**Die Landesbeauftragte
für den Datenschutz und
für das Recht auf Akteneinsicht**

LAND BRANDENBURG
LDA
Schutz der
• Persönlichkeitsrechte
• Informationsfreiheit

Umfrage zu Datenschutz und IT-Sicherheit in der Kommunalverwaltung Brandenburg 2009

1. Zielstellung der Umfrage

Die Landesbeauftragte hat im Zeitraum vom 5. Mai bis 9. Oktober 2009 eine Umfrage zum Thema Datenschutz und IT-Sicherheit in der Kommunalverwaltung des Landes Brandenburg durchgeführt. Deren Ziel war es, den Bedarf an Unterstützung im Bereich des Datenschutzes und der IT-Sicherheit im Flächenland Brandenburg zu ermitteln und daraus Empfehlungen und mögliche Unterstützungsleistungen, z. B. Beratungs- und Schulungsangebote, abzuleiten. Die Ergebnisse der Umfrage sollten von vornherein nicht als Grundlage für zusätzliche Kontrollen und Aufsichtsmaßnahmen genutzt werden. Der Ansatz einer allgemeinen Umfrage zur Erhebung des Ist-Zustandes des Datenschutzes und der IT-Sicherheit ermöglichte einen höheren Informationsgewinn als eine stichprobenartige Prüfung nur einzelner Kommunen.

Die Erhebung enthielt Fragen zum Personaleinsatz hinsichtlich des behördlichen Datenschutz- und des IT-Sicherheitsbeauftragten, zur organisatorischen Umsetzung des Datenschutzes und der IT-Sicherheit, zur Verfahrensbeschreibung und zu technischen Aspekten der IT-Sicherheit, Fragen zur IT-Infrastruktur sowie zu der gewünschten Unterstützung seitens der Landesbeauftragten. Von den 216 befragten Kommunen des Landes Brandenburg haben bis zum Stichtag ca. 80% geantwortet.

2. Ergebnisse der Umfrage

In diesem Kapitel werden die Ergebnisse der Umfrage grafisch aufbereitet dargestellt. Ziel ist es, den Kommunen einen Überblick zu geben, wie sie selbst im Vergleich zu anderen Kommunen im Bereich des Datenschutzes und der IT-Sicherheit aufgestellt sind. Eine inhaltlich vollständige Auswertung soll an dieser Stelle nicht erfolgen. Auf Auffälligkeiten wird in den jeweiligen Abschnitten hingewiesen.

Für die Auswertung wurde eine Klassifizierung der Kommunen vorgenommen. Neben der Gesamtheit der Kommunen werden

- die Landkreise und kreisfreien Städte,
- die Städte, Gemeinde und Ämter mit mehr als 100 Mitarbeitern,
- die Städte, Gemeinde und Ämter mit 20 bis 100 Mitarbeitern und
- die Städte, Gemeinde und Ämter mit weniger als 20 Mitarbeitern

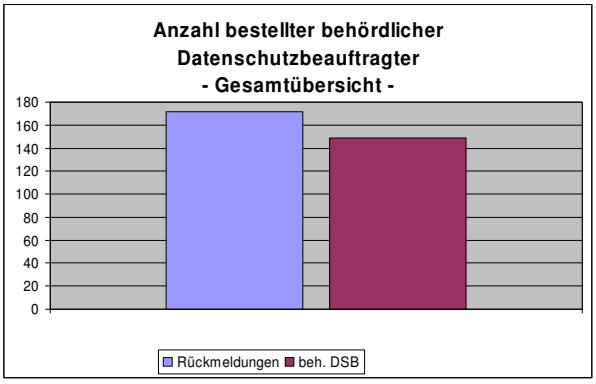
separat betrachtet. Anders wäre ein aussagekräftiges Bild über den Stand und die Umsetzung des Datenschutzes und der IT-Sicherheit nicht zu gewährleisten. Auf Grund der unterschiedlichen Größe der Kommunen und somit auch der unterschiedlichen Ausstattung an Fachpersonal und wohl auch finanzieller Mittel, lassen sich etwaige Mängel erklären.

Bei der Auswertung ist zu berücksichtigen, dass bei einigen Fragen Mehrfachantworten möglich waren.

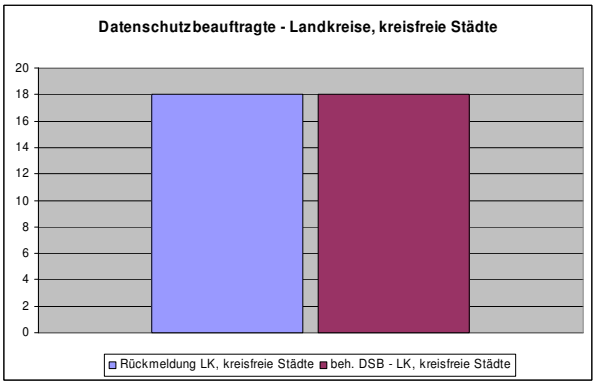
2.1 Personelles

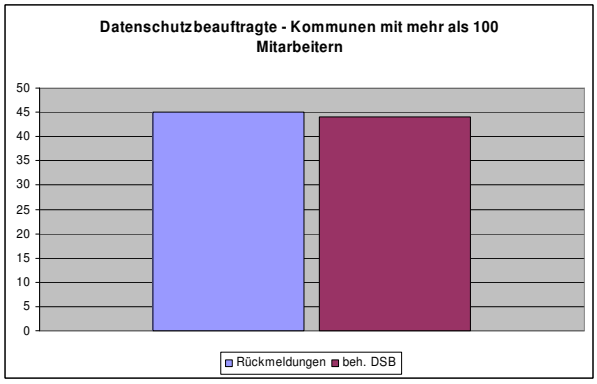
2.1.1 Fragen zum Datenschutzbeauftragten

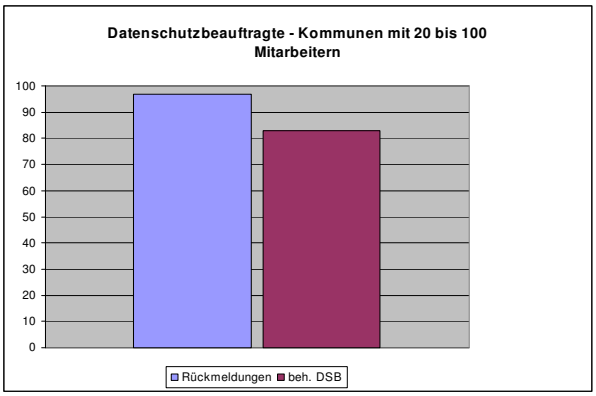
Wurde ein Datenschutzbeauftragter berufen?

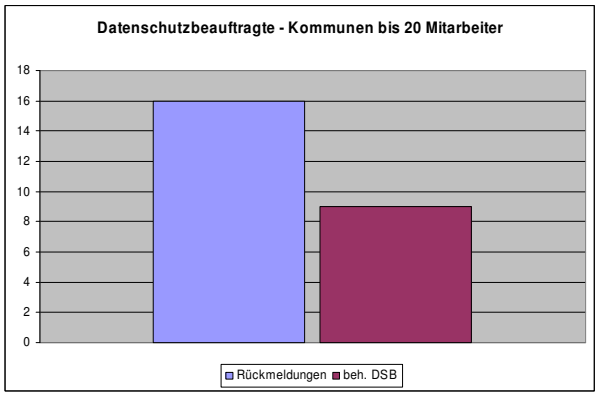


Nach § 7a Abs. 1 BbgDSG haben Daten verarbeitende Stellen einen Datenschutzbeauftragten zu bestellen. Die Auswertung zeigt, dass dies nicht in allen Kommunen des Landes Brandenburg der Fall ist. Insbesondere kleinere Kommunen weisen hier ein Defizit auf.

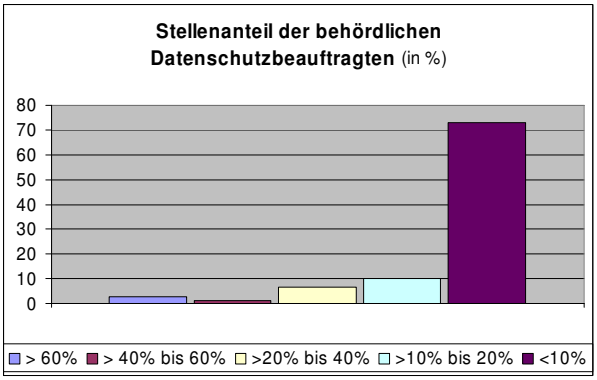




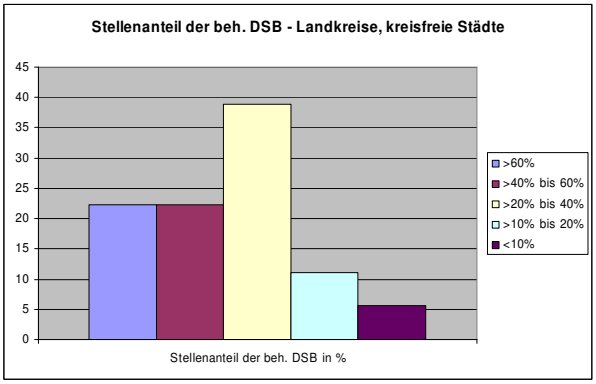


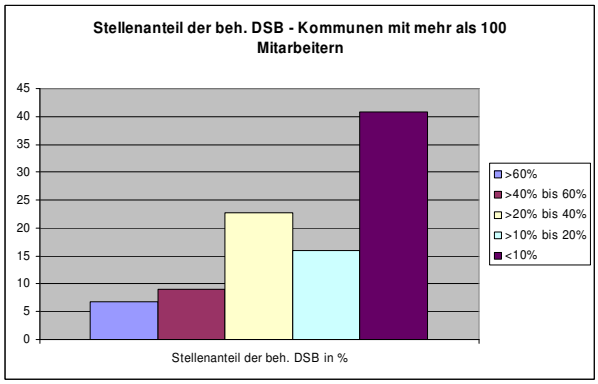


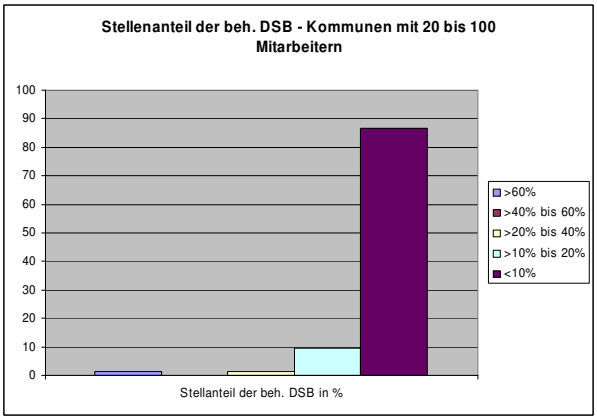
Wie hoch ist der prozentuale Stellenanteil des Datenschutzbeauftragten?

