Software-Stand
- Gleichzeitiger Erwerb von Lizenzen und Support-Leistungen möglich
- Günstige Einkaufskonditionen
- Lizenzberatung durch den Vertragsnehmer (Microsoft- Partner).

Feststellung

Durch den Mircosoft Enterprise Agreement- Vertrag hat der Kreis Borken eine gute Basis für eine rechtsichere, effiziente und effektive Lizenzverwaltung der Microsoft- Lizenzen geschaffen.

Allerdings verlässt sich der Kreis dabei vollständig auf den Vertragspartner, insbesondere auf dessen Beratungsleistungen hinsichtlich der zu beschaffenden Softwarepakete. In diesem Zusammenhang hat man bisher auch bewusst verzichtet, eigene Fachkompetenzen zu Microsoft-Lizenzmodellen (u.a. durch Fortbildungsmaßnahmen) aufzubauen.

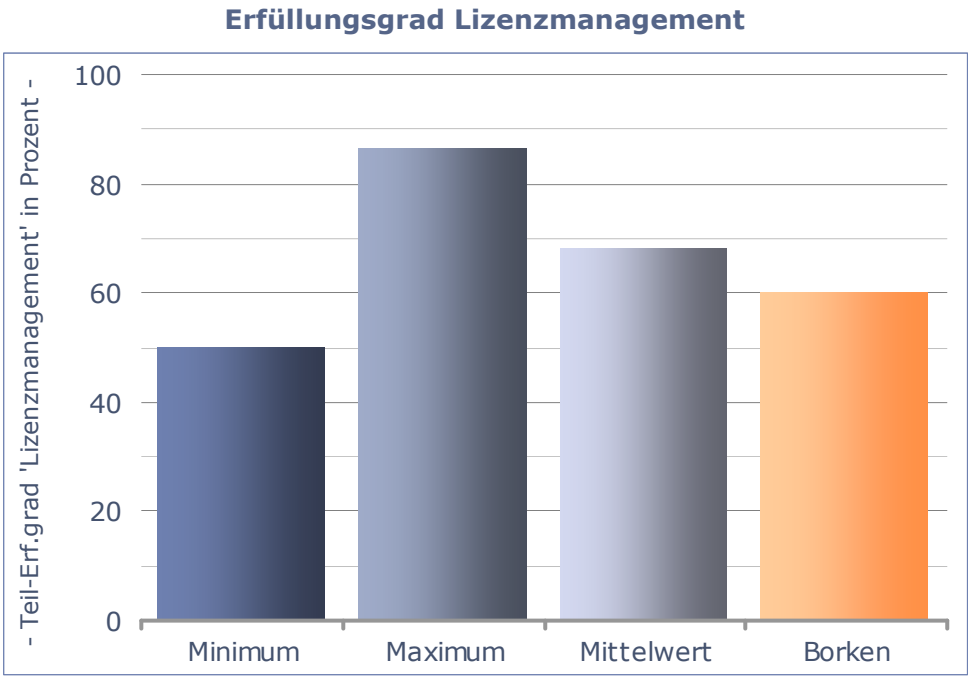
Empfehlung

Da sich der Enterprise- Agreement- (EA) Vertrag auf Microsoft-Produkte erstreckt, sollte eine Intensivierung der Lizenzverwaltung für die eingesetzten Produkte anderer Hersteller in Betracht gezogen werden. Darüber hinaus sollte trotz EA- Vertrag eigene Fachkompetenz zu den Microsoft- Lizenzmodellen aufgebaut werden.

Auch unter dem Aspekt der Umstellung des Rechnungswesens auf das NKF spielt eine vollständige und nachhaltige Softwareerfassung und Lizenzverwaltung eine wichtige Rolle, denn bilanzrechtlich betrachtet gelten Lizenzen als immaterielle Vermögenswerte und müssen daher bilanziert werden.

Lizenzmanagement im interkommunalen Vergleich

Die Ermittlung des aktuellen Standes im Bereich Lizenzmanagement wird unter Einbeziehung einer Checkliste systematisch ermittelt. Der dabei festgestellte „Erfüllungsgrad" liegt beim Kreis Borken bei 60 Prozent. Dieser Wert liegt zurzeit unter dem Mittelwert von 68,3 Prozent, der sich aus den Erfüllungsgraden der bisher 12 betrachteten Kreisverwaltungen ergibt.



Die interkommunale Betrachtung lässt jedoch nicht auf einen dringlichen Handlungsbedarf schließen, da mit dem Microsoft Enterprise Agreement-Vertrag eine Vielzahl an möglichen Risiken, die sich aus den Lizenzverträgen mit Microsoft und deren Nutzung ergeben könnten, wirksam abgedeckt werden. In diesem Zusammenhang ist auch zu berücksichtigen, dass die Microsoft- Lizenzen mit Abstand den größten Anteil an den Lizenzverträgen insgesamt ausmachen.

Dennoch sollte der Gesamtprozess des Lizenzmanagements beim Kreis Borken als ganzheitlicher Prozess ausgestaltet werden, der letztlich dazu beitragen wird, Rechtssicherheit und wirtschaftlichen Softwareeinsatz für die Gesamtheit der verwendeten Softwareprodukte sicherzustellen.

