

Stadt Sankt Augustin

Rechnungsprüfungsamt



Prüfbericht IuK

Prüfung des internen Kontroll- und Steuerungssystems
für IT –Risikofelder in ausgewählten Bereichen

Inhaltsverzeichnis:	Seite
1. Prüfungsgrundlagen	2
2. Gesamtfazit	3
3. Feststellungen und Empfehlungen	4
4. Weitere Vorgehensweise	9
5. Wirtschaftlichkeitsbetrachtung/IT- Kennzahlen	11

Anlage:
Bericht der GPA NRW
Evaluation des internen Kontroll- und Steuerungssystems der Stadt Sankt Augustin.
Betrachtung der IT- Risikofelder in ausgewählten Bereichen.

1. Prüfgrundlagen

Das Rechnungsprüfungsamt der Stadt Sankt Augustin hat im Rahmen der Jahresprüfung (risikoorientierter Prüfungsansatz) die Überprüfung der Wirksamkeit des internen Kontroll- und Steuerungssystems, das u. a. auch die vorhandenen Strukturen und Abläufe des EDV-Betriebes in den Blick nimmt, in Zusammenarbeit mit der GPA NRW geprüft.

Die Prüfung wurde im Dezember 2011 begonnen und im Juni 2012 abgeschlossen. In einem ersten Schritt wurde der Status des vorhandenen IT-Grundschutzes in den Blick genommen und zu den einzelnen Bereichen Feststellungen getroffen.

Im Einzelnen erfolgten folgende Schritte:

- Festlegung des aktuellen Status des vorhandenen IT-Grundschutzes unter Einbeziehung ausgewählter Richtlinien des BSI, nach Art der GPA NRW; untersucht wurden 13 Teilbereiche (Bausteine) mit insgesamt 145 Einzelaspekten. Die Durchführung erfolgte mittels standardisierter Checklisten im Interviewverfahren. Daneben erfolgte eine Begehung der relevanten IT Räumlichkeiten.
- Auswertung der Ergebnisse und grafische Darstellung.
- Darstellung von Risikopotentialen und interkommunale Standortbestimmung.

Ergänzend dazu wurden die Checklisten des Prüferarbeitsplatzes für die Jahresprüfung 2010 auf der Grundlage des IDW Prüfungsrahmens PS 330 zur EDV- Organisation gemeinsam aufgenommen und in die Checklisten übertragen.

Diese Checklisten betreffen folgende Bereiche:

- Funktion der Buchführung und Datenverarbeitung
- Prüfung der IT-Strategie
- Prüfung des IT-Umfeldes
- Prüfung der IT-Organisation
- Prüfung der IT-Infrastruktur
- Prüfung der IT-Anwendungen
- Prüfung der IT-gestützten Geschäftsprozesse
- Prüfung der IT-Überwachungssysteme
- Prüfung des IT-Outsourcing
- Besonderheiten der Internet Nutzung

2. Gesamtfazit

Neben der Inanspruchnahme von Dienstleistungen der Civitec betreibt die IT der Stadtverwaltung in Sankt Augustin eine eigene IT- Infrastruktur. Die technische und organisatorische Ausgestaltung der örtlichen IT ist im interkommunalen Vergleich überdurchschnittlich gut aufgestellt. Die Sicherheitsstrategie sowie die Datensicherungsstrategie werden dabei hervorgehoben, wenngleich die derzeit bestehende Vakanz in der Stelle des Sicherheitsbeauftragten als Rückschritt einer bis dahin sehr guten Ausgangslage gewertet wird. Generell kann jedoch ein sehr hohes Sicherheitsbewusstsein und eine hohe Fachkompetenz der IT- Verantwortlichen festgestellt werden.

Sicherheitsrisiken, die einen unmittelbaren Handlungsbedarf signalisieren, konnten nicht festgestellt werden. Die mit dem IT- Betrieb verbundenen Risikopotentiale sind auf ein beherrschbares Mindestmaß reduziert worden, wenngleich noch Optimierungspotentiale in dem Bereich des vorbeugenden Brandschutzes und beim Sicherheitgateway beleuchtet werden konnten.

Darüber hinaus sollte geprüft werden, ob eine redundante Ausgestaltung der Gebäudeverkabelung und des Sicherheitsgateways im Rahmen der Notfallvorsorge (Verfügbarkeitsanforderungen) erforderlich sein könnte.

Eine Betrachtung des Ressourceneinsatzes für den Einsatz der Informationstechnologie bei der Stadt Sankt Augustin war nicht Gegenstand der Prüfung.

3. Feststellungen bzw. Empfehlungen :

a) IT-Sicherheit

Verteilerraum 5. OG

Vorbeugender Brandschutz

Empfehlung 1

Um den sicheren Betrieb unter Gesichtspunkten des Brandschutzes zu gewährleisten, sollten in den Räumlichkeiten der technischen Infrastruktur Brandlasten möglichst vermieden werden. Bezüglich der weitergehenden Brandschutzmaßnahmen empfehlen wir eine Kontaktaufnahme mit dem Gebäudemanagement und der örtlichen Feuerwehr.

Stellungnahme der Verwaltung

Sämtliche vermeidbare Brandlasten, wie z.B. Kartons oder Datenträger wurden bereits aus den Räumen der technischen Infrastruktur entfernt.

Ein Anschluss an das Brandmeldesystem wurde bereits bei Fachbereich 9 beantragt. Die Beschaffenheit der Zugangstür muss abgeklärt werden. Im Rahmen der Neuverkabelungsmaßnahme 2001 wurden die Verteilerräume baulich neu und nach damals gültigem Brandschutz erstellt. Der Fachbereich 9 wurde um Prüfung gebeten.

Mit der Stellungnahme der Verwaltung ist der Empfehlung des Rechnungsprüfungsamtes gefolgt worden und ist somit erledigt.

IT-Verkabelung

Redundanzen in der Gebäudeverkabelung

Empfehlung 2

Über eine Verfügbarkeitsanalyse sollte geprüft werden, inwieweit die Gebäudeverkabelung redundant auszulegen ist.

Stellungnahme der Verwaltung

Die Risikoanalyse der Gemeindeprüfanstalt Nordrhein-Westfalen konkretisiert diese Empfehlung insofern, als das dort empfohlen wird, zuerst die Verkabelung der einzelnen Etagen-Verteilerräume untereinander redundant auszulegen und danach die Büroräume an beide Verteilerräume anzuschließen.

Bereits der erste Schritt ist mit erheblichen baulichen Maßnahmen verbunden. Ein zusätzlicher Steigschacht, der entsprechend weit vom vorhandenen Steigschacht in der Mitte des Rathauses entfernt ist, existiert nicht. Ein solcher müsste also baulich neu angefügt werden. Gleichzeitig muss je Etage ein zusätzlicher Verteilerraum erstellt werden. Danach müssen in jeden Büroraum zusätzliche Kabel eingelegt werden, so dass die dortigen EDV-Anschlussdosen wechselseitig an beide Verteiler angeschlossen werden können. Zusätzlich müssten für den zweiten Verteilerraum die aktiven LAN Komponenten je Etage redundant beschafft werden. Die Elektroverkabelung muss dann ebenfalls im gleichen Rahmen redundant ausgelegt werden. Ebenso ist eine Prüfung für die Nebenstellen im Ärztehaus und dem Technopark erforderlich.

Auf Grund der offensichtlich hohen Investitionskosten für eine solche Maßnahme sollte sie nicht allein zu diesem Zweck angegangen werden. Allerdings steht außer Frage, dass eine Verfügbarkeitsanalyse in Bezug auf eine redundanten Verkabelung dann geprüft und ausgearbeitet werden sollte, wenn ohnehin in einem der verschiedenen Gebäude Baumaßnahmen anstehen. Aus diesem Grund wird der Fachbereich 9 ebenfalls über den Inhalt meiner Stellungnahme informiert.

Mit der Stellungnahme der Verwaltung ist der Empfehlung des Rechnungsprüfungsamtes gefolgt worden und ist somit erledigt.

b) IT-Management (Konzepte, Dienstanweisungen, Risikomanagement)

Sicherheitsmanagement

Empfehlung 3

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

Stellungnahme der Verwaltung

Nach den Ausführungen des BSI gehen solche Maßnahmen i.d.R. vom IT-Sicherheitsbeauftragten aus. Aus Anlass dieses Prüfberichtes wird jedoch die Stabsstelle IuK dem VV eine IT-Sicherheitsleitlinie zur Entscheidung vorlegen. Darin wird zu den zentralen Punkten der Informationssicherheit, sowie einer IT-Sicherheitsgruppe und der Sensibilisierung der Beschäftigten Stellung bezogen.

Mit der Stellungnahme der Verwaltung ist der Empfehlung des Rechnungsprüfungsamtes gefolgt worden und ist somit erledigt.

Organisationsstruktur für Informationssicherheit

Empfehlung 4

Wir empfehlen grundsätzlich, die Nachbesetzung der Stelle eines IT-Sicherheitsbeauftragten zu prüfen.

Hierbei sind 3 Varianten denkbar, wobei die Variante 1 eine optimale Ausgangslage bietet, die Variante 2 eine befriedigende Alternative darstellt und die Variante 3 als Minimallösung bewertet wird.