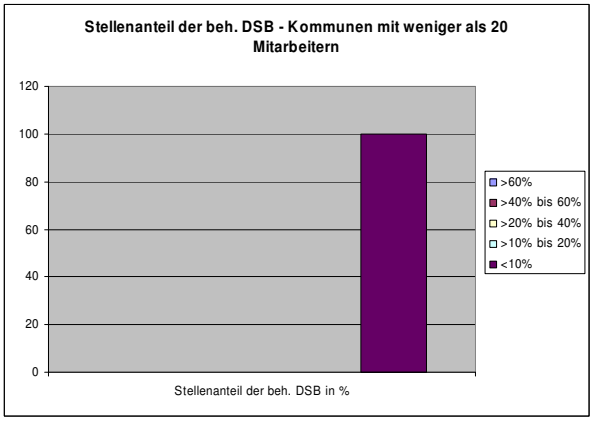


Die Aufgaben eines behördlichen Datenschutzbeauftragten nach § 7a Abs. 5 BbgDSG umfassen ein breites Spektrum. In der überwiegenden Zahl der Kommunen wendet der behördliche Datenschutzbeauftragte weniger als 10% seiner täglichen Arbeitszeit für diese Aufgaben auf. Ob dieser Stellenanteil ausreichend ist, erscheint fraglich.

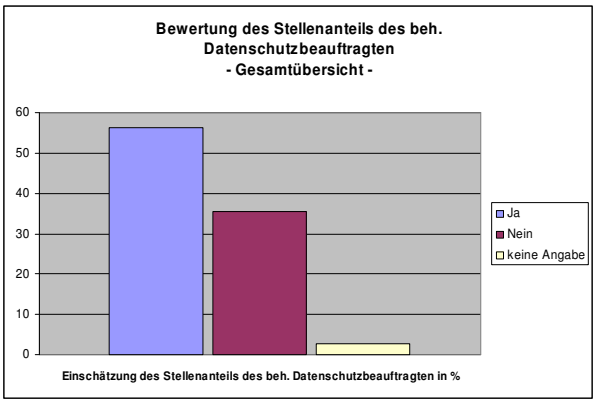




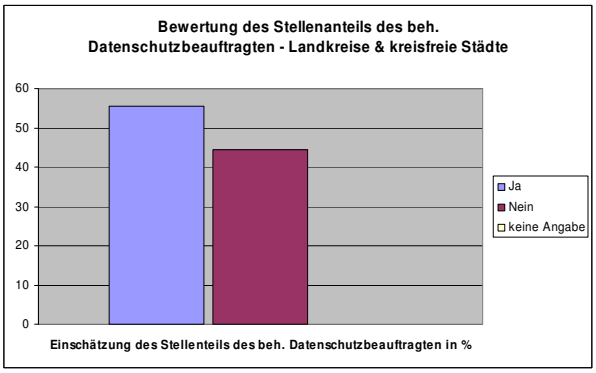


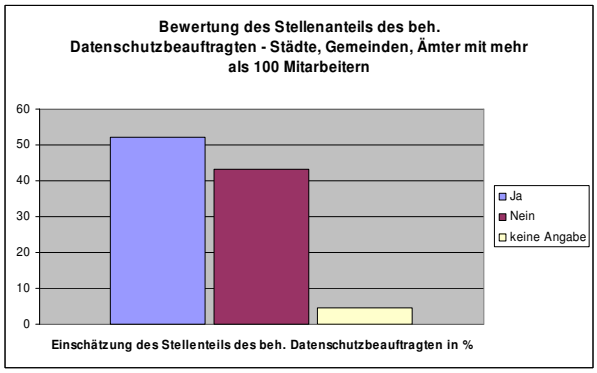


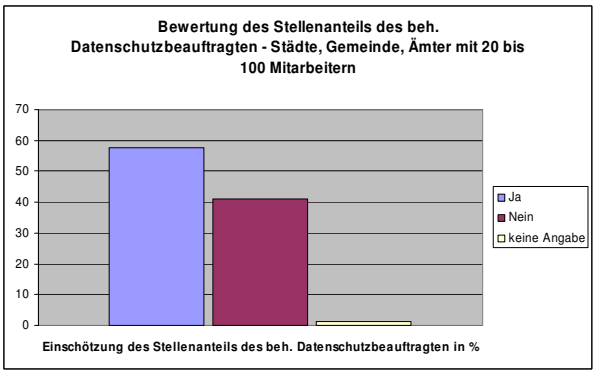
Wird der Stellenanteil als ausreichend betrachtet?

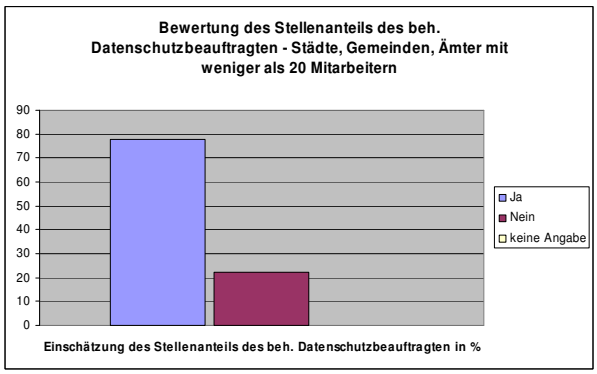


Von der Mehrzahl der Kommunen wird der jeweilige Stellenanteil des behördlichen Datenschutzbeauftragten als angemessen angesehen. Ca. 1/3 hält den Stellenanteil jedoch für unzureichend. Auffällig ist, dass mit steigender Anzahl der Verwaltungsmitarbeiter der Stellenanteil des beh. Datenschutzbeauftragten als nicht ausreichend angesehen wird.

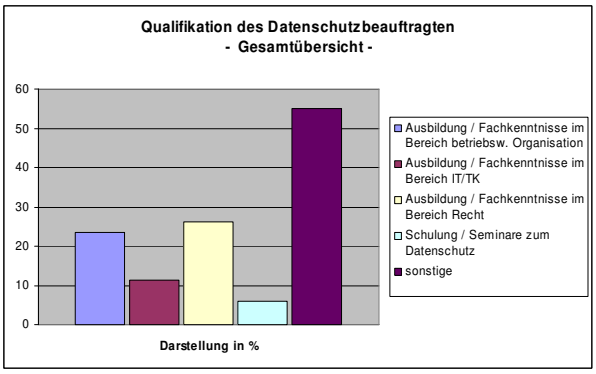




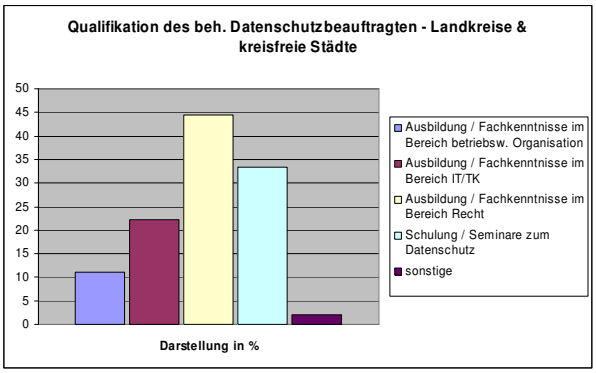


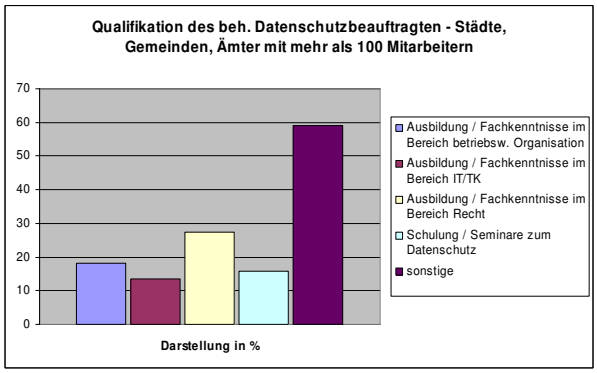


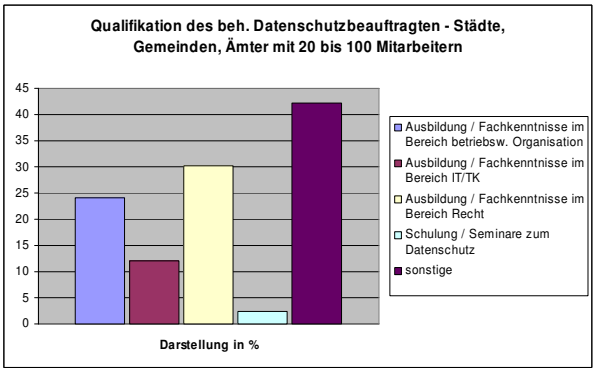
Welche Qualifikation besitzt der Datenschutzbeauftragte?

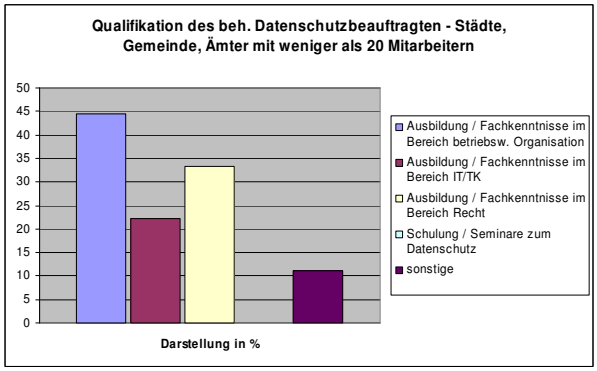


Der behördliche Datenschutzbeauftragte benötigt zur Erfüllung seiner Aufgaben die erforderliche Fachkunde. Die Vielfältigkeit der Angaben (zusammengefasst unter „sonstige“) zeigt, dass die behördlichen Datenschutzbeauftragten aus den unterschiedlichsten Ausbildungsbereichen berufen werden. Aus den im Fragebogen vorgegebenen Antworten wurde die juristische Ausbildung am häufigsten benannt.

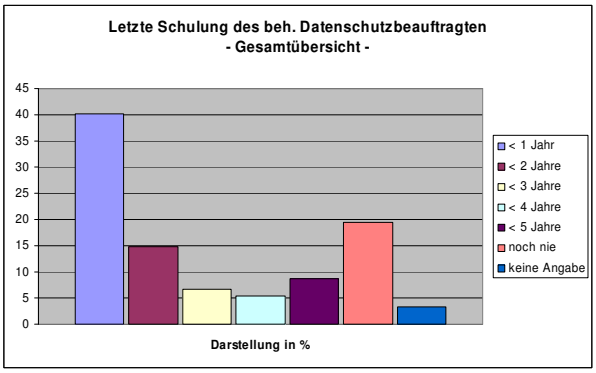






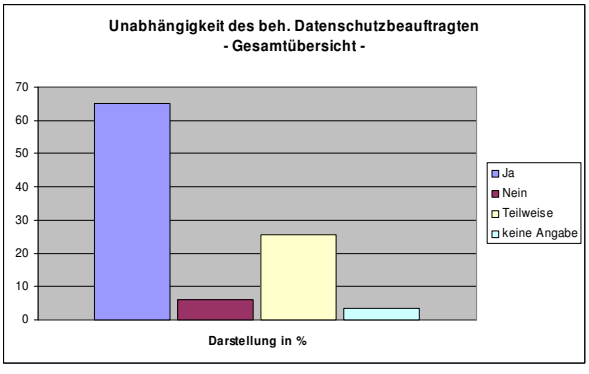


Wann wurde der Datenschutzbeauftragte letztmalig geschult?