Herne, den 22.12.2010

Michael Kuzniarek
Abteilungsleitung

Ulrich Sdunek
Prüfteamleitung

GPA NRW

Überörtliche Prüfung Informationstechnologie
- Erhebungsbogen IT-Sicherheit -

Name der Kommune:
Kreis Borken

Gesprächstermin:
20.07.2010

Prüfer:
US

Gesprächspartner in der Kommune:
Herr Temme

Fragenkreis: IT-Räume und Infrastrukturaufbau

Serverraum

Baustein Serverraum:
von 21 Maßnahmen 17x JA, 1x NEIN, 3x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Angepasste Aufteilung der Stromkreise	ja	
Handfeuerlöscher	ja	Hauptrechenzentrum (Raum 2346); Gaslöschanlage/Rechnerraum (Raum 2260): Handfeuerlöscher in unmittelbarer Nähe der Maschinen/ Empfehlung: Überlegungen zu geänderter Raumgestaltung und Handfeuerlöscher vor dem Raum; Begehung der Räumlichkeiten mit Brandschutzingenieur des Kreises
Verwendung von Sicherheitstüren und -fenstern	teilw.	Die technische Infrastruktur ist über zwei Gebäudegeschosse sowie den Bunkerkeller verteilt. Es handelt sich um getrennte Brandabschnitte. Bei der Tür zum Serverraum 2346 handelt es sich um eine Feuer- und Rauchschutztür der Klasse T-30; eine besondere Härtung gegen Einbruch besteht nicht. Die Serraumtür 2260 ist weder gegen Feuer-, Rauch noch gegen Einbruch gehärtet. Hier besteht durch das angerenzende Büro und die weiteren zwei Türen die besondere Gefahr des Übergreifens von Feuer. Ferner ist der Flur frei begehbar, was auch hinsichtlich eines Einbruchs oder Vandalismus ein Risiko beherbergt. Empfehlung: Brandschutztechnische Beratung und Beratung durch die kriminalpolizeiliche Beratungsstelle.
Geschlossene Fenster	ja	
Gefahrenmeldeanlage/Brandmelder	ja	Feuer, Einbruch, Klima, Wasser, USV
Abgeschlossene Türen	ja	Besonderer Türöffner im Raum mit der Gaslöschanlage (Raum 2346).
Vermeidung von Risiken durch wasserführende Leitungen	teilw.	Im Serverraum 2260 befinden sich Heizkörper, eine entsprechende Gefahrenmeldeanlage für Wasseraustritt ist nicht vorhanden.
Überspannungsschutz	ja	
Not-Aus-Schalter	teilw.	Im Serverraum 2260 befindet sich keine Notausschaltung, auch im Bunkerkeller mit dem Backup ist keine Notausschaltung vorhanden.
Klimatisierung	ja	Die Klimatisierung der Serverräume ist redundant ausgelegt. Nur der Bunkerkellerraum verfügt über keine Klimatisierung. Bei der Begehung ist eine entpsrechend hohe Raumtemperatur vorgefunden worden. Empfehlung: Ggf. Installtion einfache Klimatisierung mit Störungsfernanzeige prüfen.
Lokale unterbrechungsfreie Stromversorgung	ja	
Fernanzeige von Störungen	ja	s. o.
Redundanzen in der technischen Infrastruktur (ohne Storage)	ja	
Technische und organisatorische Vorgaben für Serverräume	ja	Der Raum 2345 ist im Jahre 2005 neu geplant worden, eine entsprechende Planung ist durchgeführt und dokumentiert worden.
Brandschutz von Patchfeldern	ja	Gaslöschanlage
Zutrittsregelung und -kontrolle	ja	Die Serverräume sind über elektronisch codierte Schlüssel zugänglich. Schlüssel sind beim IT-Leiter hinterlegt und werden nur bei Bedarf an die berechtigten Administratoren herausgegeben. Eine Dokumentation über das Betreten der Serverräume besteht in muneller Form. Im Rahmen der Erörterung der Checkliste wurde die Überlegung angeregt, den Zutritt elektronisch zu steuern und zu dokumentieren.
Rauchverbot	ja	
Verwendung von hochverfügbaren Architekturen	ja	
Zentrales Speichersystem vorhanden	ja	nicht redundat
Storage System redundant	nein	
Einsatz von Servervirtualisierung	ja	

IT-Verkabelung

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

Maßnahmen	erfüllt?	Bemerkungen
Verkabelungsart den technischen Anforderungen entsprechend	ja	LWL bis zu den Büros
Netz-Topologie	ja	Ethernet
Erneuerung der IT-Verkabelung	ja	2005
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	wegen LWL
Materielle Sicherung von Leitungen und Verteilern	ja	
Dimensionierung und Nutzung von Schranksystemen	ja	
Neutrale Dokumentation in den Verteilern	ja	
Laufende Fortschreibung und Revision der Netzdokumentation	ja	

Sicherheitsgateway

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

Maßnahmen	erfüllt?	Bemerkungen
Outsourcing des Sicherheitsgateway		☐ Sicherheitsgateway ausgelagert, keine unmittelbare Prüfung erfolgt
Entwicklung eines Konzepts für Sicherheitsgateways	ja	Beauftragung einer externen Firma
Auswahl geeigneter Grundstrukturen für Sicherheitsgateways	ja	Es wurde eine Studie in Auftrag gegeben, die die Grundlage für die Planung und Leistungsbeschreibung darstellte.
Content-Filter im Einsatz	ja	Die Installation ist durch die IT-Steuerungsgruppe beschlossen.
Proxyserver im Einsatz	ja	
Gateway redundant	ja	
Schulung der Administratoren des Sicherheitsgateways	ja	
Protokollierung der Sicherheitsgateway-Aktivitäten	ja	im Managed Service enthalten
Integration von Proxyservern in das Sicherheitsgateway	ja	
Integration von VPN-Komponenten in ein Sicherheitsgateway	ja	
Integration von Virenscannern in ein Sicherheitsgateway	ja	Es werden zwei unterschiedliche Virenscanner genutzt.
Einsatz von Stand-alone-Systemen zur Nutzung des Internets	ja	
Adressumsetzung - NAT (Network Address Translation)	ja	
Intrusion Detection und Intrusion Prevention Systeme	ja	
Integration eines Webservers in ein Sicherheitsgateway	nein	
Integration eines E-Mailservers in ein Sicherheitsgateway	ja	
Integration eines Datenbank-Servers in ein Sicherheitsgateway	nein	
Integration eines DNS-Servers in ein Sicherheitsgateway	ja	
Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway	ja	
Notfallvorsorge bei Sicherheitsgateways	ja	Das Sicherheitsgateway ist zwar redundant ausgelegt, in einem besonderen Notfallvorsorgekonzeot wird es aber nicht behandelt.