Variante 1	Stelle des Sicherheitsbeauftragten wiederbesetzen
Variante 2	Funktion des Sicherheitsbeauftragten an die Stelle des Datenschutzbeauftragten koppeln
Variante 3	Einrichten einer Arbeitsgruppe „IT-Sicherheit“

Unabhängig davon, welche Variante hier bevorzugt wird, ist die künftige Einbindung des RPA als obligatorisch zu betrachten, da hier wesentliche und unbedingt notwendige Informationen für die nachfolgende Fortführung und Weiterentwicklung des Internen Kontroll- Systems (IKS) zu erzielen sind.

Stellungnahme der Verwaltung

IUK empfiehlt die Einrichtung einer Arbeitsgruppe „IT-Sicherheit“ und hat diesen Vorschlag dem Verwaltungsvorstand zur Entscheidung für die Sitzung am 6.11.2012 vorgelegt. Lt. Mitteilung der Verwaltung hat der Verwaltungsvorstand beschlossen, eine Leitlinie zur IT Sicherheit und die Einrichtung eines IT-Sicherheitsteam beschlossen. Das IT Sicherheitsteam besteht aus dem Datenschutzbeauftragten, dem Steuerungsdienst und dem Bereich Information und Kommunikation.

Mit der Stellungnahme der Verwaltung ist der Empfehlung des Rechnungsprüfungsamtes gefolgt worden und ist somit erledigt.

Management-Berichte zur IT-Sicherheit

Empfehlung 5

Da bei der Stadt Sankt Augustin derzeit die Stelle des IT-Sicherheitsbeauftragten unbesetzt ist, sollten übergangsweise die Berichte zur IT-Sicherheit von der IT erstellt werden, um der Verwaltungsleitung alle Informationen für eine Risikobewertung transparent zu machen und eine Basis für notwendige Entscheidungen zu liefern.

Stellungnahme der Verwaltung

Über die IT-Sicherheit wird momentan in den regelmäßig stattfindenden Rücksprachen von IuK berichtet. Bestehende Gefahren oder Sicherheitsvorfälle werden je nach Ihrer Wichtigkeit oder Gefährdungsstufe direkt dem Bürgermeister gemeldet. Die Entscheidung, was vorgelegt wird und wann es vorgelegt wird erfolgt im Ermessen des Stabsstellenleiters IuK.

Mit der Stellungnahme der Verwaltung ist der Empfehlung des Rechnungsprüfungsamtes gefolgt worden und ist somit erledigt.

Empfehlung 6

Für das IT-Personal sollten regelmäßig Schulungen zum Thema IT-Sicherheit erfolgen, um zusätzliche Kompetenzen zu grundsätzlichen Risiken und aktuellen Gefährdungslagen aufzubauen, die zur Schulung der Mitarbeiter herangezogen werden können.

Stellungnahme der Verwaltung

Dieses Jahr hat bisher ein Mitarbeiter der LuK eine IT-Sicherheits Informationsveranstaltung besucht. Der Besuch einer weiteren Veranstaltung durch einen anderen ist bereits terminiert. Die dort erworbenen Kenntnisse werden im Rahmen der Multiplikation an die übrigen Mitarbeiter der LuK weitergegeben. Des weiteren wird IT-Sicherheit in regelmäßig stattfindenden Dienstbesprechung behandelt.

Die Stabsstelle LuK wird dem Verwaltungsvorstand jedoch zusätzlich vorschlagen, dass für alle Beschäftigten regelmäßig Fortbildungsveranstaltungen zum Thema IT-Sicherheit im Hause durchgeführt werden. In diesen Veranstaltungen werden die Beschäftigten über die bestehenden Gefahren informiert und zum verantwortungsbewussten Handeln befähigt.

Mit der Stellungnahme der Verwaltung ist der Empfehlung des Rechnungsprüfungsamtes gefolgt worden und ist somit erledigt.

4. Weitere Vorgehensweise

In den kommenden Jahresprüfungen sind folgende Stichpunktprüfungen durchzuführen bzw. folgende Datenbestände in regelmäßigen Abständen auf Plausibilität zu prüfen. Dies wird teilweise auch durch externe Unterstützung erfolgen:

Themenbereich	Geschätzter Zeitaufwand ¹
Erfassung aller relevanten Arbeitsschritte zur Aufnahme von rechnungslegungsrelevanten Daten (bisher besteht hier nur eine Übergangsregelung).	1 bis 3 Monate
Überprüfung der Rechtestruktur/Berechtigungen (jährliche Stichprobenprüfung).	<1 Monat, hohe Priorität
Erarbeiten einer IT-Prüfungsplanung und Vorbereitung auf künftige IT-Prüfungen durch Fortbildungen.	<1 Monat
Plausibilitätsprüfungen der IT-Investitions- und Personalbedarfsplanung.	>3 Monate
Aufnahme und Bewertung von bestehenden Abhängigkeiten zu einzelnen IT-Mitarbeitern und Dienstleistern.	<1 Monat
Vergleich Soll-/Ist-Zustand der IT-Stellenbeschreibungen sowie Beurteilung der IT-Tätigkeitsbeschreibungen.	>3 Monate
Aufnahme und Bewertung der Zusammenarbeit zwischen IT und den Fachbereichen (Effizienz/Effektivität).	>3 Monate
Fortlaufende Betrachtung der Einhaltung der Regelungen zur Benutzerverwaltung (Werden die Regelungen zur Vergabe von Nutzerberechtigungen zufriedenstellend umgesetzt – Kooperation mit Da-	<1 Monat, jährlicher Aufwand

¹ Der hier dargestellte Zeitaufwand kann nur eine Tendenz aufzeigen, da die individuellen Bedarfe nur durch eine konkrete Einschätzung des akuten Sachverhaltes bestimmt werden können.

Themenbereich	Geschätzter Zeitaufwand ¹
tenschutzbeauftragtem).	
Aufnahme und Bewertung von der sachgerechten Behandlung von Fehlern und Problemfällen bei der Datensicherung.	<1 Monat, hohe Priorität
Beurteilung der Wirksamkeit der Wiederanlaufverfahren.	<1 Monat
Regelmäßige Kontrolle der Software-Versionsstände.	<1 Monat
Regelmäßige Kontrolle der Freigabeverfahren und Testverfahren für Fachverfahren (auch für Updates).	<1 Monat
Kontrolle der Umsetzung der Handlungsempfehlungen der externen Prüfungen mit IT-Bezug.	<1 Monat

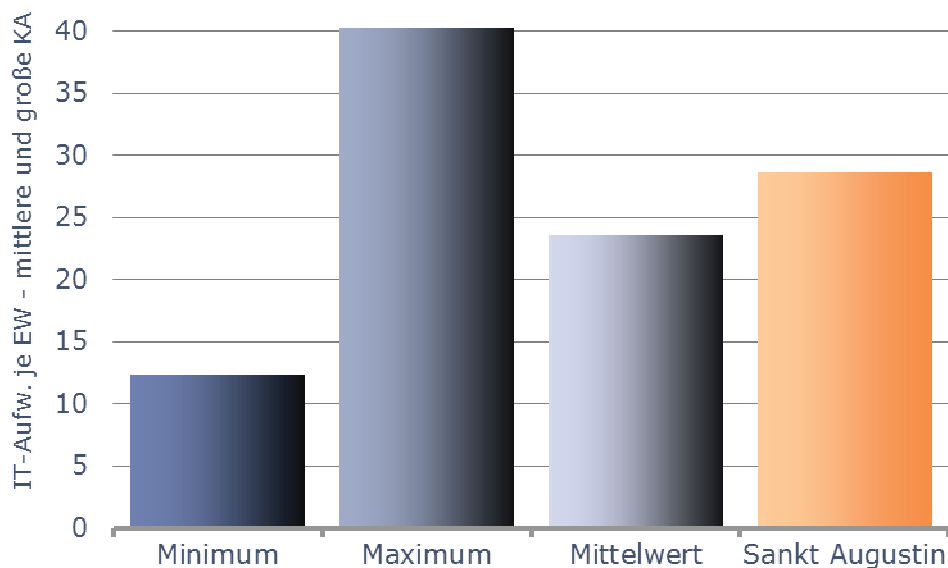
5. Wirtschaftlichkeitsbetrachtung/ IT- Kennzahlen

Im Rahmen der Beratung wurden mit der GPA NRW auch Methoden der Kennzahlenerhebung erörtert. Zielsetzung war hier die Idee, Wirtschaftlichkeitskennzahlen zukünftig darstellen zu wollen, die eine interne Entwicklung im Zeitreihenvergleich darstellen kann und zugleich auch einen interkommunalen Vergleich zur Standortbestimmung zulässt.