Datenschutzschulungen sind ein wichtiges Instrument um die Qualifikation und Kompetenz des behördlichen Datenschutzbeauftragten sicherzustellen. Diese sollten regelmäßig durchgeführt werden. Nur 40% der behördlichen Datenschutzbeauftragten wurden innerhalb des letzen Jahres geschult. Die Tatsache, dass ca. 1/5 der behördlichen Datenschutzbeauftragten noch nie geschult wurde, zeigt den entsprechenden Nachholbedarf.

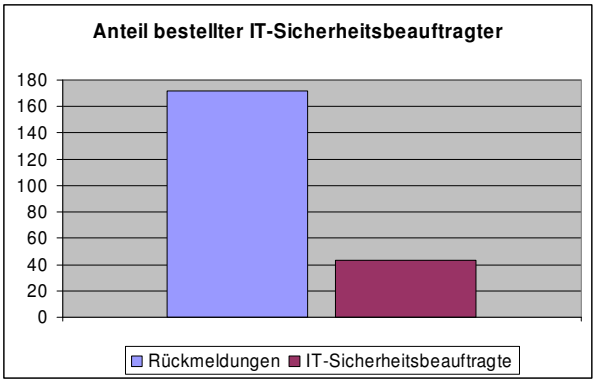
Ist der Datenschutzbeauftragte in seiner Tätigkeit frei und unabhängig?



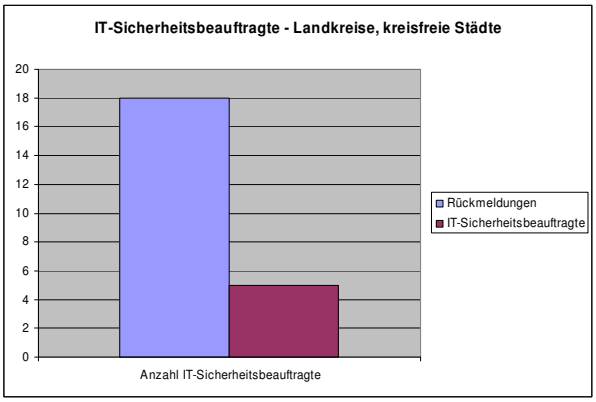
Die Unhabhängigkeit des behördlichen Datenschutzbeauftragten ist in den meisten Kommunen nach deren eigener Einschätzung gegeben. Die Einschränkungen sind zumeist ressourcenbedingt oder an die Haupttätigkeit des behördlichen Datenschutzbeauftragten geknüpft.

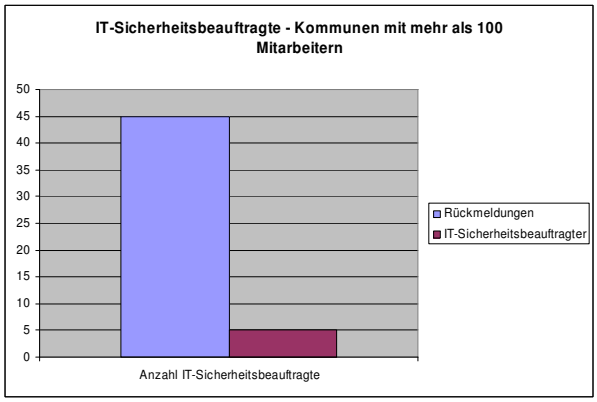
2.1.2 Fragen zum IT-Sicherheitsbeauftragten

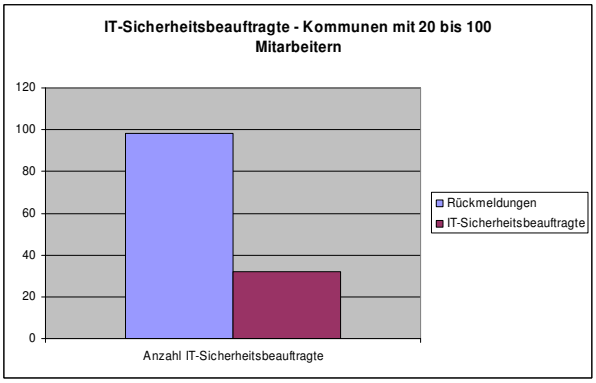
Haben Sie einen IT-Sicherheitsbeauftragten bestellt?

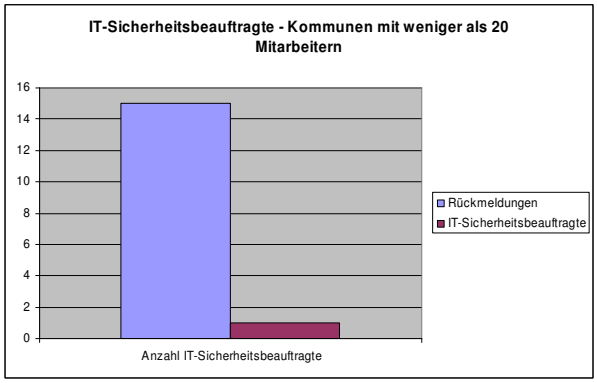


Der IT-Sicherheitsbeauftragte ist keine durch das BbgDSG geforderte Position. Er übt aber eine wichtige Funktion in der Kommunalverwaltung aus, um die IT-Sicherheit zu gewährleisten und zu fördern. Derzeit wird diese Position nur von einem sehr kleinen Teil der Kommunen besetzt.

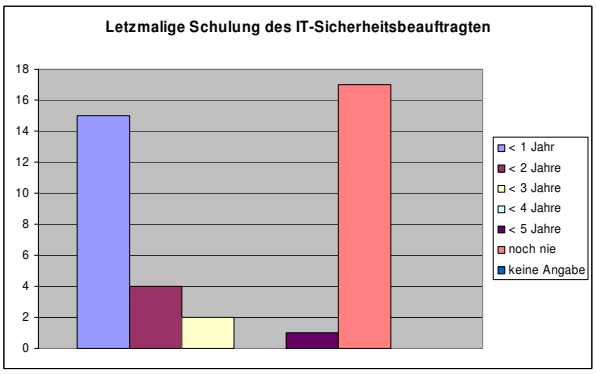








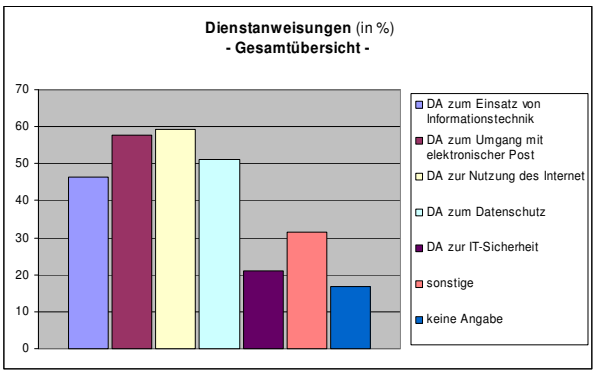
Wann wurde der IT-Sicherheitsbeauftragte letztmalig geschult?



Die bestellten IT-Sicherheitsbeauftragten sind zumeist ADV-Sachbearbeiter der Kommunen, die auf Grund ihrer Ausbildung und Erfahrung diese Position ausüben. Ca. 50% haben noch keine Schulung zum IT-Sicherheitheitsbeauftragten oder zum IT-Sicherheitsmanagement erhalten.

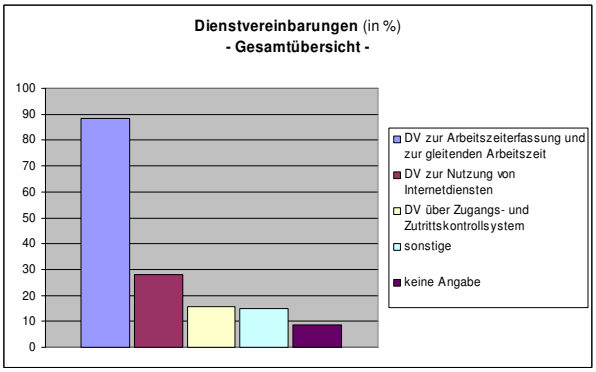
2.2 Organisatorisches

Welche Dienstanweisungen sind bei Ihnen erlassen worden?



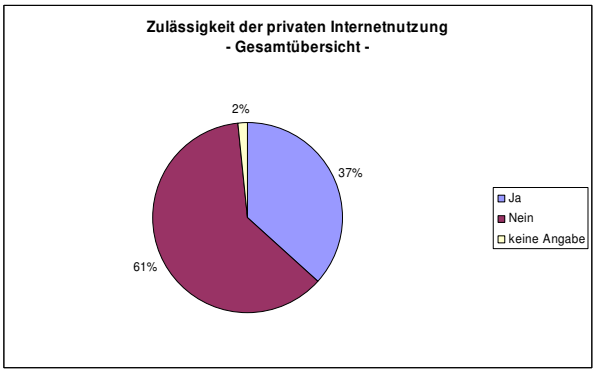
Der Einsatz von Dienstanweisungen für die Nutzung der Netz-Dienste und Informationstechnik ist unbedingt notwendig, um den Umgang mit der IT zu regeln und Mitarbeiter auf die bestehenden Gefahren hinzuweisen. Auch Datenschutzaspekte sind zu berücksichtigen. Der überwiegende Teil der Kommunen regelt dies in mehreren Dienstanweisungen bzw. fasst diese zusammen.

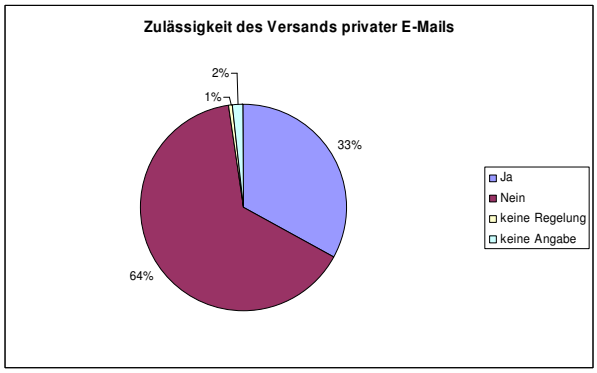
Welche Dienstvereinbarungen sind bei Ihnen verabschiedet worden?



Dienstvereinbarungen können dort abgeschlossen werden, wo der Personalrat ein Mitbestimmungsrecht hat. Hier werden insbesondere die Rechte der Mitarbeiter vertreten und die Befugnisse des Arbeitgebers geregelt. Ziel ist u. a. der Schutz der Privatsphäre ihrer Tätigkeit.

Ist in Ihrer Verwaltung die private Nutzung des Internet oder der Versand privater E-Mails erlaubt?

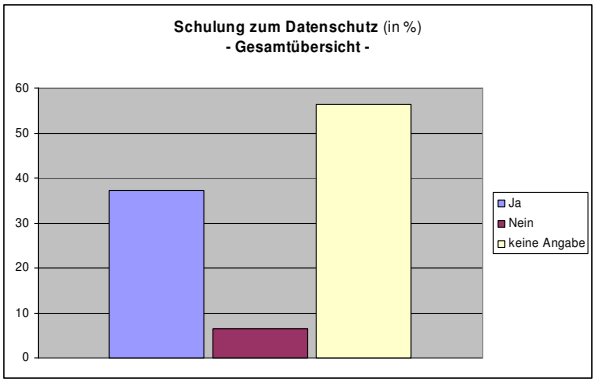




Die private E-Mail- und Internetnutzung kann eine zusätzliche Gefährdung der IT-Sicherheit und des Datenschutzes in den Kommunen bedeuten. Eine direkte Kontrolle des Netzwerkverkehrs ist nicht mehr gegeben. Eine entsprechende Dienstvereinbarung kann auch hier nur bedingt Abhilfe leisten.