WLAN

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

Maßnahmen	erfüllt?	Bemerkungen
Geeignete Aufstellung von Access Points	ja	
Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung	ja	Das WLAN Projekt ist noch nicht abgeschlossen, eine Richtlinie sowie eine Dokumentation wird im Rahmen dieses Prozesse erstellt werden.
Auswahl eines geeigneten WLAN-Standards	ja	
Auswahl geeigneter Kryptoverfahren für WLAN	ja	

Geeignetes WLAN-Schlüsselmanagement	ja	Smartpass
Schulung zum sicheren WLAN-Einsatz	ja	Im Rahmen der Einführung des WLAN ist eine Schulung enthalten.
Sichere Konfiguration der Access Points	ja	
Sichere Konfiguration der WLAN-Clients	ja	
Regelmäßige Sicherheitschecks in WLANs	ja	ist im Rahmen des Betriebes geplant

Fragenkreis: Technische Ausstattung der Arbeitsplätze

Notebooks

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

Maßnahmen	erfüllt?	Bemerkungen
Existiert bei Notebooks Homogenität?	ja	
Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz	ja	
Einsatz von Diebstahl-Sicherungen	nein	
Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung	ja	Richtlinie für die Nutzung mobiler Geräte
Regelmäßiger Einsatz eines Anti-Viren-Programms	ja	
Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme	ja	Ein Verschlüsselungsprodukt ist beschafft und wird implementiert.
Sichere Kommunikation von unterwegs	ja	
Sicherer Anschluss von Notebooks an lokale Netze	ja	
Datensicherung bei mobiler Nutzung des IT-Systems	entfällt	lokale Datenhaltung nicht zulässig

Allgemeiner Client

Baustein Allgemeiner Client:
von 14 Maßnahmen 13x JA, 0x NEIN, 0x teilweise, 1x 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?		4 Jahre
Wird ein Systemmanagement eingesetzt?	ja	
Wird Remote Desktop genutzt?	ja	
Herausgabe einer PC-Richtlinie	ja	Dienstanweisung
Dokumentation der Systemkonfiguration	ja	
Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	ja	
Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz	ja	Betriebshandbuch
Geregelte Außerbetriebnahme eines Clients	ja	Derzeit wird das Tool Novell Identity Manager implementiert (Benutzer Lifecycle Management).
Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung	ja	
Regelmäßiger Einsatz eines Anti-Viren-Programms	ja	
Einrichten einer Referenzinstallation für Clients	ja	
Regelmäßige Datensicherung	entfällt	keine lokale Datenhaltung

Fragenkreis: IT-Management

Sicherheitsmanagement

Baustein Sicherheitsmanagement:
von 8 Maßnahmen 2x JA, 4x NEIN, 2x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Erstellung einer Leitlinie zur Informationssicherheit	nein	
Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	ja	Sicherheitsbeauftragte (seit 01.04.2010 im Einsatz); direkt dem Landrat unterstellt
Erstellung eines Sicherheitskonzepts	teilw.	Es sind externe Untersuchungen zur Sicherheit in der IT in Auftrag gegeben worden (Security Scan). Die Untersuchung hat im Wesentlichen die Netzinfrastruktur und das Sicherheitsgateway betroffen.
Management-Berichte zur Informationssicherheit	ja	Aktuell ist ein Managementbericht erstellt worden, regelmäßige Berichte sind beabsichtigt.
Dokumentation des Sicherheitsprozesses	teilw.	
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	
Vergabe von Zugriffsrechten	ja	
Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln	ja	
Schlüsselverwaltung	ja	
Kontrollgänge	ja	

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	IT-Koordinatoren in den Facheinheiten
Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen	ja	
Schulung vor Programmnutzung	ja	
Schulung zu IT-Sicherheitsmaßnahmen	ja	u. a. auch über das Intranet
Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern	ja	
Schulung des Wartungs- und Administrationspersonals	ja	
Personaleinsatz und -qualifizierung	ja	
Vertraulichkeitsvereinbarungen	teilw.	

Notfallvorsorgekonzept

Baustein Notfallvorsorgekonzept:
von 15 Maßnahmen 4x JA, 10x NEIN, 1x teilweise, 0x entfällt

Maßnahmen	erfüllt?	Bemerkungen
Erstellung einer Übersicht über Verfügbarkeitsanforderungen	nein	
Notfall-Definition, Notfall-Verantwortlicher	nein	
Erstellung eines Notfall-Handbuches	teilw.	Betriebshandbuch enthält gewisse Bestandteile
Dokumentation der Kapazitätsanforderungen der IT-Anwendungen	nein	
Definition des eingeschränkten IT-Betriebs	nein	
Untersuchung interner und externer Ausweichmöglichkeiten	nein	
Regelung der Verantwortung im Notfall	ja	Betriebshandbuch enthält Regelungen
Alarmierungsplan	nein	
Notfall-Pläne für ausgewählte Schadensereignisse	nein	

Erstellung eines Wiederanlaufplans	nein	
Durchführung von Notfallübungen	nein	
Erstellung eines Datensicherungsplans	ja	
Ersatzbeschaffungsplan	nein	
Abschließen von Versicherungen	ja	
Redundante Kommunikationsverbindungen	ja	

Hard- und Softwaremanagement

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

Maßnahmen	erfüllt?	Bemerkungen
Regelung des Passwortgebrauchs	ja	
Hinterlegen des Passwortes	ja	
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	Es ist ein Workflow installiert.
Kontrolle der Protokolldateien	ja	