Um für eine erste Standortbestimmung einen Orientierungswert erhalten zu können, wurde vom Rechnungsprüfungsamt die für die IT zugehörigen Finanzdaten ermittelt und nach einem von der GPA NRW bereitgestellten Muster aufbereitet. Die Orientierungsdaten aus dem bisher bei der GPA NRW vorhanden interkommunalen Vergleich wurden dem Rechnungsprüfungsamt zur Verfügung gestellt. Danach ergibt sich folgendes Bild zum Ressourceneinsatz für die Informationstechnik:

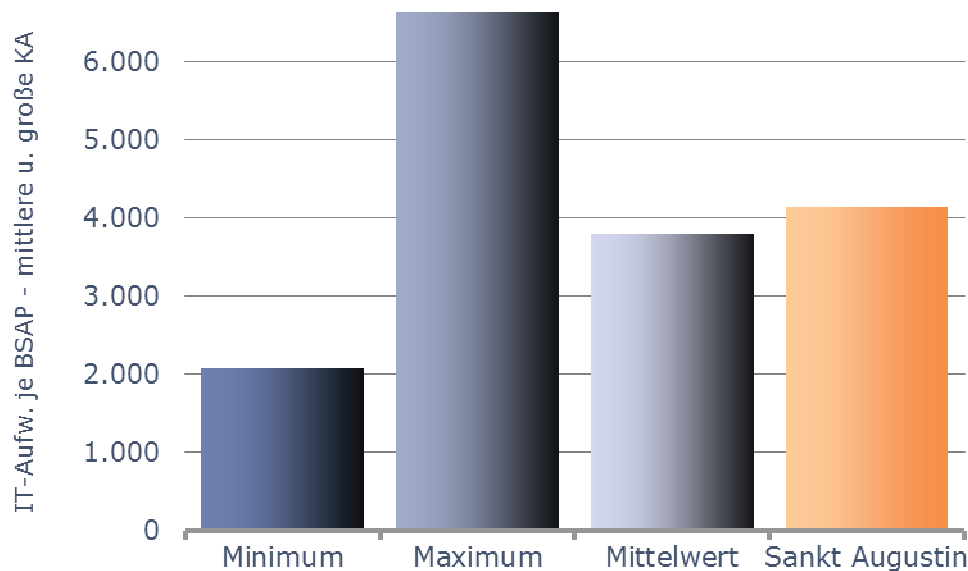
Kennzahl IT- Aufwendungen € je Einwohner

Minimum	12,29
Maximum	40,32
Mittelwert	22,97
Sankt Augustin	28,66



Kennzahl IT- Aufwendungen € je Bildschirmarbeitsplatz

Minimum	2.196
Maximum	6.630
Mittelwert	3.899
Sankt Augustin	4.151



Bei beiden erhobenen Kennzahlen zeigt der Vergleich zu anderen Kommunen eine Positionierung, die etwas oberhalb des Mittelwertes liegt. Auf Empfehlung der GPA NRW sollten die auf dem Vergleichsjahr 2010 basierenden Zahlen für die Haushaltsjahre bis 2012 fortgeschrieben werden, um auch ein Gesamtbild der Entwicklung des Ressourceneinsatzes unter Berücksichtigung der aktuellen Personalsituation aufzeigen zu können. Im Rahmen der Fortschreibung werden wir zukünftig eine Aufschlüsselung der einzelnen Haushaltspositionen vornehmen (z.B. Unterhaltungsaufwand) und dabei die wichtigsten Kostentreiber herausarbeiten. Ziel wird hier mittelfristig sein, mögliche Konsolidierungspotentiale aufzuzeigen.

Sankt Augustin, den 14.11.2012

Peter Fey

Rechnungsprüfungsamtsleiter

Evaluation des IKS bei der Stadt Sankt
Augustin

Betrachtung der IT- Risikofelder in aus-
gewählten Bereichen

IT- Sicherheitsbetrachtung
Sankt Augustin

Inhaltsverzeichnis

Inhaltsverzeichnis	1
IT-Sicherheit	2
Allgemeine Sicherheitsanforderungen	3
Unterlagen und Ansprechpartner	5
Fragenkreis „IT-Räume und Infrastrukturaufbau“	6
Fragenkreis „Technische Ausstattung der Arbeitsplätze/ Client-Umgebung“	10
Fragenkreis „IT-Management“	11
Fragenkreis „Backup und Archivierung“	19
Interkommunale Standortbestimmung	19
Erfüllungsgrad der IT-Sicherheit im interkommunalen Vergleich	19
Gesamtfazit	21
Empfehlungen für die weitere Vorgehensweise	21

IT-Sicherheit

Das Beratungsmodul 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 der Beratung 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 Stadt Sankt Augustin eingeführt und umgesetzt wurde, eine große Rolle.

Die Betrachtung wird überwiegend unter Verwendung von Checklisten durchgeführt. Diese Checklisten wurden anhand anerkannter Kriterien des BSI¹ erarbeitet und sind in unterschiedliche Fragenkreise aufgeteilt.

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

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

in den Blick genommen.

Die Betrachtung erfolgt im Dialog mit den Verantwortlichen für die IT-Organisationseinheiten sowie dem örtlichen RPA.

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

¹ Bundesamt für Sicherheit in der Informationstechnik

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, GoB, GoDV

Die Betrachtung der Sicherheitsanforderung durch die GPA NRW 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 betrachtete 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 Betrachtung 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 Betrachtungsumfanges ist jedoch nicht vorgesehen, die Ergebnisse der Interviews systematisch zu überprüfen; dies kann nur in Einzelfällen als Stichprobe erfolgen.

Dort wo die Sicherheitsbetrachtung zu Empfehlungen oder führt, sind nachfolgend entsprechende Ausführungen enthalten.

Unterlagen und Ansprechpartner

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

- Allgemeine Geschäftsweisung der Stadt Sankt Augustin (AGA), in der Fassung vom 03.12.2007
- Dienstanweisung über die Internetnutzung und den E-Mail- Verkehr, in der Fassung vom 29.05.2007
- Dienstanweisung über den Datenschutz und die Datensicherheit, in der Fassung vom 23.01.2007
- Dienstanweisung über die Einführung eines Dokumenten- und Workflowmanagementsystems, in der Fassung vom 14.11.2011
- Dienstvereinbarung über den Einsatz und die Nutzung einer Helpdesk- Software, in der Fassung vom 01.10.2003
- Organisationsverfügung „Einführung neuer ADV- Programme“
- Organisationsverfügung „Passwortschutz“
- Organisationsverfügung „Planung und Einführung von DV- Verfahren“
- Organisationsverfügung „Verfahrensweise bei der Abwicklung von Beschaffungsverfahren,...“

Als Ansprechpartner stand uns die Teamverantwortliche für den Bereich der Informationstechnologie zur Verfügung.

Fragenkreis „IT-Räume und Infrastrukturaufbau“

Zu diesem Fragenkreis haben wir folgende Teilbereiche betrachtet:

IT- Technik- Räume, IT-Verkabelung, WLAN², Sicherheitgateway (Firewall).

Grundsätzlich sollte die Konzeption eines Serverraums einen abgeschlossenen Sicherheitsbereich vorsehen. Er sollte möglichst gut zu sichernde Zugangstüren haben, die vor Gefährdungen durch Umgebungseinflüsse, insbesondere aber gegen Feuer und Einbruch schützen.

Auch die Alarmsicherung des IT-Bereichs und der Serverraumtüren stellt für den Fall eines Einbruchs nur eine sekundäre Präventionsmaßnahme dar. Allein eine bautechnische Härtung der Serverraumzugänge trägt dazu bei, Schäden durch Diebstahl und Vandalismus so weit wie möglich vorzubeugen.

Der zentrale Serverraum der Stadt Sankt Augustin befindet sich im Untergeschoss des Rathauses, unmittelbar am Zugang zu dem Parkbereich. Die Serverraumtür ist durch einen Zugangsschutz mit Einbruchssicherung geschützt. Die Serverraumtür ist massiv ausgestaltet und mit einem Anschluss an eine Einbruchsmeldeanlage versehen. Offensichtliche Mängel waren zum Zeitpunkt der Begehung nicht erkennbar

Der Serverraum bietet ein ausreichendes Platzangebot, um die Infrastruktur angemessen unterzubringen und behinderungsfrei bedienen zu können.

Die Raumtemperatur war dem technischen Umfeld entsprechend angemessen. Anzeichen einer überhöhten Raumtemperatur waren nicht erkennbar.

Die Infrastrukturmerkmale zeigen eine gut konzipierte, leistungsfähige und moderne, zukunftsorientierte Konzeption auf, die eine gute Grundlage für eine effiziente und effektive Leistungserbringung durch die örtliche IT möglich machen kann. Die mit dem Serverbetrieb verbundenen Risiken sind insgesamt durch die getroffenen Sicherheitsmaßnahmen auf ein akzeptables und handhabbares Mindestmaß reduziert.

² Wide Local Area Network

Neben den Serverräumen gehören jedoch auch die Verteilerräume, die insgesamt mit den Serverräumen als IT- Technikräume bezeichnet werden, zu den Räumlichkeiten, die Sicherheitsanforderungen zu erfüllen haben und insoweit auch als Gesamtheit zu betrachten sind. Grundsätzlich reicht es daher nicht aus, nur die Serverräume in einen guten Zustand zu versetzen, sondern hier gilt vielmehr das Prinzip des „schwächsten Gliedes“.

Die im Rahmen der Prüfung identifizierten Sachverhalte führen zu folgenden Empfehlungen.

Verteilerraum 5. OG

Vorbeugender Brandschutz

Bei der Begehung des Verteilerraumes im 5 Obergeschoss des Rathauses war festzustellen, dass der Raum nicht an das Brandmeldesystem des Hauses angeschlossen ist. Die nächstgelegenen Brandmelder befinden sich im Flurbereich vor dem Verteilerraum und können eine Alarmmeldung erst dann auslösen, wenn eine Brandausweitung im Verteilerraum schon weit fortgeschritten ist. Die Zugangstür zum Verteilerraum verfügt über keine Brandschutz-Zertifizierungszeichen, so dass hier möglicherweise eine Schwachstelle hinsichtlich der Feuerhemmung und Verhinderung der Brandausweitung gegeben sein kann. Im Raum selbst befinden sich zusätzliche vermeidbare Brandlasten.

Empfehlung

Um den sicheren Betrieb unter Gesichtspunkten des Brandschutzes zu gewährleisten, sollten in den Räumlichkeiten der technischen Infrastruktur Brandlasten möglichst vermieden werden. Bezüglich der weitergehenden Brandschutzmaßnahmen empfehlen wir eine Kontaktaufnahme mit dem Gebäudemanagement und der örtlichen Feuerwehr.