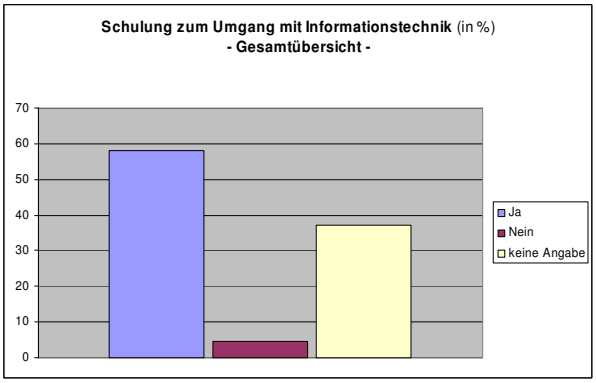
2.3 Schulung und Sensibilisierung der Mitarbeiter

Werden die Mitarbeiter regelmäßig auf dem Gebiet des Datenschutzes geschult?



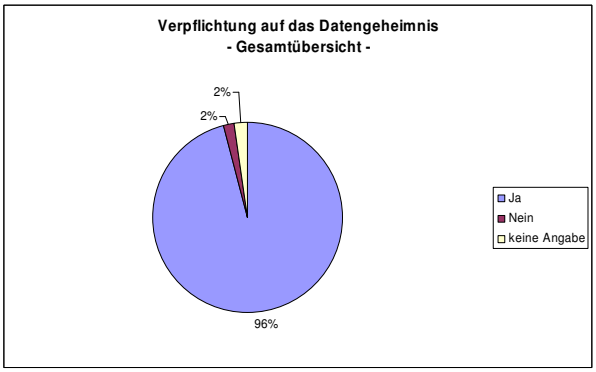
Der Schutz der personenbezogenen Daten, die in der Kommunalverwaltung verarbeitet werden, ist Grundlage für das Vertrauen der Bürger in die Kommune. Der sichere und vertrauensvolle Umgang sollte regelmäßig geschult werden. Nur rund ein Drittel erfüllt diese Aufgabe.

Werden die Mitarbeiter regelmäßig auf den sachgerechten Umgang mit Informationstechnik geschult / hingewiesen und für mögliche Gefährdungen sensibilisiert?



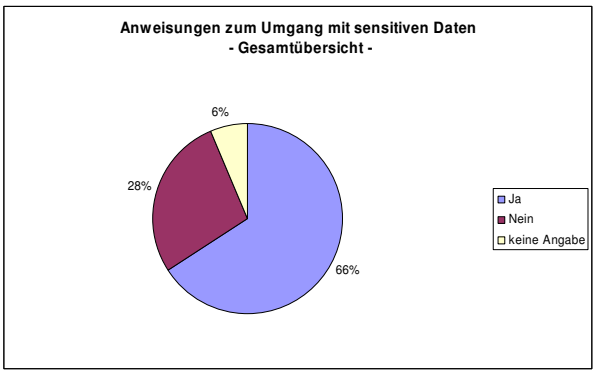
Informationstechnik bestimmt in immer stärkerem Maß die Arbeit der Verwaltung. Schulungen zum sachgerechten Umgang werden durch die Mehrheit der Kommunen regelmäßig durchgeführt. In den meisten Kommunen erfolgen die Schulungen nach Bedarf, z.B. bei der Einführung neuer IT-Systeme und Verfahren.

Sind die Mitarbeiter auf das Datengeheimnis verpflichtet?



Der Verpflichtung der Mitarbeiter auf das Datengeheimnis sind fast alle Kommunen (96%) nachgekommen. Dies zeigt, dass sich die Kommunen Ihrer Verantwortung der durch den Bürger anvertrauten Daten im vollen Umgang bewusst sind.

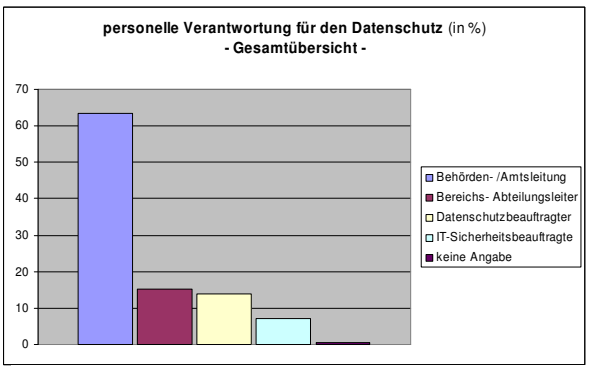
Gibt es spezielle Anweisungen der Mitarbeiter für den Umgang mit sensitiven Daten?

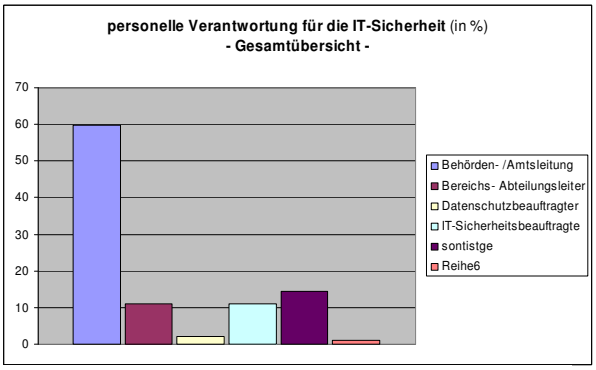


Rund 2/3 der Kommunen erachten es als notwendig, spezielle Anweisungen in Bezug auf den Umgang mit sensitiven personenbezogenen Daten zu erlassen. Insbesondere bei personenbezogenen Daten mit einem hohen oder sehr hohen Schutzbedarf können diese den Schutz der Daten erhöhen und das Vertrauen der Bürger fördern.

2.4 Verantwortlichkeiten

Wer trägt die Verantwortung für die Einhaltung des Datenschutzes und der IT-Sicherheit?

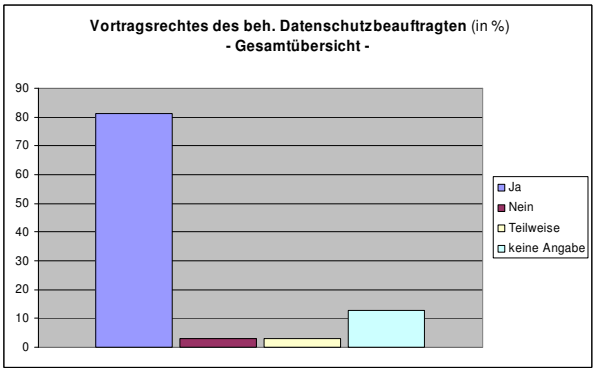




Die Verantwortung für den Datenschutz und die IT-Sicherheit liegt bei der Behördenleitung. Der Datenschutzbeauftragte als auch der IT-Sicherheitsbeauftragte unterstützen die Behördenleitung bei der Ausübung ihrer Tätigkeit in Bezug auf Datenschutz und IT-Sicherheit.

Über diesen Umstand sind sich nur rund 2/3 der Kommunen im Klaren. Eine Verlagerung der Verantwortung auf den behördlichen Datenschutzbeauftragten oder IT-Sicherheitsbeauftragten ist nicht möglich. Eventuell kann bei größeren Institutionen ein Teil der Verantwortung an Bereichs- oder Abteilungsleiter delegiert werden.

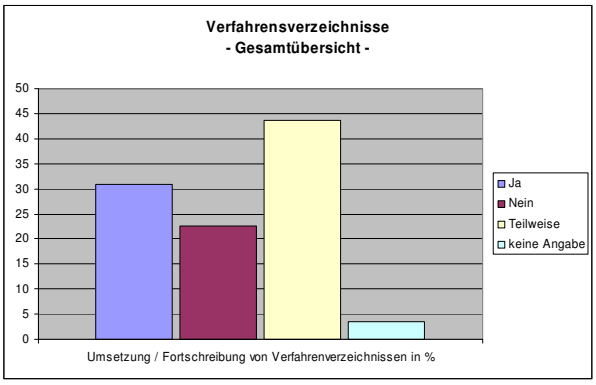
Ist dem Datenschutzbeauftragten und dem IT-Sicherheitsbeauftragten ein uneingeschränktes Vortragsrecht bei der Behördenleitung eingeräumt?

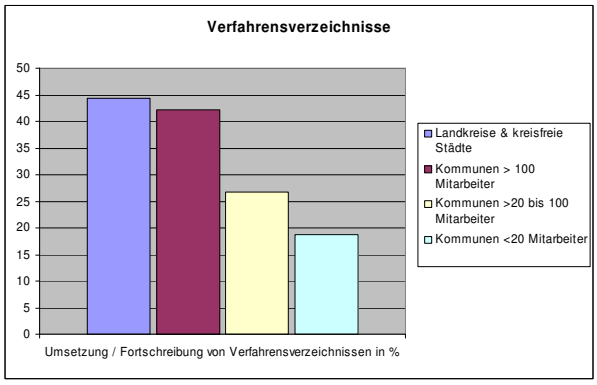


Zur Ausübung der Verantwortung der Behördenleitung gegenüber Datenschutz und IT-Sicherheit müssen diese über bestehende Probleme oder Gefährdungen unterrichtet werden. Aus eigenem Interesse sollte die Behördenleitung dem Datenschutzbeauftragten und dem IT-Sicherheitsbeauftragten ein uneingeschränktes Vortragsrecht einräumen. Ca. 80% der Kommunen setzen dies um.

2.5 Verfahrens- und Sicherheitsbetrachtung

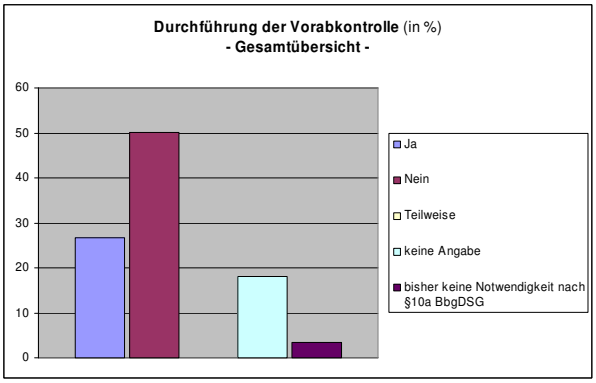
Liegen für Ihre Fachverfahren (mit Personenbezug) Verfahrensverzeichnisse nach § 8 BbgDSG vor?





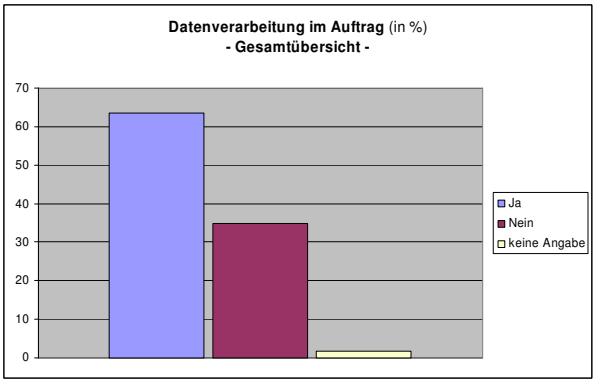
Nach § 8 BbgDSG sind für automatisierte Verarbeitungen personenbezogener Daten durch die Daten verarbeitende Stelle Verfahrensverzeichnisse zu führen. Hier besteht erheblicher Nachholbedarf auf Seiten der Kommunen.