Virenschutz

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

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

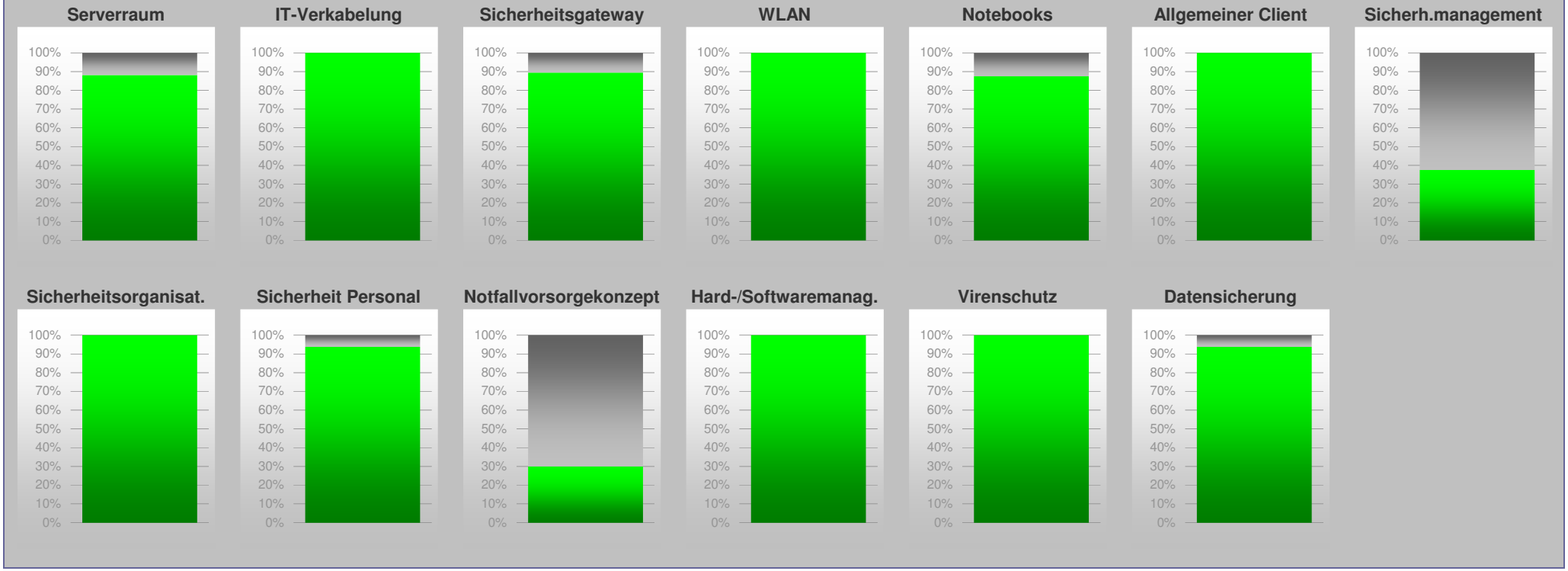
Fragenkreis: Backup und Archivierung

Datensicherung

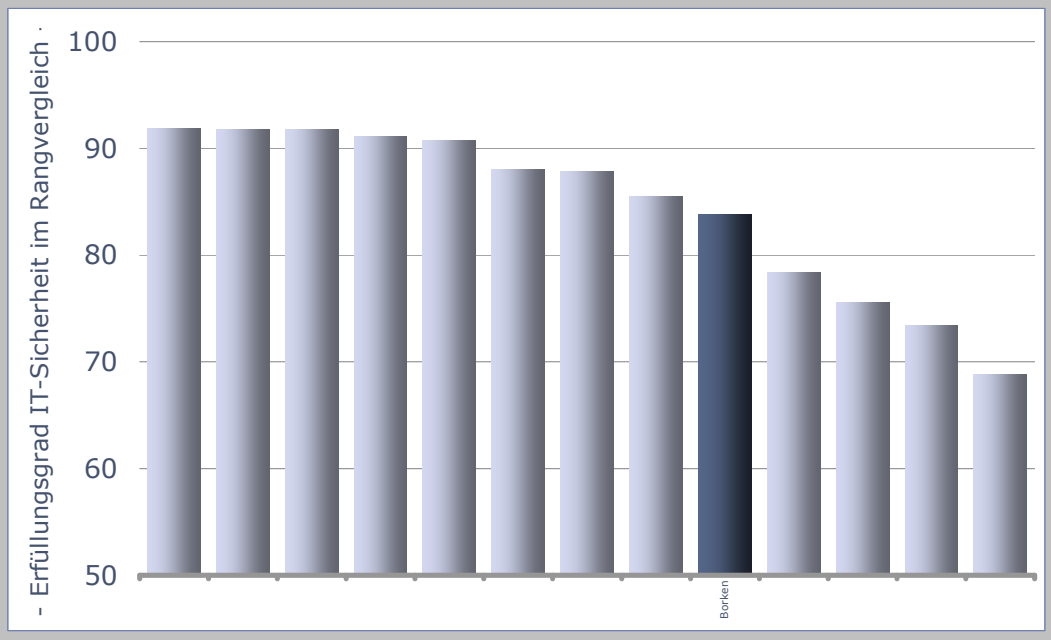
Baustein Datensicherung:
von 9 Maßnahmen 7x JA, 0x NEIN, 1x teilweise, 1x entfällt