IT-Verkabelung

Redundanzen in der Gebäudeverkabelung

Die Überlegungen zur Planung der Gebäudeverkabelung verfolgt in der Regel neben Leitungsdurchsatz und Integrität auch das Schutzziel der Verfügbarkeit. Wenn die Anforderungen der Fachbereiche so weit gehen, dass auch bei umfassenderen Vorfällen die Anbindung und die Netzinfrastruktur des Gebäudes nutzbar bleiben muss, so sollte dies durch eine durchdachte redundante Trassenführung angestrebt werden.

Empfehlung

Die Stadt Sankt Augustin sollte über eine Verfügbarkeitsanalyse prüfen, inwieweit die Gebäudeverkabelung redundant auszulegen ist.

Die IT-Verkabelung umfasst alle Kommunikationskabel, die in eigener Regie betrieben werden. Sie ist somit die physikalische Grundlage der internen Kommunikationsnetze. Die IT-Verkabelung reicht von Übergabepunkten aus einem Fremdnetz (z. B. ISDN-Anschluss eines TK-Anbieters, DSL-Anbindung eines Internet-Providers) bis zu den Anschlusspunkten der Büroarbeitsplätze

Die IT-Verkabelung als Teil der technischen Infrastruktur von Gebäuden und Liegenschaften wird nach der gängigen Betrachtungs- und Vorgehensweise der strukturierten Verkabelung in Primär-, Sekundär- und Tertiärbereich unterschieden.

Mit Primärbereich wird der Bereich der Kabelführung, der Gebäude miteinander verbindet, bezeichnet. Der Primärbereich überbrückt große Entfernungen mit hohen Übertragungsraten zwischen wenigen Anschlusspunkten.

Mit Sekundärbereich wird die Verkabelung zwischen dem Gebäudeverteiler und Verteilern der Etagen oder Gebäudebereichen bezeichnet. Diese Verkabelung ist in vielen größeren Gebäuden anzutreffen.

Die Tertiärverkabelung ist die Anbindung der Endgeräte an einen zentralen Verteilpunkt (z. B. in der Etage).

Bei hohen Verfügbarkeitsanforderungen sollte überlegt werden, in den relevanten Gebäuden die Verkabelung redundant auszulegen. Dazu wird die Sekundärverkabelung, also die Verbindung der Etagen, über mindestens zwei Steigschächte geführt, die sich in verschiedenen Brandabschnitten des Gebäudes befinden sollten. Beispielsweise könnte die Sekundärverkabelung an den gegenüberliegenden Gebäudeseiten (z. B. Nord und Süd oder Ost und West) geführt werden.

Alle Räume, in denen Teilnehmer zu versorgen sind, werden dann jeweils an beide Sekundärverkabelungen angeschlossen. Die Hälfte der Anschlüsse in einem Raum wird mit einem Verteiler auf der einen Gebäudeseite verbunden, die andere Hälfte der Anschlüsse wird an einen Verteiler auf der anderen Seite des Gebäudes angeschlossen.

Damit ist es auch bei einem gravierenden Schaden möglich, den Betrieb auf den Etagen mindestens behelfsweise aufrecht zu erhalten, sofern der Schaden nicht beide Gebäudehälften betrifft.

Da die Schaffung einer redundanten Verkabelung mit Kosten verbunden ist, sollte hier ein Abwägungsprozess stattfinden, der letztlich die Notwendigkeit einer entsprechenden Verfügbarkeit der Bildschirmarbeitsplätze aufgabenkritisch beleuchtet. Dieser Abwägungsprozess ist letzter Konsequenz auch ein wesentlicher Bestandteil des Notfallvorsorgekonzeptes, in dem ganz grundsätzlich die gewünschte und als notwendig erachtete Ausfallsicherheit der DV- Systeme und DV- Verfahren festzustellen ist.

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 Betrachtung sind 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 alle Behörden von existenzieller Bedeutung. Dabei können Informationen entweder auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Für den Schutz der Informationen reicht es nicht aus, nur technische Sicherheitslösungen einzusetzen.

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

Im Rahmen der sicherheitstechnischen Betrachtung war positiv festzustellen, dass bei der Stadt Sankt Augustin ein sehr hohes und auch nachahmenswertes Sicherheitsbewusstsein vorhanden ist und hier in der Vergangenheit bereits zahlreiche Prozesse in Gang gesetzt wurden, für die man in anderen vergleichbarem Kommunen erst intensiv werben muss. So ist hier beispielsweise auch die Funktionsstelle eines IT-Sicherheitsbeauftragten eingerichtet worden, was in der interkommunalen Betrachtung derzeit leider noch selten ist, wenngleich die Tendenzen sich hier positiv darstellen. Zu Zeitpunkt der Sicherheitsbetrachtung, die im Zusammenhang mit der Einführung des internen Kontrollsystems durchgeführt wurde, war die Stelle des Sicherheitsbeauftragten IT allerdings unbesetzt, und soll nach Aussagen der Verwaltung auch künftig nicht mehr nachbesetzt werden.

Darüber hinaus ist positiv anzumerken, dass zahlreiche Sicherheitsaspekte in den vorgelegten Dienstanweisungen enthalten sind, die auch

klar die bewusste Gesamtverantwortung für die Informationssicherheit durch die Leitungsebene erkennen lässt.

Leitlinie

Nach Aussage der Verwaltung ist derzeit die Erstellung einer Leitlinie zur Informationssicherheit in Planung. Hierbei sollten in dem anstehenden Prozess die nachfolgenden Aspekte lt. BSI- Empfehlungen berücksichtigt werden.

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 Mitarbeiterinnen und 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.

Empfehlung

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

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.

Sankt Augustin hatte in der Vergangenheit bereits eine entsprechende Funktionsstelle eingerichtet, die aber künftig entfallen soll. Dies ist jedoch auch Sicherheitsaspekten ein Rückschritt aus einer bis dahin vorbildhaften Struktur.

Empfehlung

Wir empfehlen grundsätzlich, die Nachbesetzung der Stelle eines IT-Sicherheitsbeauftragten zu prüfen.

Die Aufgaben des IT-Sicherheitsbeauftragten sind unter anderem:

- den IT-Sicherheitsprozess zu steuern und zu koordinieren,
- die Erstellung von IT-System-Sicherheitsrichtlinien zu initiieren und zu koordinieren,
- die Erstellung des IT-Sicherheitskonzeptes, des Notfallvorsorgekonzeptes und anderer Teilkonzepte zu koordinieren,
- den Realisierungsplan für die IT-Sicherheitsmaßnahmen zu erstellen und deren Realisierung zu initiieren und zu überprüfen,

- der Leitungsebene zu berichten und bei Entscheidungen zu Sicherheitsaspekten aus der Sicht eines „unabhängigen Dritten“ zu beraten,
- sicherheitsrelevante Projekte zu koordinieren und den Informationsfluss zwischen Bereichs-IT, IT-Projekt- sowie IT-System-Sicherheitsbeauftragten sicherzustellen,
- sicherheitsrelevante Zwischenfälle zu untersuchen sowie
- Sensibilisierungs- und Schulungsmaßnahmen zur IT-Sicherheit zu initiieren und zu steuern.

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

Die Funktion des IT-Sicherheitsbeauftragten kann von einer qualifizierten Mitarbeiterin oder einem qualifizierten Mitarbeiter neben anderen Aufgaben wahrgenommen werden. Maßgeblich ist, dass dem IT-Sicherheitsbeauftragten ausreichend Zeit zur sachgerechten Erfüllung seiner Aufgaben zugewilligt wird. Vor allem bei der erstmaligen Einrichtung des IT-Sicherheitsprozesses müssen hierfür auch hinreichende zeitliche Ressourcen eingeplant werden.

Um Interessenkollisionen zu vermeiden, sollte eine kontrollierende Instanz mit einer solchen Aufgabe nicht dem IT-Bereich angehören.

Sofern eine Nachbesetzung der Stelle des Sicherheitsbeauftragten nicht möglich sein sollte, bieten sich auch Alternativen an, die im Rahmen der überörtlichen Prüfung bekannt wurden und als „funktional“ eingestuft werden können.

So wäre es auch denkbar, eine Arbeitsgruppe „IT- Sicherheit“ einzurichten, die hier die wesentlichen Kontrollaufgaben und Berichtsaufgaben eines Sicherheitsbeauftragten übernimmt. Die personelle Zusammensetzung dieser Arbeitsgruppe könnte dabei beispielsweise sein: jeweils ein Mitglied der IT, der Fachbereichsleitung, des Steuerungsdienstes /Organisation, des RPA sowie des Datenschutzbeauftragten. Ggf. könnte auch ein externer Berater hinzugezogen werden.

Eine andere Alternative stellt die unmittelbare Koppelung der Aufgaben eines Sicherheitsbeauftragten an die Funktion des Datenschutzbeauftragten dar. Dieses Modell ist in der Praxis häufiger zu finden und auch sachlich nachvollziehbar, da der Betrachtungsbereich des Datenschutzbeauftragten sich in zahlreichen Bereichen mit denen des Sicherheitsbeauftragten deckt.

Im Ergebnis lässt sich somit für Sankt Augustin ein 3- Varianten- Modell darstellen, wobei die Variante 1 eine optimale Ausgangslage bietet, die Variante 2 eine befriedigende Alternative darstellt und die Variante 3 als Minimallösung bewertet wird.