Wurde eine Vorabkontrolle nach § 10a BbgDSG (falls notwendig) durchgeführt?



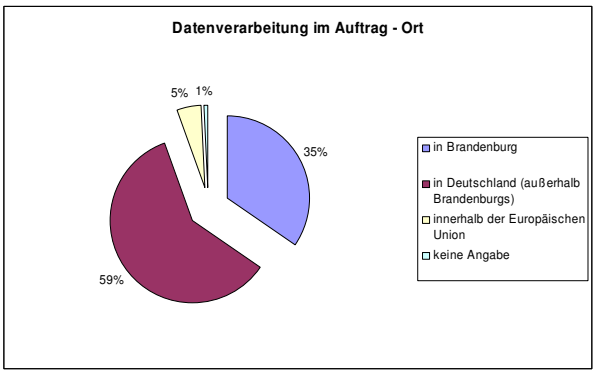
Bei der Verarbeitung von Daten, von denen besondere Risiken für die Rechte und Freiheiten der Betroffenen ausgehen, ist nach § 10a BbgDSG eine Vorabkontrolle durchzuführen. Nach den vorliegenden Ergebnissen ist von über 60% der Kommunen noch nie eine Vorabkontrolle durchgeführt worden. Dies heißt im Umkehrschluss, 60% der Kommunen schätzen ein, dass von den von Ihnen betriebenen Verfahren keine besonderen Risiken ausgehen. Dies darf bezweifelt werden.

Werden Daten, die unter Ihrer Verantwortung stehen, außer der Dienststelle verarbeitet?



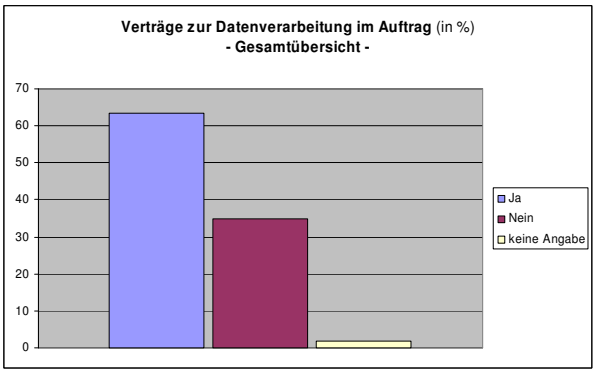
Datenverarbeitung im Auftrag ist eine etablierte Vorgehensweise in der Kommunalverwaltung. Rund 2/3 der Kommunen lassen Daten im Auftrag verarbeiten.

Wo werden diese Daten verarbeitet?



Bei der Datenverarbeitung im Auftrag findet diese zumeist in Deutschland statt. Ein geringer Anteil lässt Daten außerhalb Deutschlands, aber innerhalb der europäischen Union verarbeiten. Es kann festgehalten werden, dass in diesen Fällen bei der Datenverarbeitung im Auftrag angemessene Datenschutzrichtlinien vorliegen.

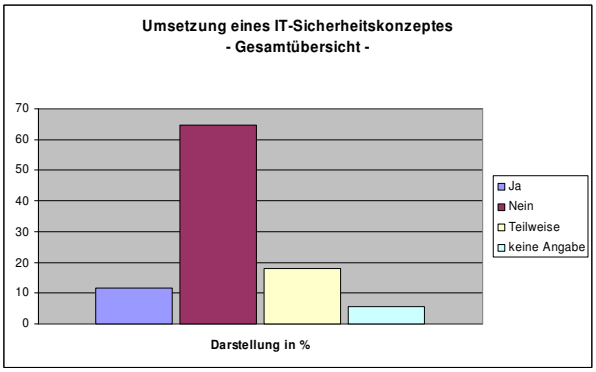
Bestehen für die Datenverarbeitung außerhalb der Dienststelle vertragliche Vereinbarungen für die Auftragsdatenverarbeitung nach § 11 BbgDSG?

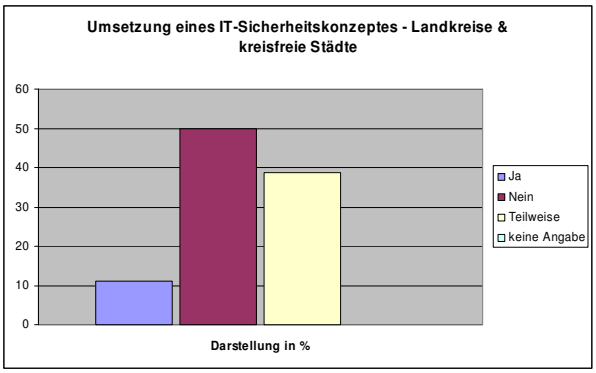


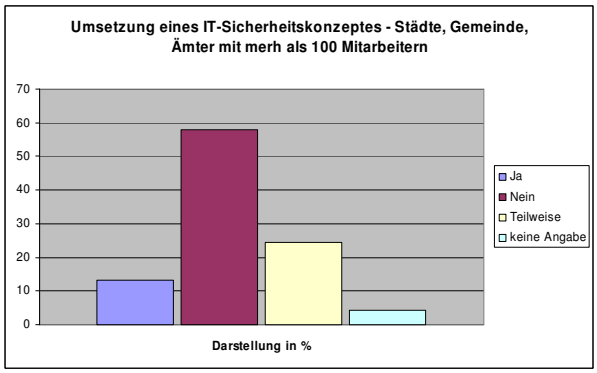
Vertragliche Vereinbarungen bei der Datenverarbeitung im Auftrag bilden die Grundlage für eine sichere und nachvollziehbare Datenverarbeitung. Bedenklich ist, dass rund 1/3 der Kommunen keine entsprechenden Vereinbarungen getroffen hat. Dies ist nachzuholen.

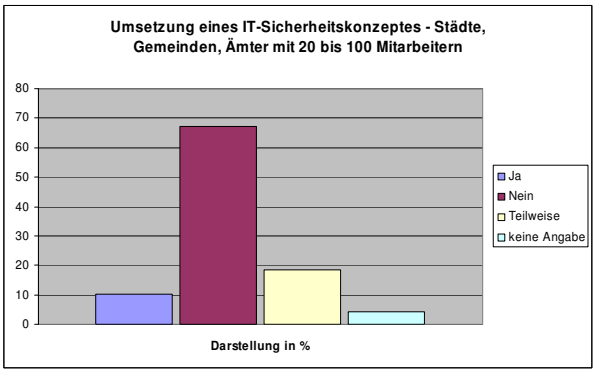
Haben Sie verfahrensspezifische Sicherheitskonzepte entwickelt?

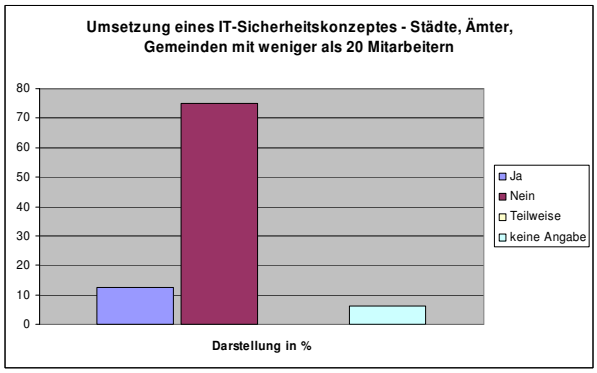
Nach § 7 Abs. 3 BbgDSG darf ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten erst freigegeben werden, wenn ein aus einer Risikoanalyse entwickeltes Sicherheitskonzept ergeben hat, dass die von dem Verfahren ausgehenden Gefahren für die Rechte und Freiheiten der Betroffenen durch technisch-organisatorische Maßnahmen beherrscht werden können. Eine Beachtung dieser datenschutzrechtlichen Anforderungen findet in der Kommunalverwaltung Brandenburg nur zu einem sehr geringen Teil statt. Gerade mal 12% der Kommunen setzen diese um. Ca. 20% geben an, teilweise ein Sicherheitskonzept entwickelt zu haben.



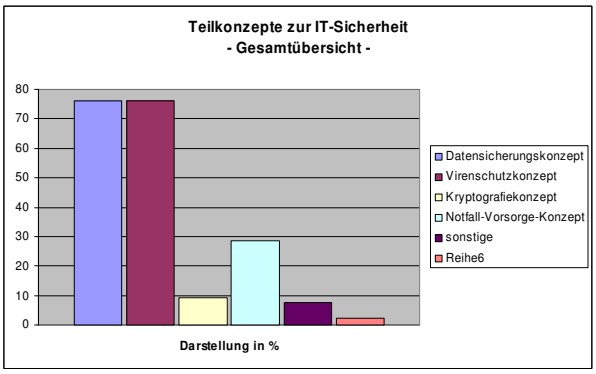




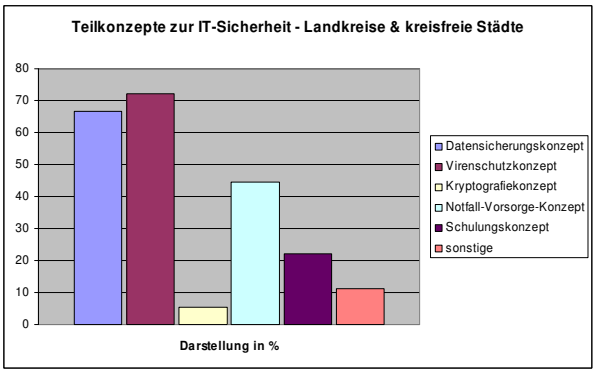


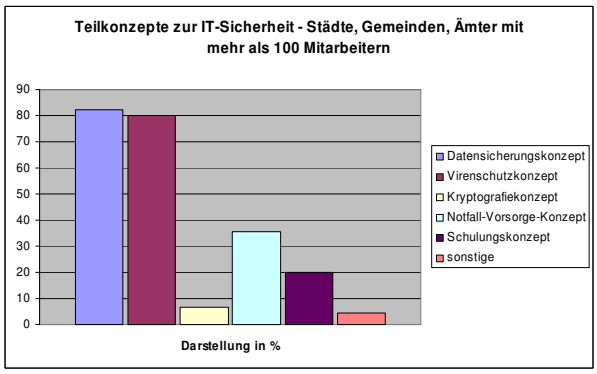


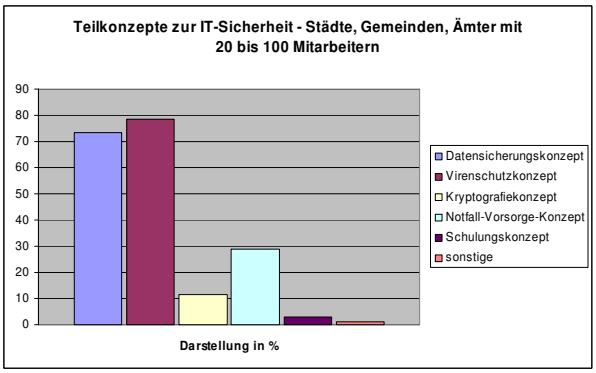
Haben Sie Teilkonzepte zur IT-Sicherheit entwickelt?