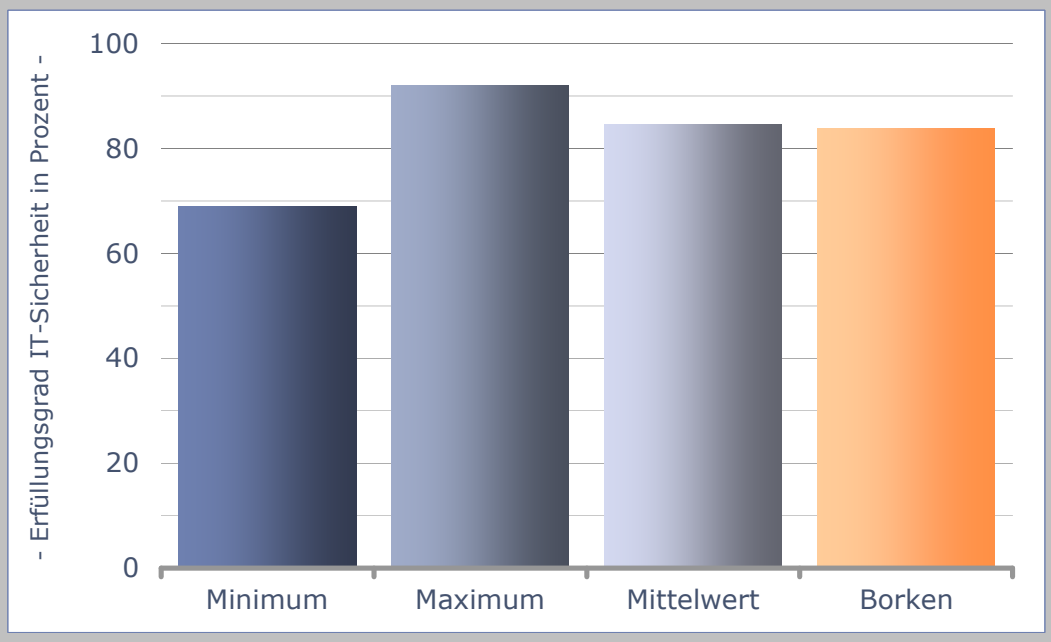
Maßnahmen	erfüllt?	Bemerkungen
Verpflichtung der Mitarbeiter zur Datensicherung	entfällt	keine lokale Datenhaltung
Beschaffung eines geeigneten Datensicherungssystems	ja	
Geeignete Aufbewahrung der Backup-Datenträger	teilw.	Das Backup-System mit der Tape Library ist in einem Schutzkeller untergeracht, der über keine Klimatisierung verfügt.
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 Kreis Borken -

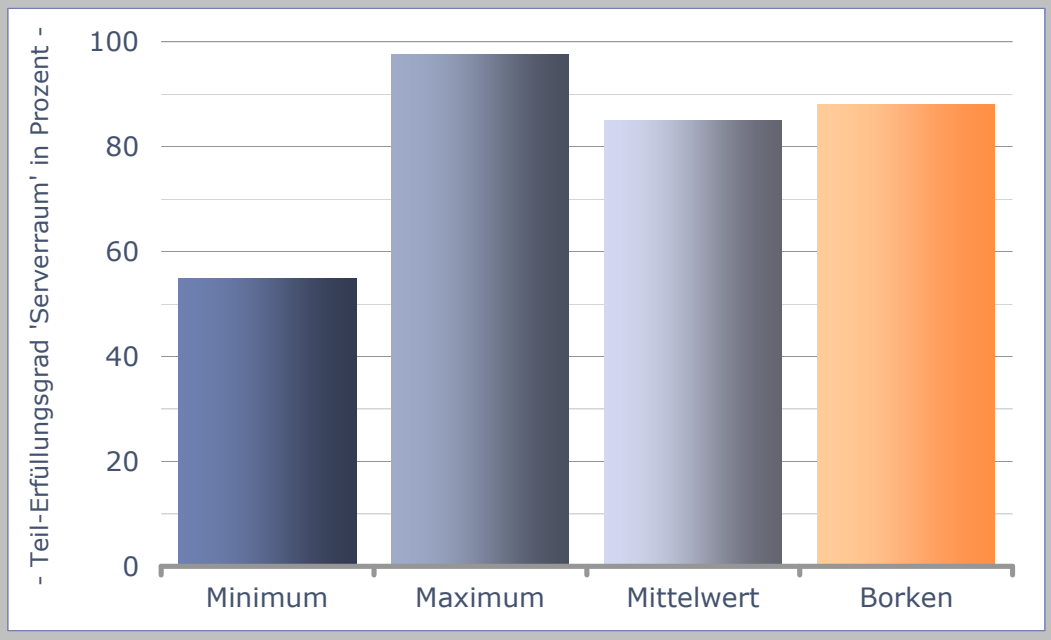


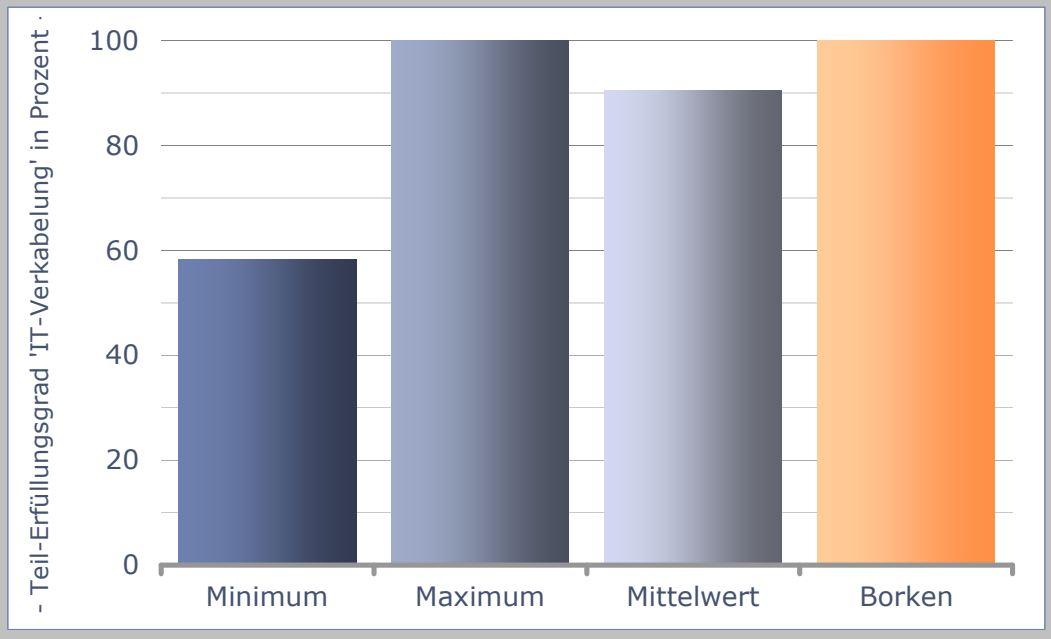
Überörtliche Prüfung Informationstechnologie
- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -
(Kreise 2010/2011)