Variante 1	Stelle des Sicherheitsbeauftragten wiederbesetzen
Variante 2	Funktion des Sicherheitsbeauftragten an die Stelle des Datenschutzbeauftragten koppeln
Variante 3	Einrichten einer Arbeitsgruppe „IT-Sicherheit“

Unabhängig davon, welche Variante hier bevorzugt wird, ist die künftige Einbindung des RPA als obligatorisch zu betrachten, das hier wesentliche und unbedingt notwendige Informationen für die nachfolgende Fortführung und Weiterentwicklung des Internen Kontroll- Systems (IKS) zu erzielen sind.

Management-Berichte zur IT-Sicherheit

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

Empfehlung

Da beim der Stadt Sankt Augustin derzeit die Stelle des IT-Sicherheitsbeauftragten unbesetzt ist, sollten übergangsweise die Berichte zur IT-Sicherheit von der IT erstellt werden, um der Verwaltungsleitung alle Informationen für eine Risikobewertung transparent zu machen und eine Basis für notwendige Entscheidungen zu liefern.

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

Ein Management-Bericht 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.

Schulungen zu IT-Sicherheitsmaßnahmen

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

Empfehlung

Für das IT-Personal sollten regelmäßig Schulungen zum Thema IT-Sicherheit erfolgen, um zusätzliche Kompetenzen zu grund-

sätzlichen Risiken und aktuellen Gefährdungslagen aufzubauen, die zur Schulung der Mitarbeiter herangezogen werden können.

Notfallvorsorge

Auch im Bereich der Notfallvorsorge ist die Stadt Sankt Augustin gut aufgestellt, wenngleich ein ausdrückliches Notfallhandbuch noch nicht vorhanden ist. Dies ist jedoch insoweit nicht schwerwiegend, als hier zahlreiche Festlegungen getroffen und Maßnahmen durchgeführt wurden, die üblicherweise inhaltlich einem Notfallhandbuch zuzuordnen wären, z.B. Erstellung von Wiederanlaufplänen, Alarmierung, Datensicherungsplan für Notfälle, etc.

Fragenkreis „Backup und Archivierung“

Bei der Stadt Sankt Augustin besteht eine mustergültige Backup- Strategie, die methodisch auf einer umfangreichen und sehr gut beschriebenen Konzeption aufbaut und technisch nach Best- Practice – Ansätzen umgesetzt ist. Kernstück der Backup- Strategie ist hier eine Datensicherung auf Datenblock- Basis, die eine sehr schnelle, effiziente und effektive Sicherung der Datenbestände ermöglicht.

Im Rahmen der Betrachtung sind keine Sachverhalte identifiziert worden, die zu einer Empfehlung führen.

Interkommunale Standortbestimmung

Im Rahmen der überörtlichen Prüfung der IT- Sicherheit ermittelt die GPA NRW einen Erfüllungsgrad IT- Sicherheit, der die umgesetzten Organisatorischen und technischen Maßnahmen in der IT berücksichtigt, die geeignet sind, um die mit dem Betrieb der IT- Technik verbundenen Risiken auf ein beherrschbares und angemessenes Maß zu reduzieren.

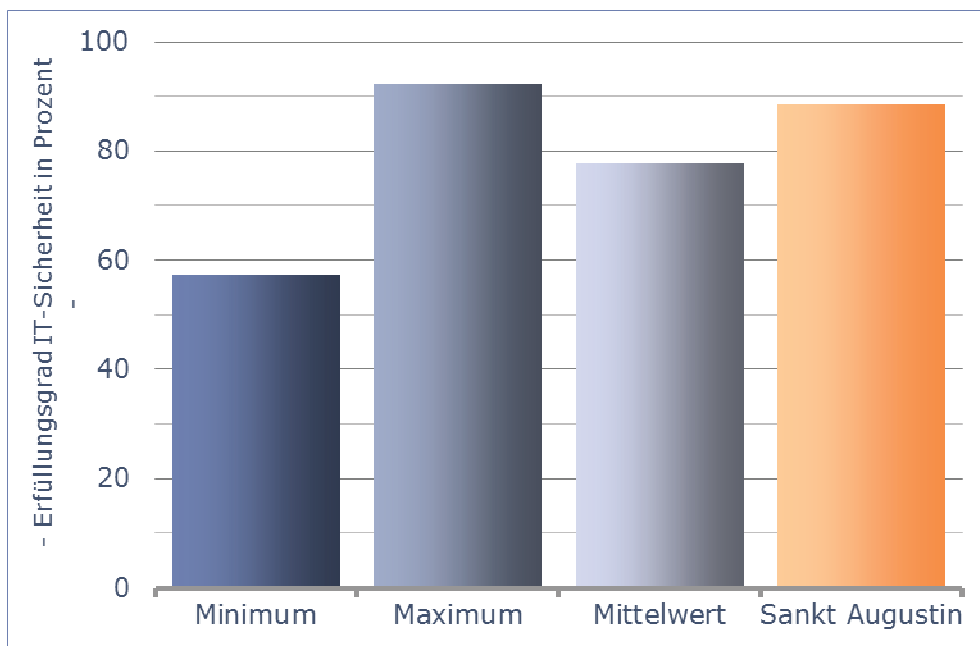
Im Rahmen der Einführung des Internen Kontrollsystems wurde vereinbart, dass das Ergebnis der oben geführten Betrachtung in den vorhandenen interkommunalen Vergleich mit einbezogen wird, um eine Standortbestimmung zu erhalten.

Erfüllungsgrad der IT-Sicherheit im interkommunalen Vergleich

Mit den umgesetzten Maßnahmen zur IT-Sicherheit nimmt die Stadt Sankt Augustin im Vergleich eine Position unter den zehn Besten des Vergleichsrings der großen, kreisangehörigen Kommunen ein. Der mit dieser Prüfung festgestellte Gesamterfüllungsgrad beträgt rund 89 Prozent und liegt damit deutlich über dem Wert von 80 Prozent, der nach unserer Empfehlung als Voraussetzung für einen sicheren und ordnungsgemäßen IT-Betrieb mindestens erreicht werden sollte. Der Mit-

telwert für die bisher geprüften Kommunen liegt bei 77,7 Prozent. Der Maximalwert liegt bei 92 Prozent.

Erfüllungsgrad IT- Sicherheit im interkommunalen Vergleich



Erfüllungsgrad IT-Sicherheit gesamt	
Minimum	57,3 %
Maximum	92,1 %
Mittelwert	77,7 %
Sankt Augustin	88,6 %

Das positive Ergebnis der interkommunalen Standortbestimmung bestätigt nachdrücklich das spürbare hohe Sicherheitsbewusstsein der IT-Verantwortlichen und deren hohe Fachkompetenz sowohl in technischer als auch in IT-organisatorischer Sicht.

Gesamtfazit

Neben der Inanspruchnahme von Dienstleistungen der Civitec betreibt die IT der Stadtverwaltung in Sankt Augustin eine eigene IT- Infrastruktur. Die technische und organisatorische Ausgestaltung der örtlichen IT ist im interkommunalen Vergleich überdurchschnittlich gut aufgestellt. Die Sicherheitsstrategie sowie die Datensicherungsstrategie werden dabei hervorgehoben, wenngleich die derzeit bestehende Vakanz in der Stelle des Sicherheitsbeauftragten als Rückschritt einer bis dahin sehr guten Ausgangslage gewertet wird. Generell kann jedoch ein sehr hohes Sicherheitsbewusstsein und eine hohe Fachkompetenz der IT- Verantwortlichen festgestellt werden.

Sicherheitsrisiken, die einen unmittelbaren Handlungsbedarf signalisieren, konnten im Rahmen der Beratung nicht festgestellt werden. Die mit dem IT- Betrieb verbundenen Risikopotentiale sind auf ein beherrschbares Mindestmaß reduziert worden, wenngleich noch Optimierungspotentiale in dem Bereich des vorbeugenden Brandschutzes und beim Sicherheitsgateway beleuchtet werden konnten.

Darüber hinaus sollte geprüft werden, ob eine redundante Ausgestaltung der Gebäudeverkabelung und des Sicherheitsgateways im Rahmen der Notfallvorsorge (Verfügbarkeitsanforderungen) erforderlich sein könnte.

Eine Betrachtung des Ressourceneinsatzes für den Einsatz der Informationstechnologie bei der Stadt Sankt Augustin war nicht Gegenstand des Beratungsauftrages.

Empfehlungen für die weitere Vorgehensweise

Nach Abschluss der Beratung unter Berücksichtigung der vor Ort geführten Gespräche sowie der Auswertung der VERPA-Checklisten erscheint es sinnvoll, durch das RPA folgende Stichpunktprüfungen durchzuführen bzw. folgende Datenbestände in regelmäßigen Abständen auf Plausibilität zu prüfen:

Themenbereich	Geschätzter Zeitaufwand ³
Erfassung aller relevanten Arbeitsschritte zur Aufnahme von rechnungslegungsrelevanten Daten (bisher besteht hier nur eine Übergangsregelung).	1 bis 3 Monate
Überprüfung der Rechtestruktur/Berechtigungen (jährliche Stichprobenprüfung).	<1 Monat, hohe Priorität
Erarbeiten einer IT-Prüfungsplanung und Vorbereitung auf künftige IT-Prüfungen durch Fortbildungen.	<1 Monat
Plausibilitätsprüfungen der IT-Investitions- und Personalbedarfsplanung.	>3 Monate
Aufnahme und Bewertung von bestehenden Abhängigkeiten zu einzelnen IT-Mitarbeitern und Dienstleistern.	<1 Monat
Vergleich Soll-/Ist-Zustand der IT-Stellenbeschreibungen sowie Beurteilung der IT-Tätigkeitsbeschreibungen.	>3 Monate
Aufnahme und Bewertung der Zusammenarbeit zwischen IT und den Fachbereichen (Effizienz/Effektivität).	>3 Monate
Fortlaufende Betrachtung der Einhaltung der Regelungen zur Benutzerverwaltung (Werden die Regelungen zur Vergabe von Nutzerberechtigungen zufriedenstellend umgesetzt – Kooperation mit Datenschutzbeauftragtem).	<1 Monat, jährlicher Aufwand
Aufnahme und Bewertung von der sachgerechten Behandlung von Fehlern und Problemfällen bei	<1 Monat, hohe Priorität

³ Der hier dargestellte Zeitaufwand kann nur eine Tendenz aufzeigen, da die individuellen Bedarfe nur durch eine konkrete Einschätzung des akuten Sachverhaltes bestimmt werden können.