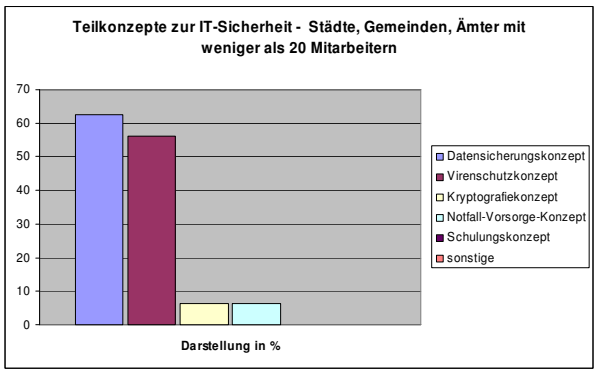


Datenschutz- und Virenschutzkonzepte sind in der Kommunalverwaltung weit verbreitet.
Konzepte zur Notfall-Vorsorge, zur Schulung oder zum Einsatz von Verschlüsslungsverfahren liegen in den seltensten Fällen vor.

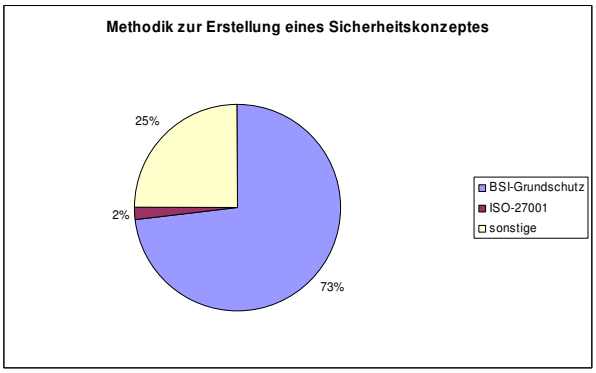






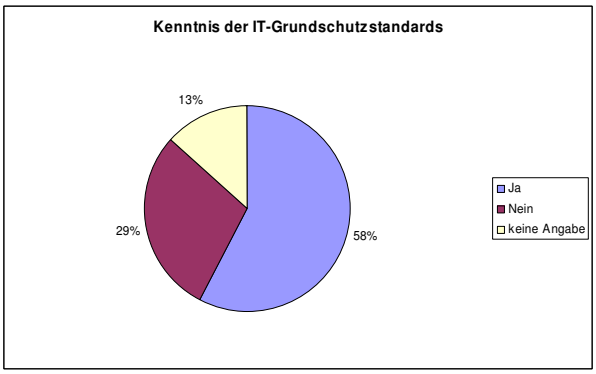


Nach welcher Methodik sind sie dabei vorgegangen?



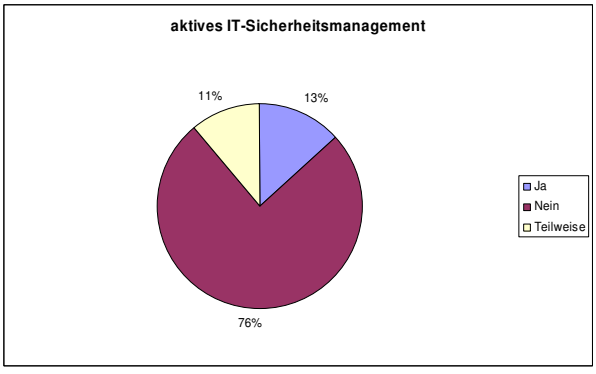
Werden Sicherheitskonzepte umgesetzt, wird in der überwiegenden Mehrzahl nach den IT-Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vorgegangen.

Ist Ihnen die Vorgehensweise nach IT-Grundschutz (BSI) bekannt?



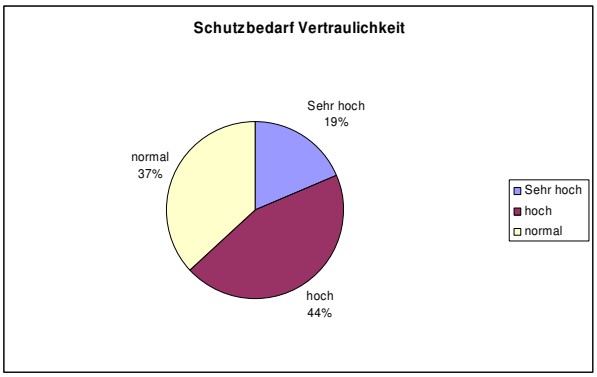
Die IT-Grundschutzstandards selbst sind aber nur 58% der Kommunen bekannt.

Betreiben Sie ein aktives Sicherheitsmanagement?

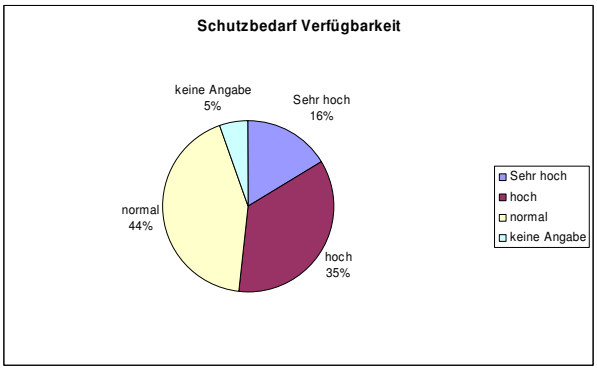


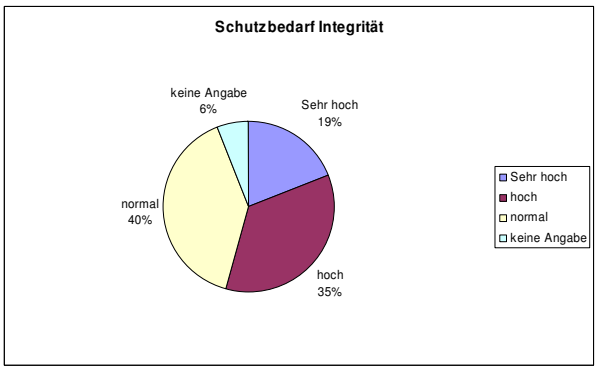
Ein aktives Sicherheitsmanagement wird vor allem von den Kommunen betrieben, die auch einen IT-Sicherheitsbeauftragten berufen haben. Wie sich dieses darstellt, wurde in der Umfrage nicht erfasst.

Wie schätzen sie den max. Schutzbedarf der von Ihnen verarbeiteten (personenbezogenen) Daten in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität ein?

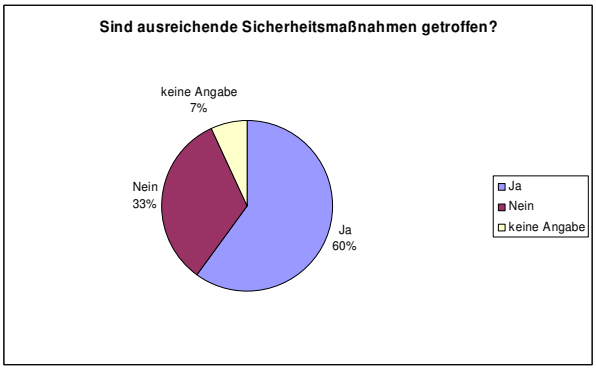


Trotz des überwiegend hohen und sehr hohen Schutzbedarfs der verarbeiteten Daten wurde, wie Antworten auf andere Fragen zeigen, durch den überwiegenden Teil der Kommunen bislang weder eine Vorabkontrolle durchgeführt noch ein vollständiges Sicherheitskonzept entwickelt.





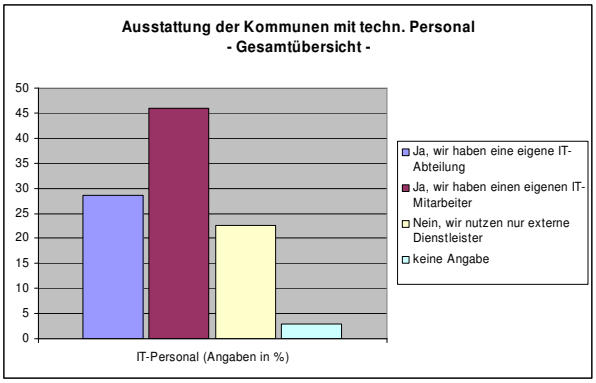
Sind aus Ihrer Sicht alle notwendigen Sicherheitsmaßnahmen getroffen?



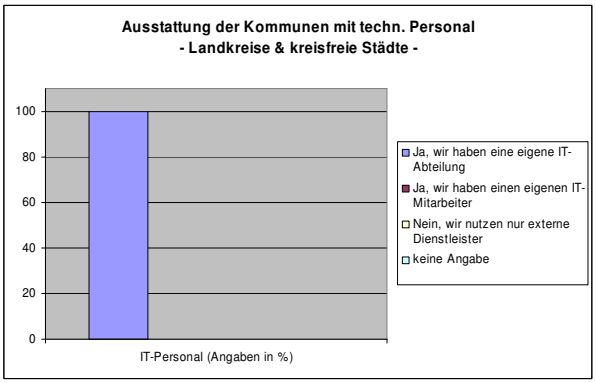
Trotz der Nichtumsetzung eines Sicherheitskonzeptes und dem Verzicht auf eine Vorabkontrolle geben 60% der Kommunen an, ausreichende Sicherheitsmechanismen getroffen zu haben. An dieser Stelle ist zu prüfen, woraus sich die Einschätzung der Kommunen ergibt. Schließlich beschreibt ein Sicherheitskonzept die umgesetzten Sicherheitsmaßnahmen.

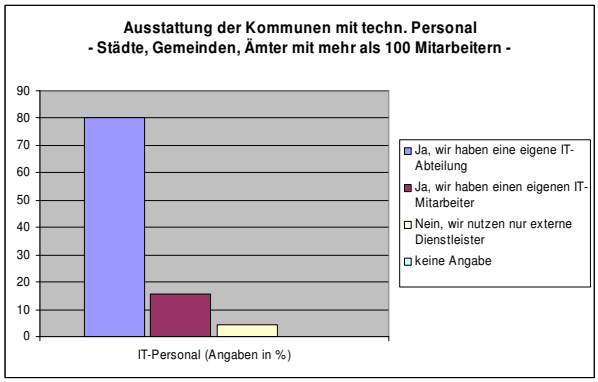
2.6 IT-Ausstattung

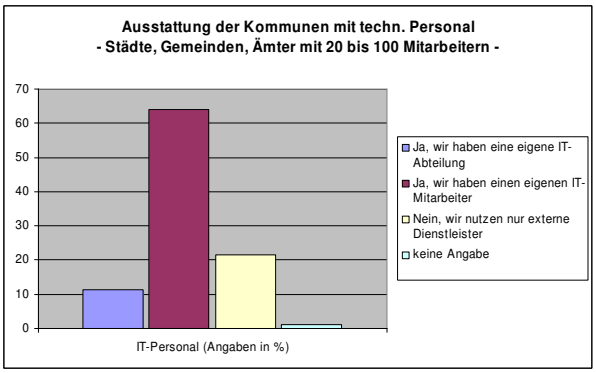
Haben Sie eine eigene IT-Abteilung?