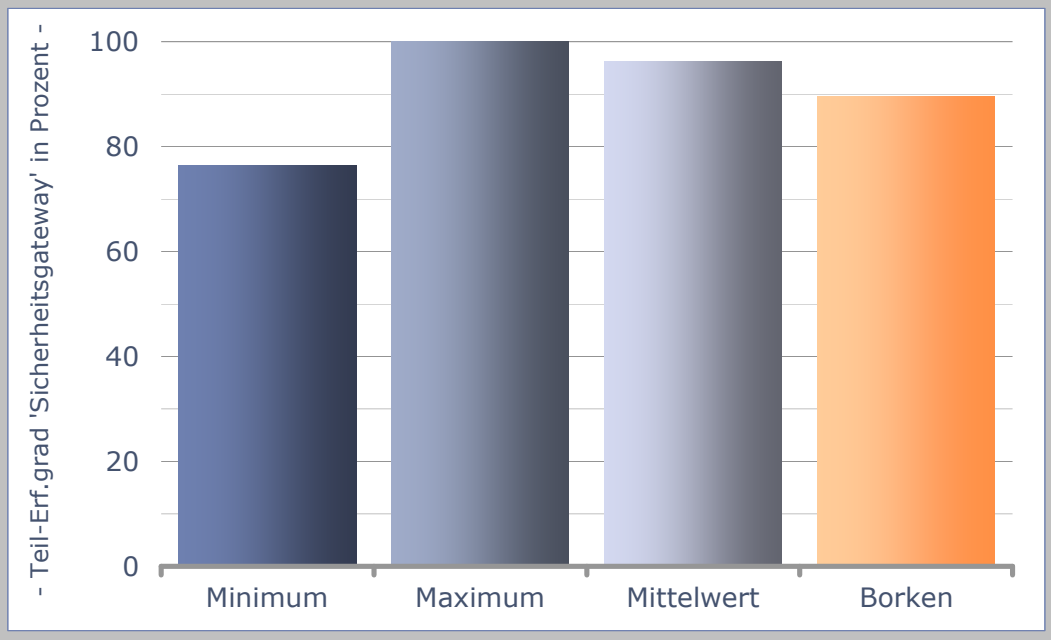


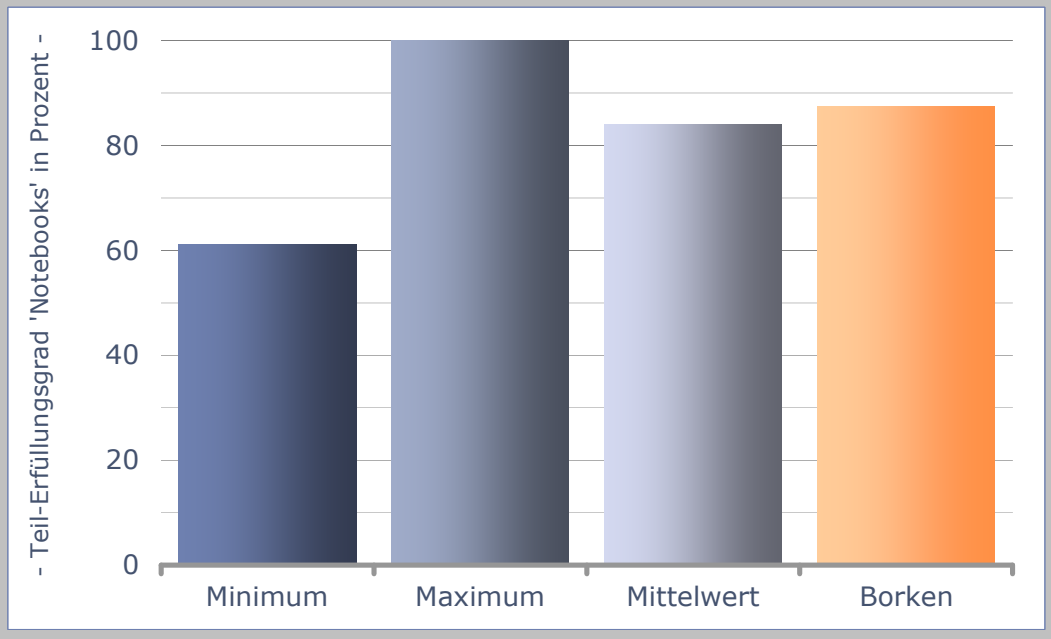
Überörtliche Prüfung Informationstechnologie
- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -
(Kreise 2010/2011)