Themenbereich	Geschätzter Zeitaufwand ³
der Datensicherung.	
Beurteilung der Wirksamkeit der Wiederanlaufverfahren.	<1 Monat
Regelmäßige Kontrolle der Software-Versionsstände.	<1 Monat
Regelmäßige Kontrolle der Freigabeverfahren und Testverfahren für Fachverfahren (auch für Updates).	<1 Monat
Kontrolle der Umsetzung der Handlungsempfehlungen der externen Prüfungen mit IT-Bezug.	<1 Monat



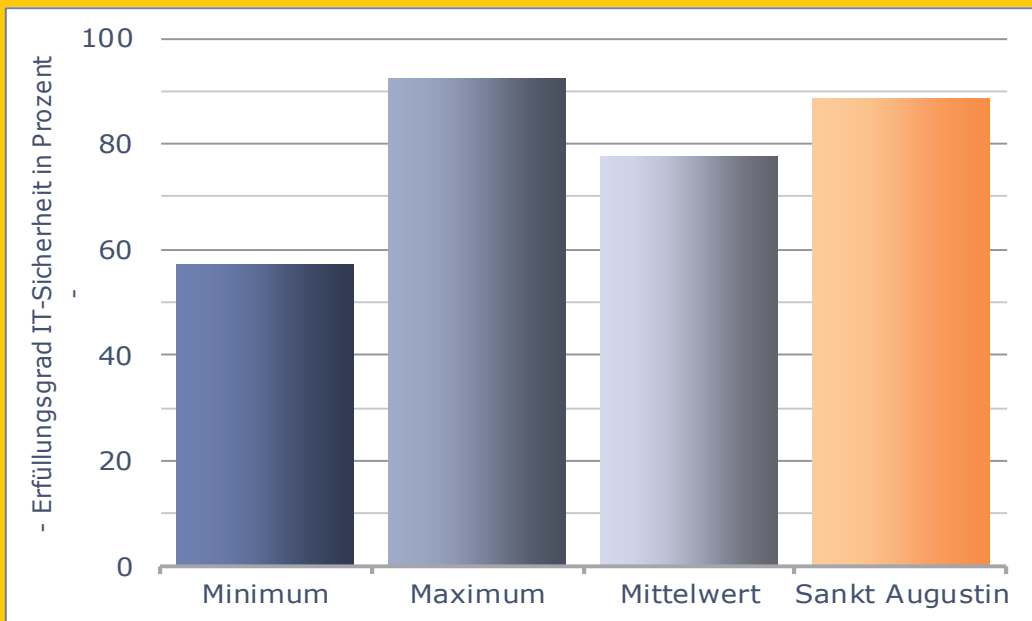
Überörtliche Prüfung Informationstechnologie

- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -

(mittlere und große kreisangehörige Städte, 2009-2012)

Stadt wählen →

Erfüllungsgrad IT-Sicherheit gesamt	
Minimum	57,3 %
Maximum	92,1 %
Mittelwert	77,7 %
Sankt Augustin	88,6 %



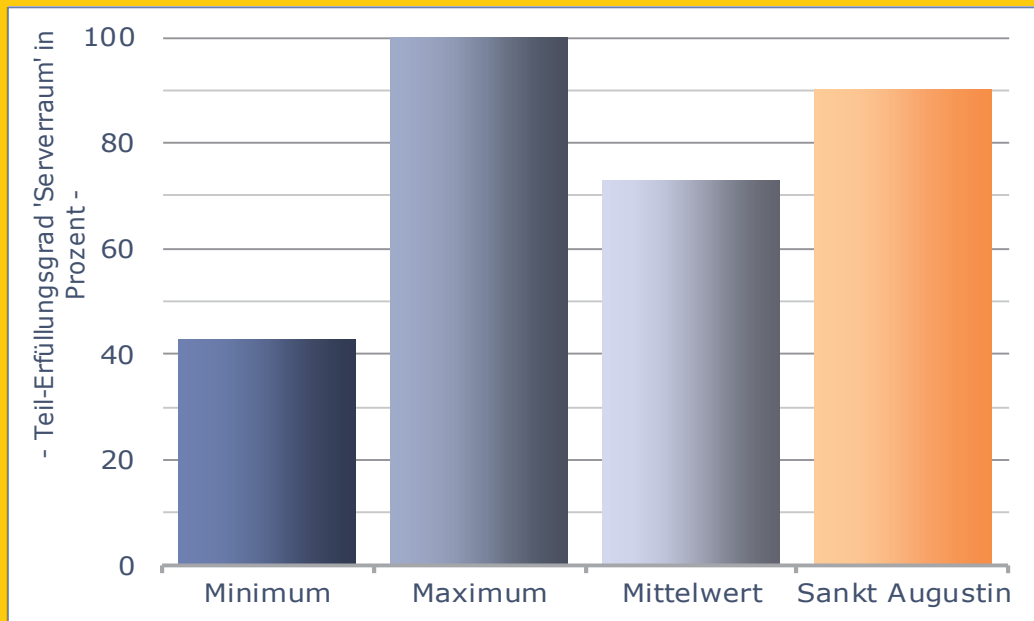


Überörtliche Prüfung Informationstechnologie

- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -

(mittlere und große kreisangehörige Städte, 2009-2012)

Teil-Erfüllungsgrad Serverraum	
Minimum	42,9 %
Maximum	100,0 %
Mittelwert	72,7 %
Sankt Augustin	90,0 %



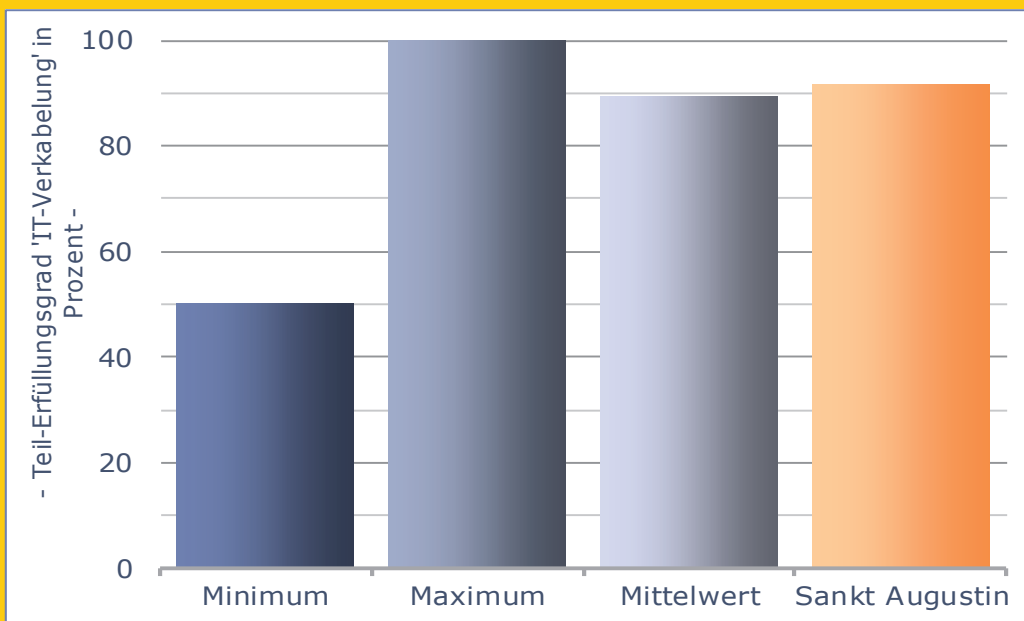


Überörtliche Prüfung Informationstechnologie

- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -

(mittlere und große kreisangehörige Städte, 2009-2012)

Teil-Erfüllungsgrad IT-Verkabelung	
Minimum	50,0 %
Maximum	100,0 %
Mittelwert	89,4 %
Sankt Augustin	91,7 %