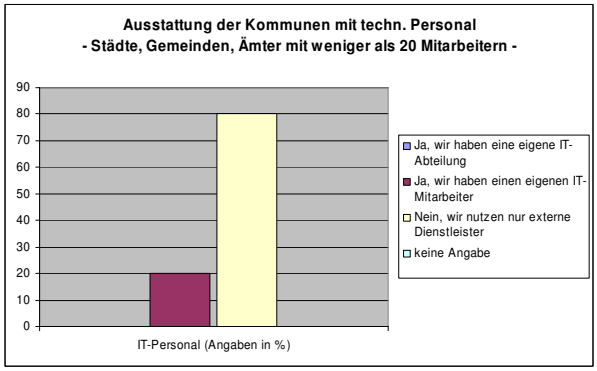


Interessant an der Frage der Personalausstattung ist die Betrachtung der kleineren Kommunen. Trotz der erhebliche Aufgabenfülle steht Ihnen nur ein oder in der Mehrheit der Kommunen kein eigener Mitarbeiter zur Verfügung. Der Einsatz von externen Dienstleistern ist quasi ein „Muss“ um die Ihnen übertragenen Aufgaben erfüllen zu können.

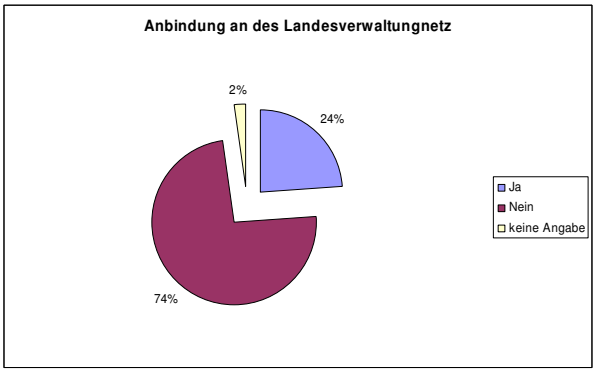




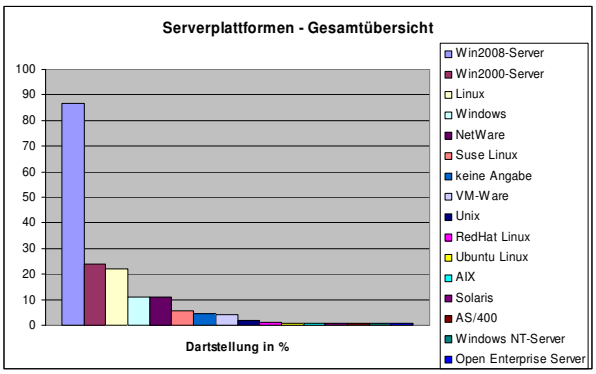




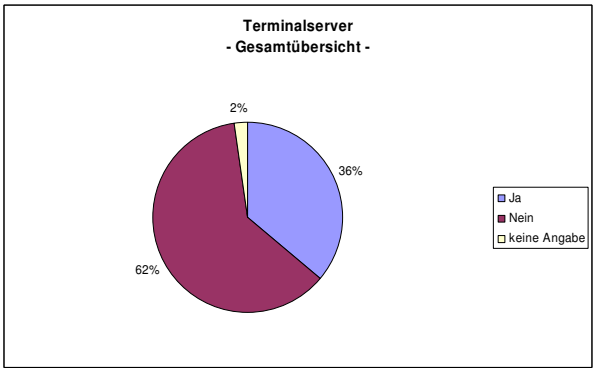
Sind Sie an das Landesverwaltungsnetz angebunden?



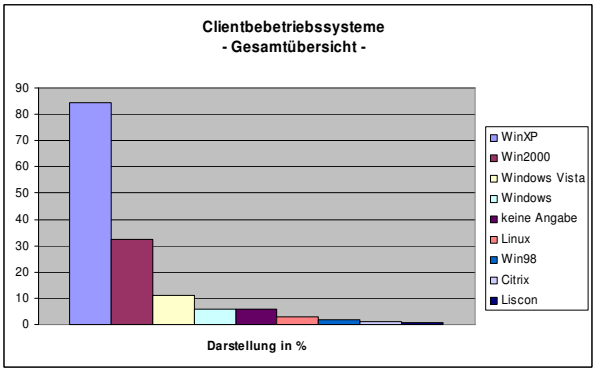
Welche Betriebssystemplattform (-en) nutzen Sie für Ihre Server?



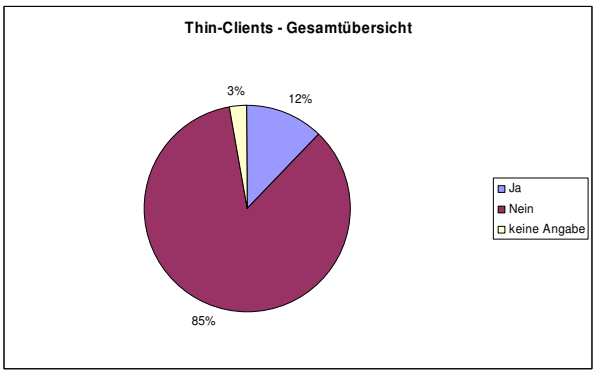
Setzen Sie Terminalserver ein?



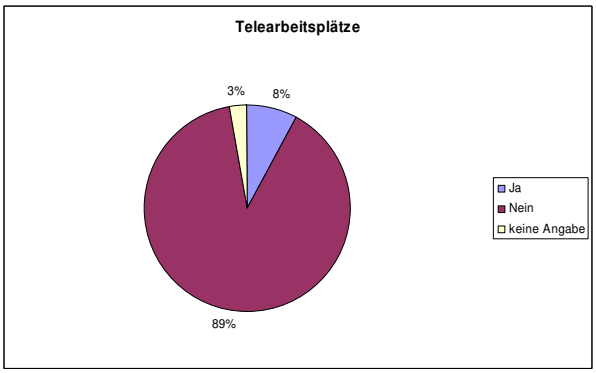
Welche Betriebssysteme setzen Sie auf Clientseite ein?



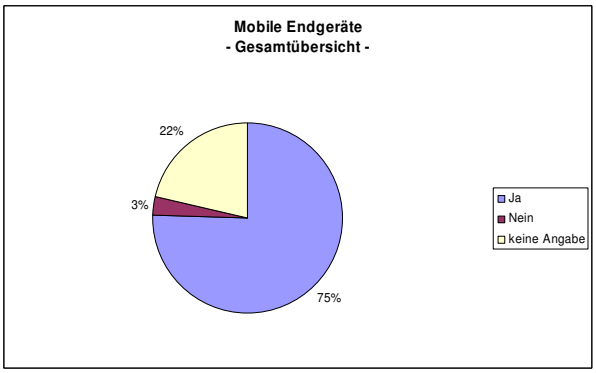
Setzen Sie Thin-Clients ein?



Werden bei Ihnen Telearbeitsplätze eingesetzt?

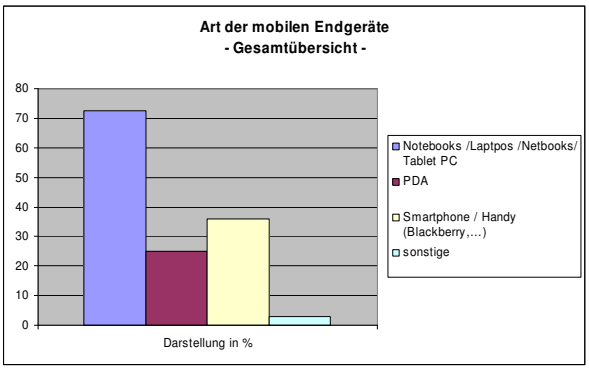


Setzen Sie Mobile Endgeräte ein?



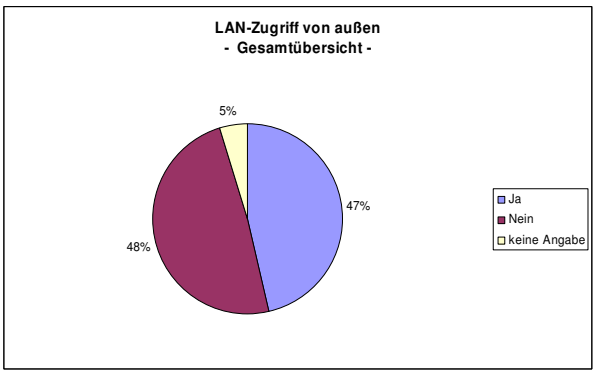
Der Einsatz mobiler Endgeräte ist in der Kommunalverwaltung weit verbreitet. Hieraus ergeben sich aber erhöhte Anforderungen an die IT-Sicherheit und den Datenschutz, da bspw. der Verlust der Endgeräte auch zu einem Verlust der verarbeiteten personenbezogenen Daten führen kann.

Welcher Art sind diese mobilen Endgeräte?



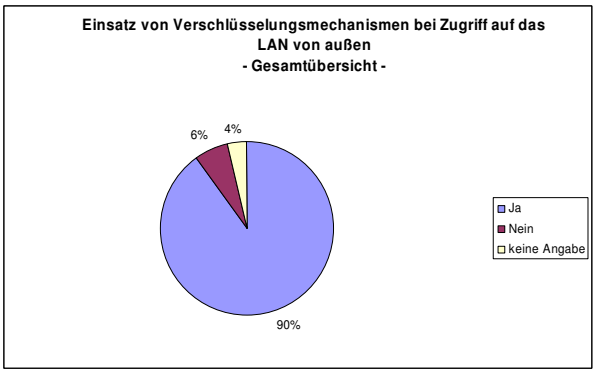
Insbesondere die Kategorie Notebooks / Laptops / Netbooks findet in den Kommunen Anwendung. Dem Einsatz entsprechende Geräte, oder auch PDAs oder Smartphones steht aber der zu betrachtende Schutzbedarf der auf den mobilen Endgeräten verarbeiteten Daten entgegen.

Ist ein Zugriff von außerhalb auf das LAN gestattet?



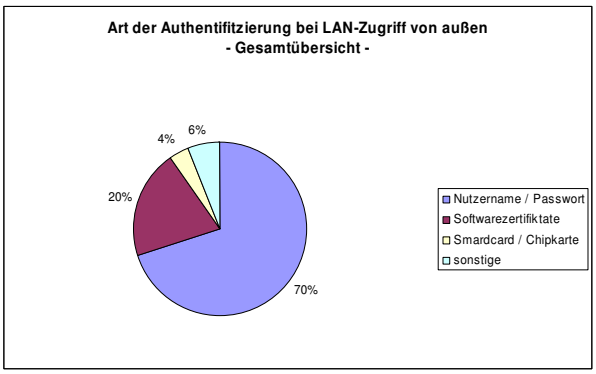
Den externen Zugriff auf das lokale Netz der Kommunalverwaltung erlauben immerhin knapp 50% der Kommunen. Ob dieser Zugriff immer notwendig ist oder er sich nicht eventuell vermeiden ließe, könnte sich aus den Beschreibungen der Verfahrensverzeichnisse und IT-Sicherheitskonzepte ableiten lassen. Schlussendlich muss die Kommune sicherstellen, dass die verarbeiteten personenbezogenen Daten vor einem unberechtigten Zugriff geschützt werden.