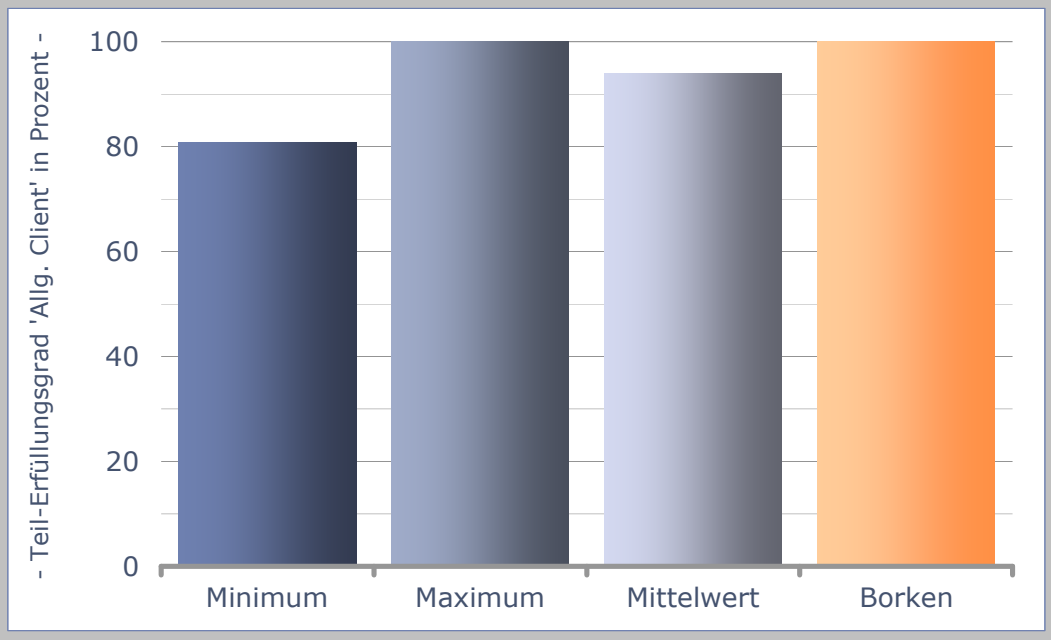


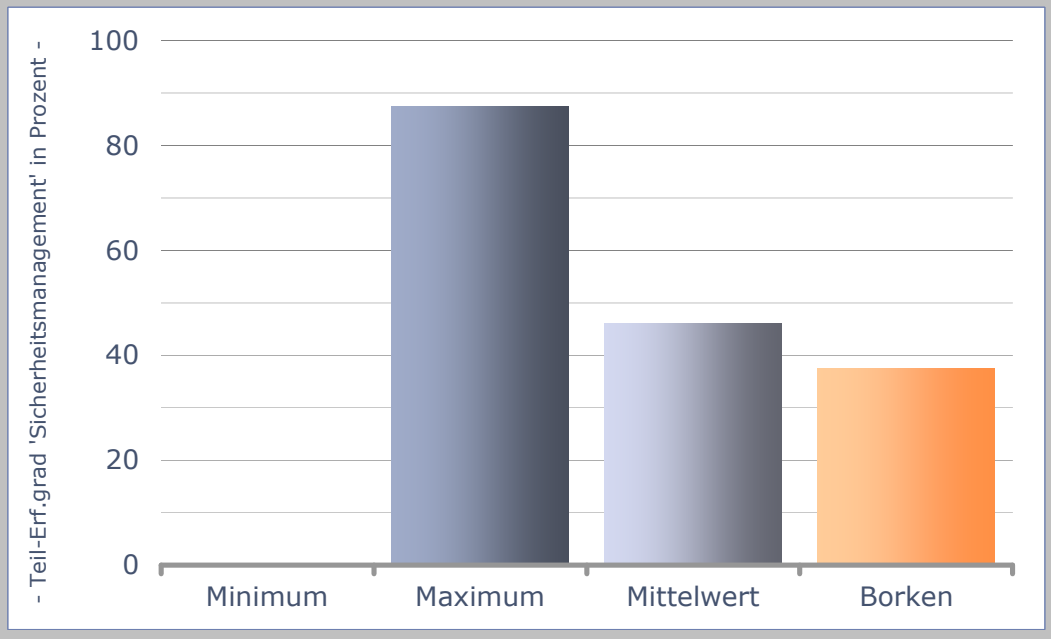
Überörtliche Prüfung Informationstechnologie
- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -
(Kreise 2010/2011)