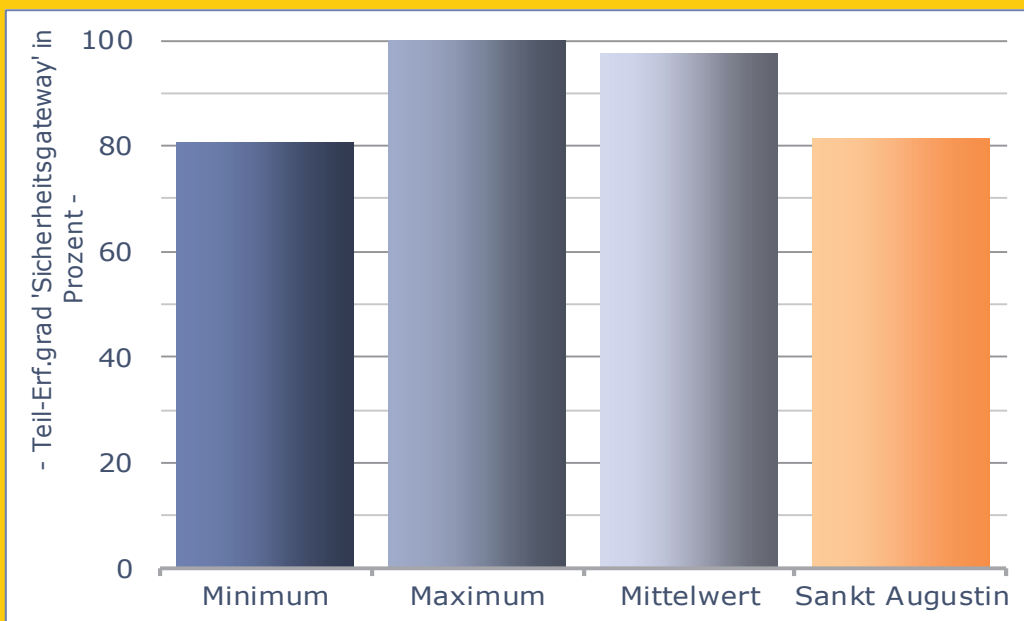


Überörtliche Prüfung Informationstechnologie

- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -

(mittlere und große kreisangehörige Städte, 2009-2012)

Teil-Erfüllungsgrad Sicherheitgateway	
Minimum	80,6 %
Maximum	100,0 %
Mittelwert	97,4 %
Sankt Augustin	81,3 %



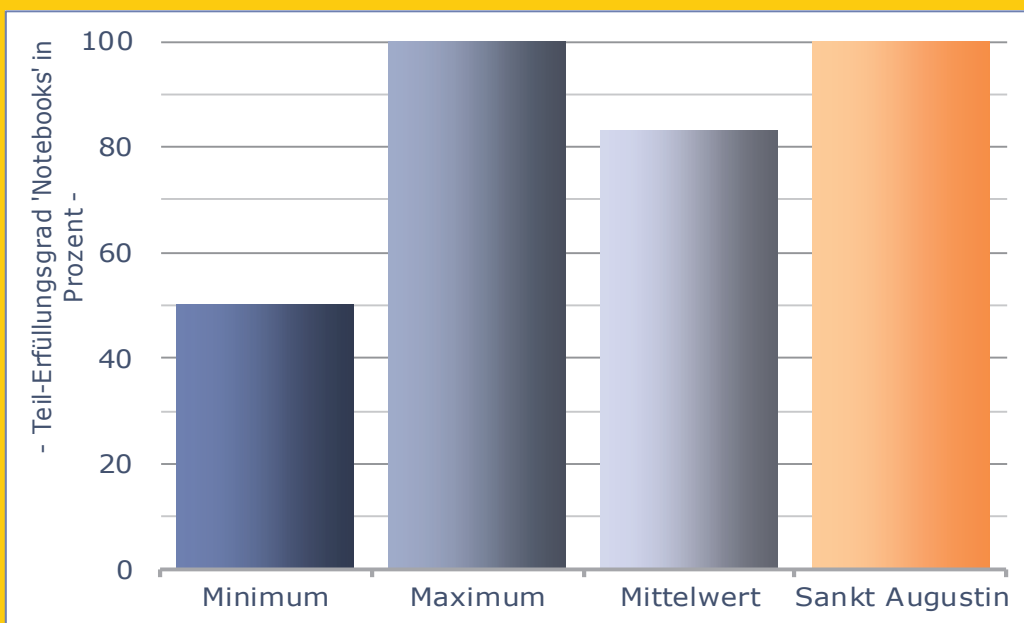


Überörtliche Prüfung Informationstechnologie

- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -

(mittlere und große kreisangehörige Städte, 2009-2012)

Teil-Erfüllungsgrad Notebooks	
Minimum	50,0 %
Maximum	100,0 %
Mittelwert	83,1 %
Sankt Augustin	100,0 %



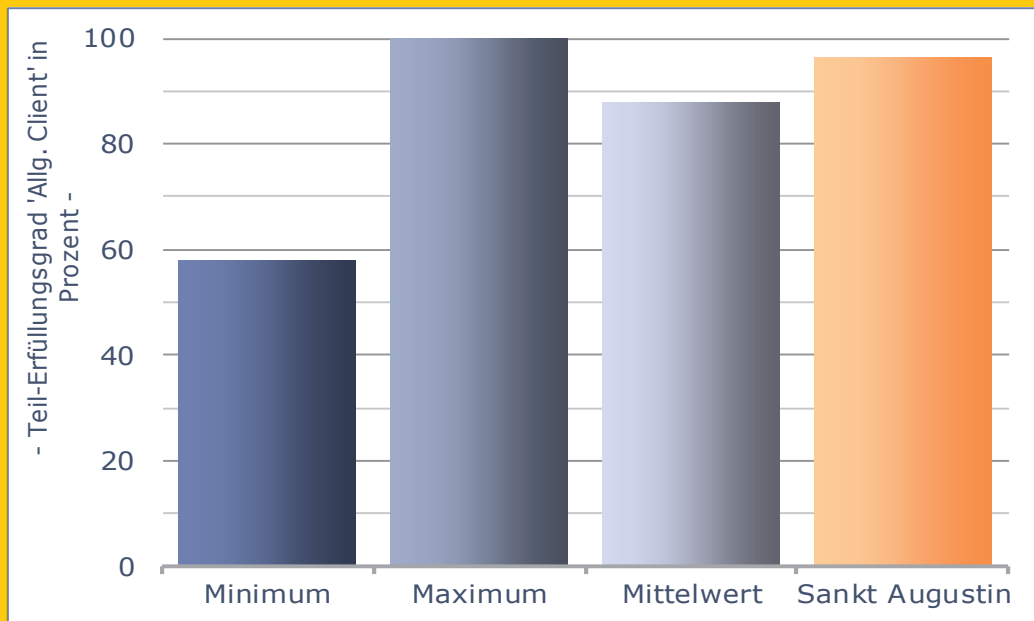


Überörtliche Prüfung Informationstechnologie

- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -

(mittlere und große kreisangehörige Städte, 2009-2012)

Teil-Erfüllungsgrad Allgemeiner Client	
Minimum	57,7 %
Maximum	100,0 %
Mittelwert	87,9 %
Sankt Augustin	96,2 %



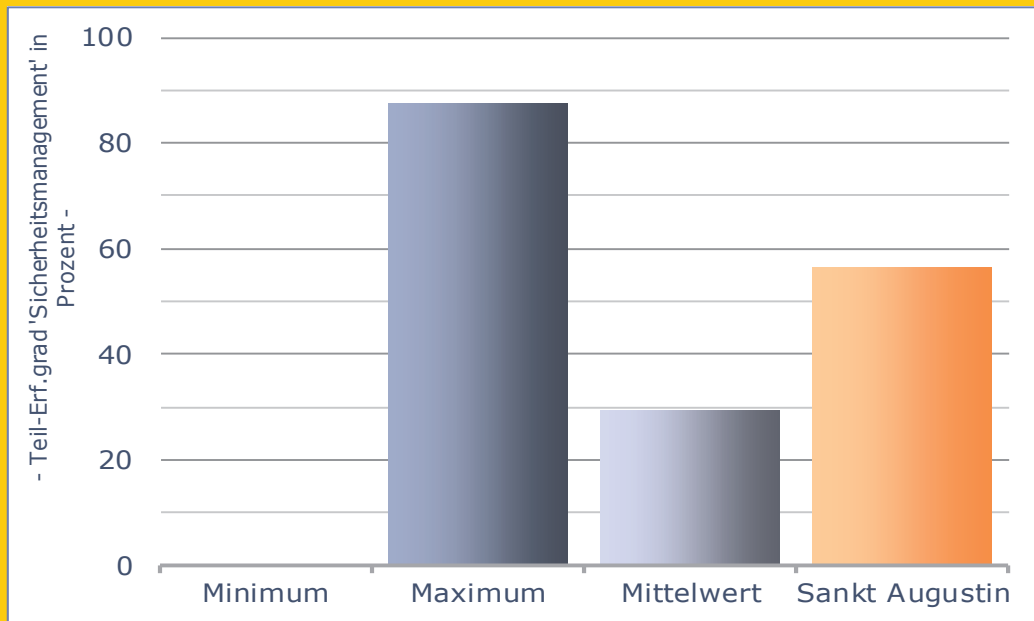


Überörtliche Prüfung Informationstechnologie

- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -

(mittlere und große kreisangehörige Städte, 2009-2012)

Teil-Erfüllungsgrad Sicherheitsmanagement	
Minimum	0,0 %
Maximum	87,5 %
Mittelwert	29,4 %
Sankt Augustin	56,3 %



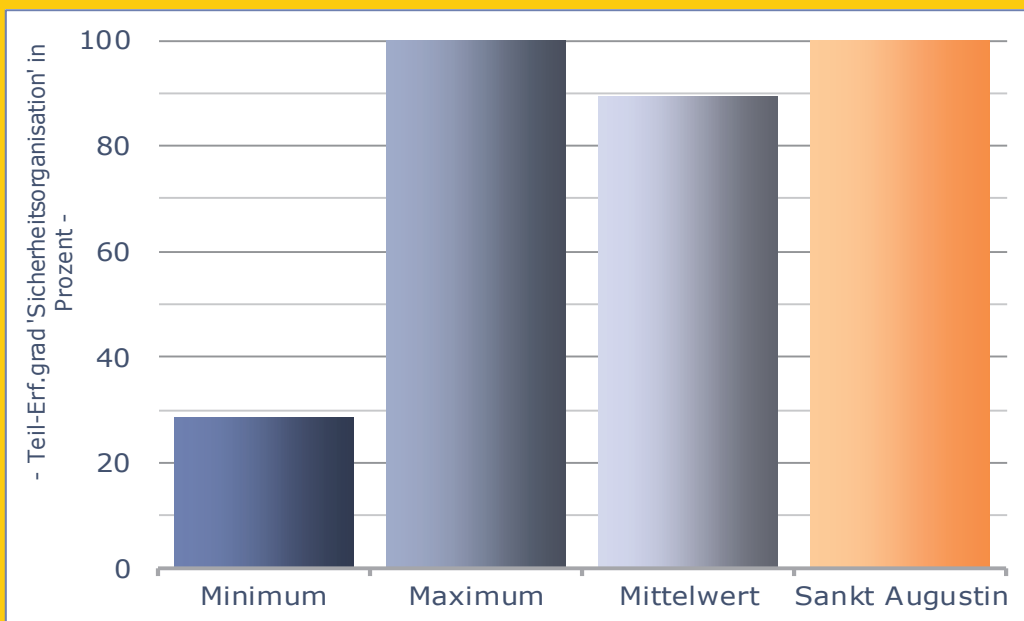


Überörtliche Prüfung Informationstechnologie

- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -

(mittlere und große kreisangehörige Städte, 2009-2012)

Teil-Erfüllungsgrad Sicherheitsorganisation	
Minimum	28,6 %
Maximum	100,0 %
Mittelwert	89,3 %
Sankt Augustin	100,0 %



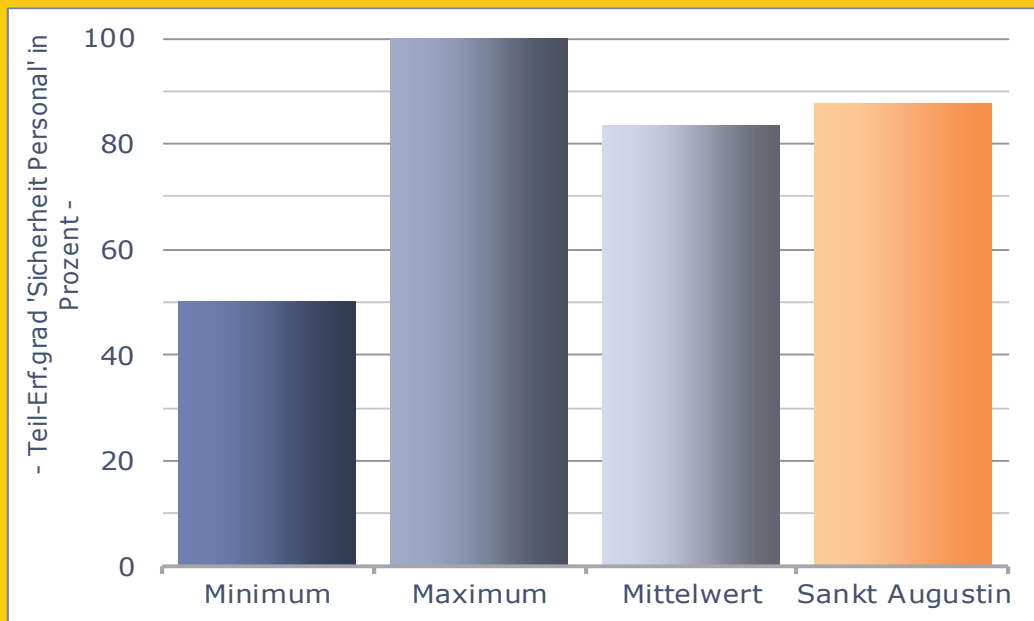


Überörtliche Prüfung Informationstechnologie

- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -

(mittlere und große kreisangehörige Städte, 2009-2012)

Teil-Erfüllungsgrad Sicherheit Personal	
Minimum	50,0 %
Maximum	100,0 %
Mittelwert	83,3 %
Sankt Augustin	87,5 %



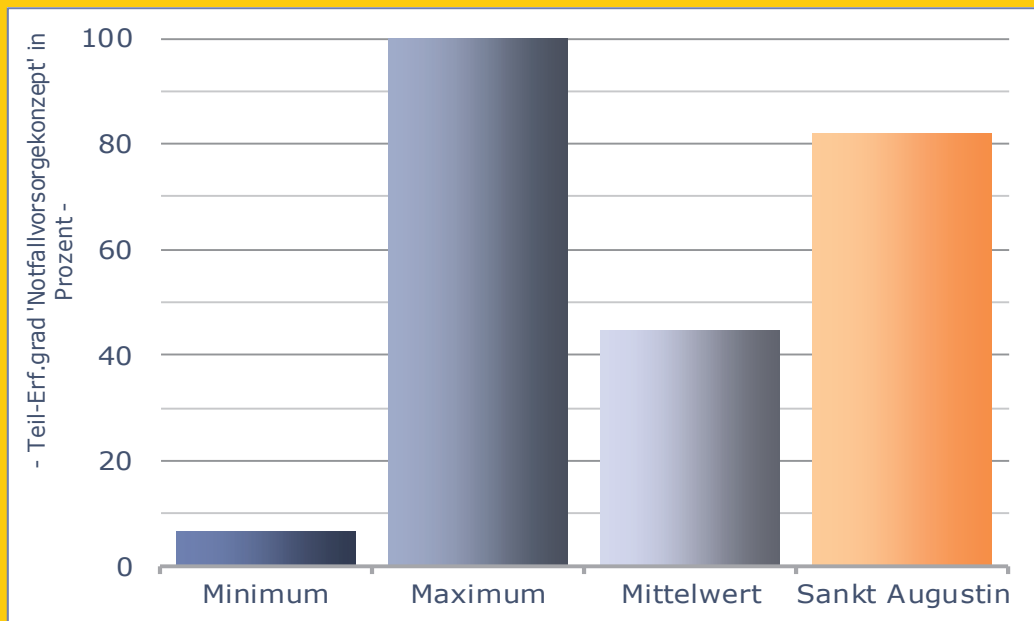


Überörtliche Prüfung Informationstechnologie

- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -

(mittlere und große kreisangehörige Städte, 2009-2012)

Teil-Erfüllungsgrad Notfallvorsorgekonzept	
Minimum	6,7 %
Maximum	100,0 %
Mittelwert	44,7 %
Sankt Augustin	82,1 %





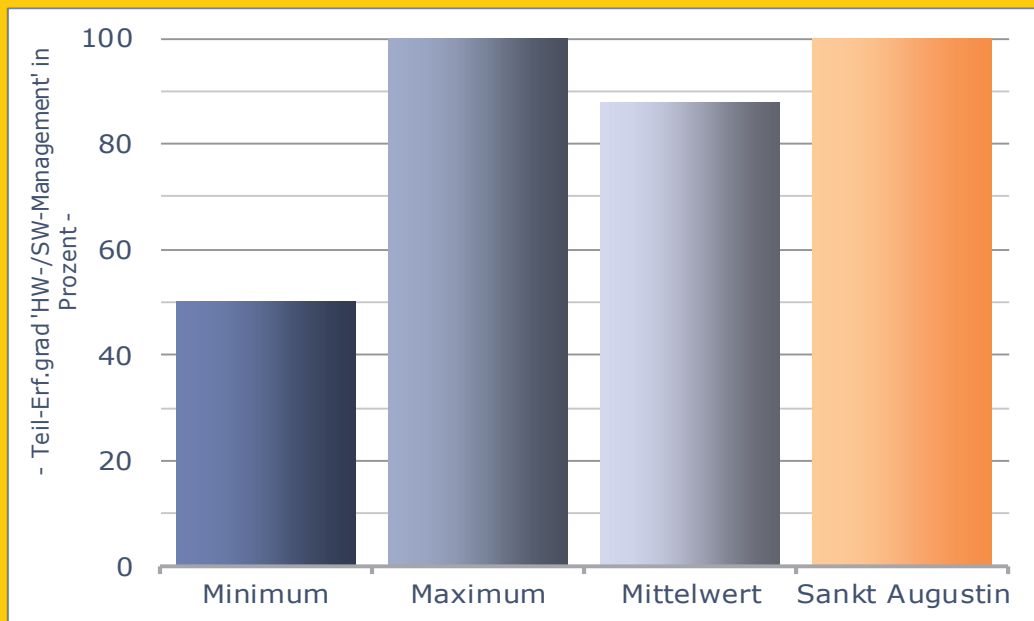
Überörtliche Prüfung Informationstechnologie

- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -

(mittlere und große kreisangehörige Städte, 2009-2012)

Teil-Erfüllungsgrad Hard- und Softwaremanagement

Minimum	50,0 %
Maximum	100,0 %
Mittelwert	88,0 %
Sankt Augustin	100,0 %





Überörtliche Prüfung Informationstechnologie

- Erfüllungsgrade IT-Sicherheit im interkommunalen Vergleich -

(mittlere und große kreisangehörige Städte, 2009-2012)

Teil-Erfüllungsgrad Datensicherung	
Minimum	25,0 %
Maximum	100,0 %
Mittelwert	89,6 %
Sankt Augustin	100,0 %