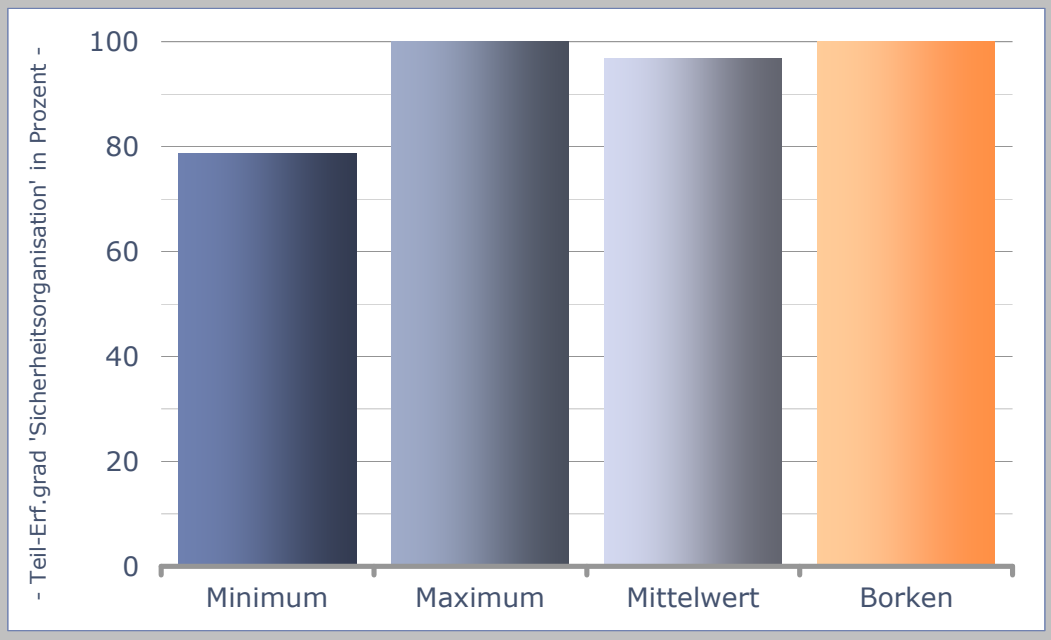


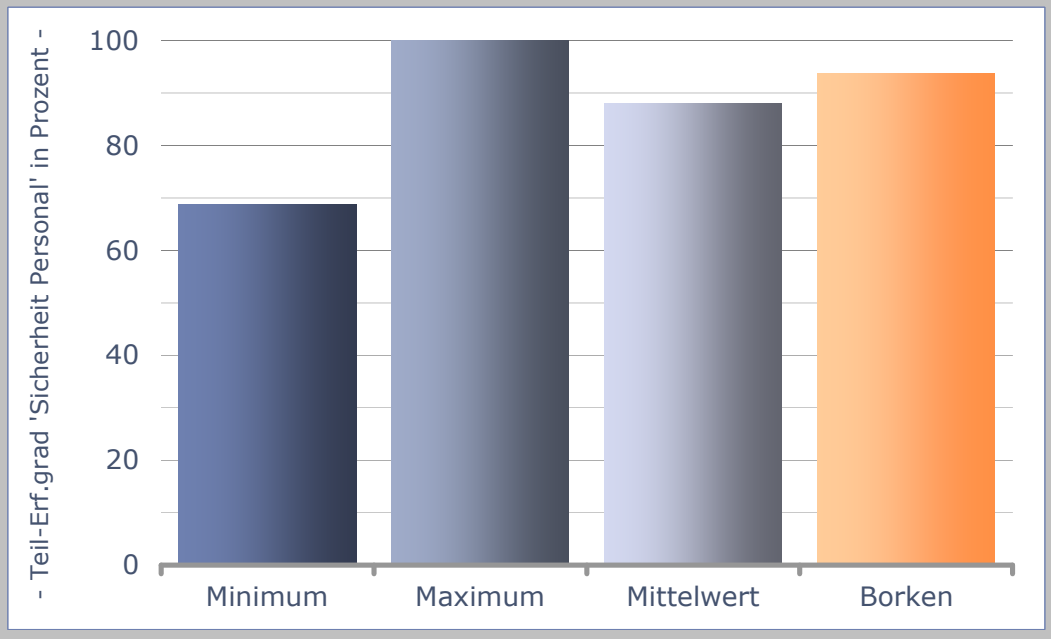
Überörtliche Prüfung Informationstechnologie
- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -
(Kreise 2010/2011)



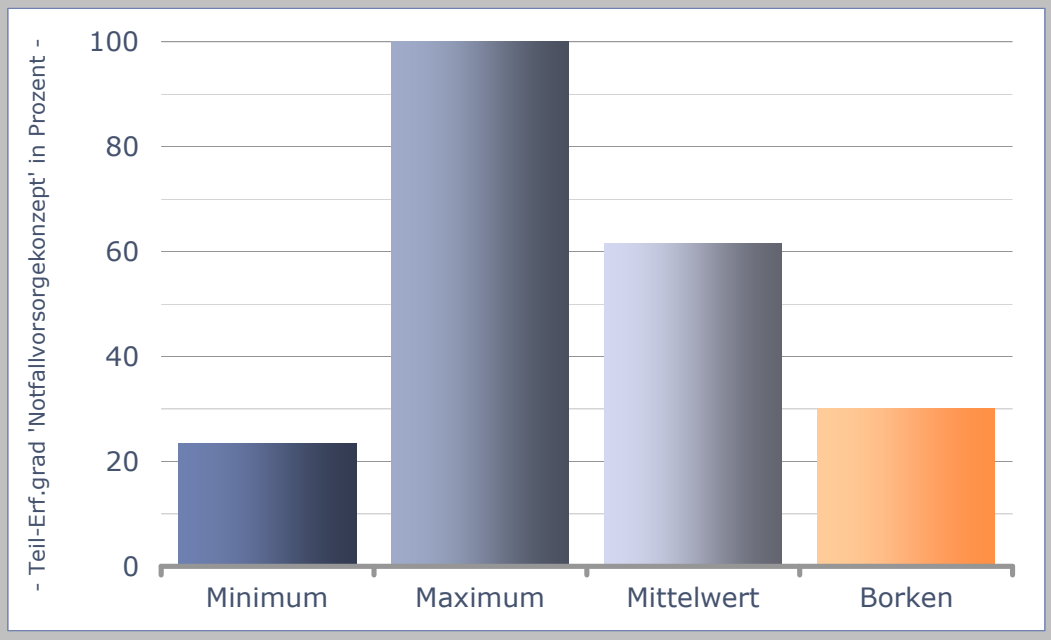


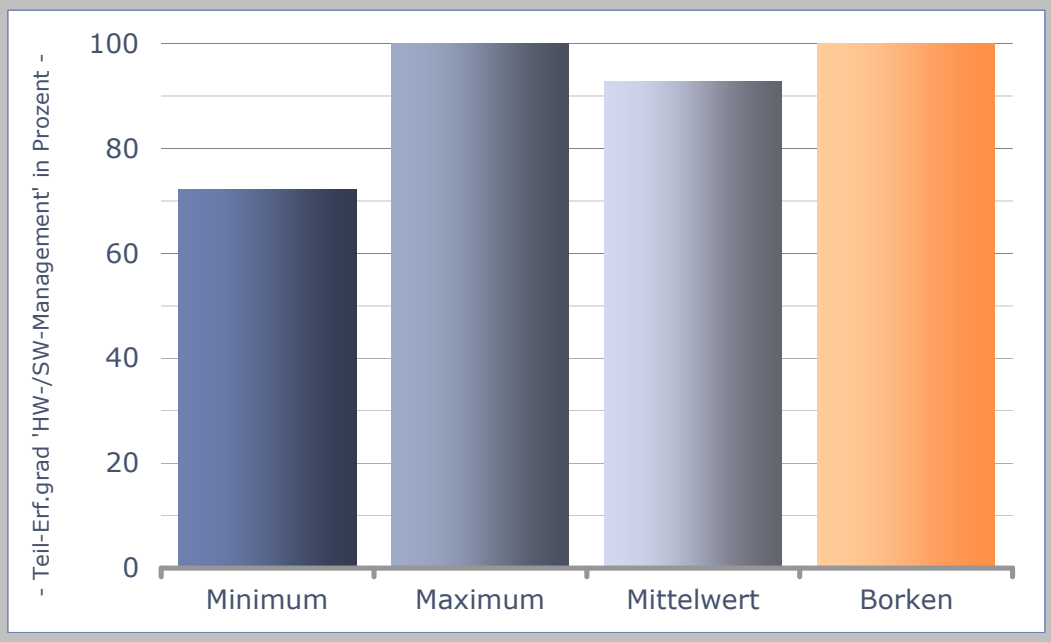
Überörtliche Prüfung Informationstechnologie
- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -
(Kreise 2010/2011)





Überörtliche Prüfung Informationstechnologie
- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -
(Kreise 2010/2011)





Überörtliche Prüfung Informationstechnologie
- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -
(Kreise 2010/2011)