Setzen Sie Verschlüsselungsmechanismen für diesen Zugriff auf das LAN ein?



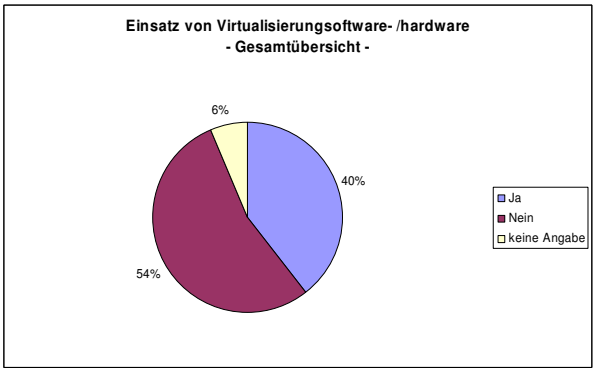
Als eine der Schutzmaßnahmen setzen 90% der Kommunen Verschlüsselungsmechanismen ein. Bedenklich sind die dargestellten 6% der Kommunen die andere Methoden verwenden. Hier ist davon auszugehen, dass die übertragenen Daten im Klartext vorliegen. Die Vertraulichkeit und Integrität ist hier nicht gewährleistet.

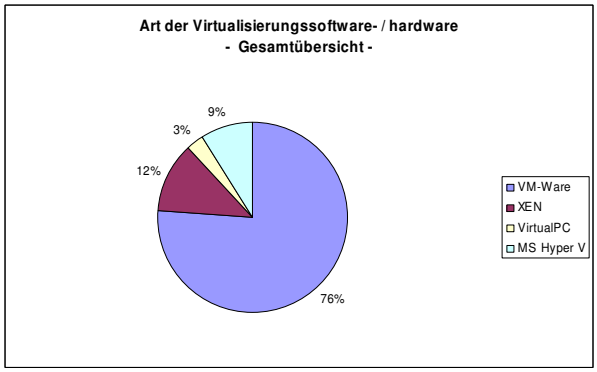
Welche Art der Authentifizierung setzen Sie für den Zugriff von außen auf das LAN ein?



Die Authentifizierung mittels Nutzername / Passwort ist die beim externen Zugriff auf das LAN am häufigsten eingesetzte Authentifizierungsmethode. Insbesondere beim Zugriff auf Verfahren mit hohem oder sehr hohem Schutzbedarf reicht dies nicht aus.

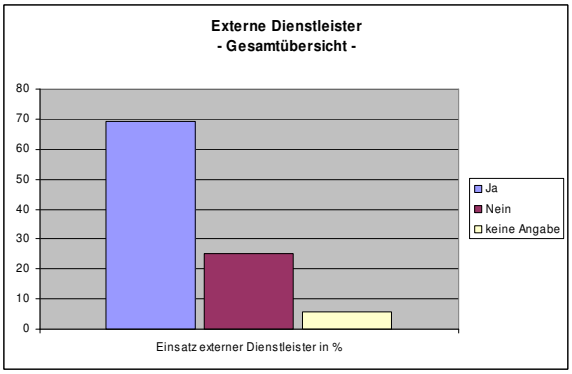
Setzen Sie Virtualisierungssoftware ein, wenn ja welche?



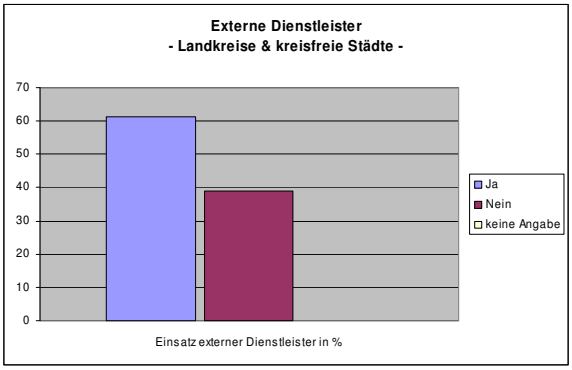


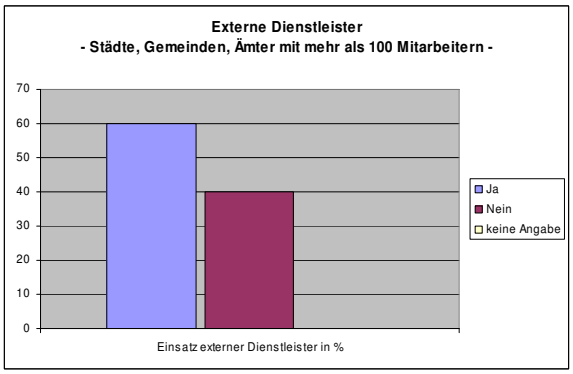
Der Einsatz von Virtualisierungssoftware hat in den letzen Jahren zugenommen. In der Kommunalverwaltung setzen zurzeit rund 40% Virtualisierungssoftware ein (vorrangig VM-Ware). Mit einer weiteren Zunahme ist zu rechnen.

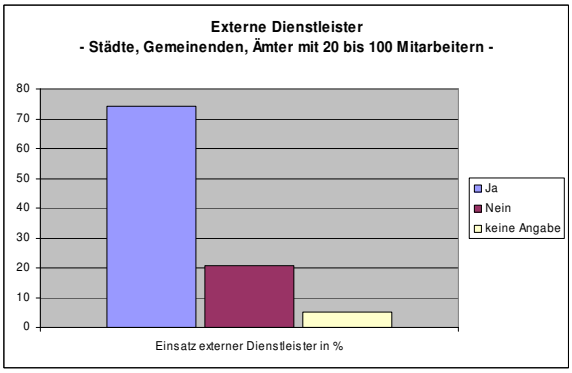
Nehmen Sie für den Betrieb Ihrer IT-Infrastruktur externe Dienstleistungen in Anspruch?

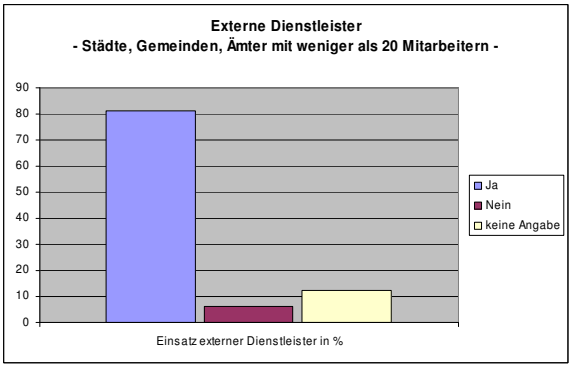


Der Einsatz externer Dienstleister ist in den Kommunalverwaltungen stark verbreitet. Rund 70% aller Kommunen nutzen externe Fachkräfte. Interessant ist der prozentuale Anstieg des Einsatzes externer Dienstleister gegenüber der verminderten Anzahl an Mitarbeitern kleinerer Kommunen. So setzen „nur“ 60% der Kommunen mit mehr als 100 Mitarbeitern externe Dienstleister ein, Kommunen mit weniger als 20 Mitarbeitern hingegen knapp über 80%.

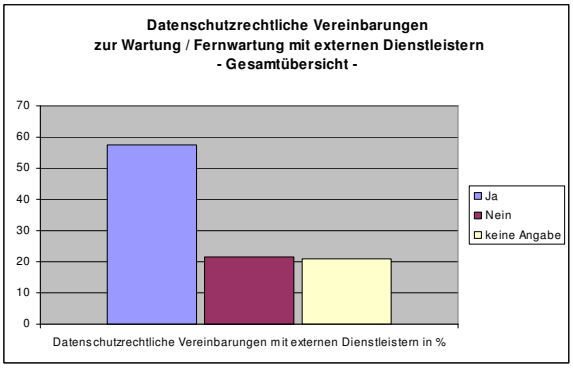




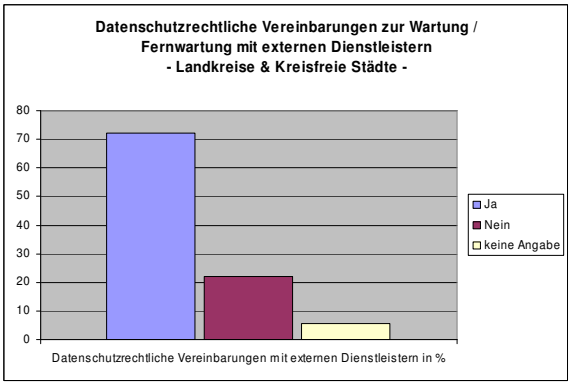


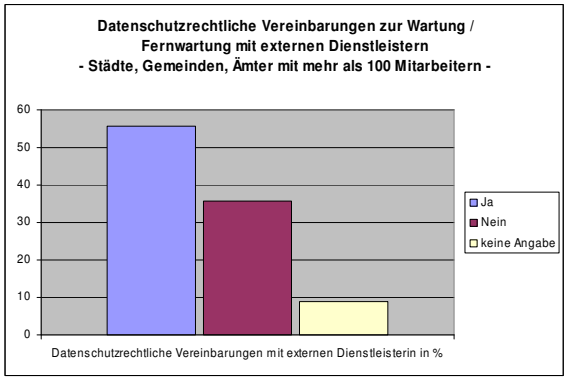


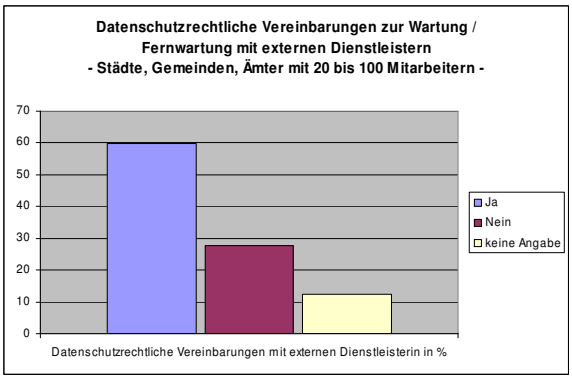
Haben Sie datenschutzrechtliche Vereinbarungen zur Wartung / Fernwartung mit ihren externen Dienstleistern?

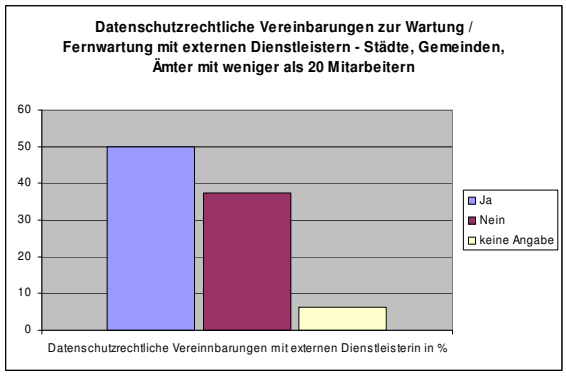


Bei den datenschutzrechtlichen Vereinbarungen zur Wartung / Fernwartung gibt es einen erheblichen Nachholbedarf. Nur knapp 60% der Kommunen besitzen entsprechende Vereinbarungen. D.h. im Umkehrschluss existieren bei 40% der Kommunen keine Regelungen bzgl. personenbezogener Daten, die dem Dienstleister im Rahmen der Wartung zur Kenntnis gelangen.



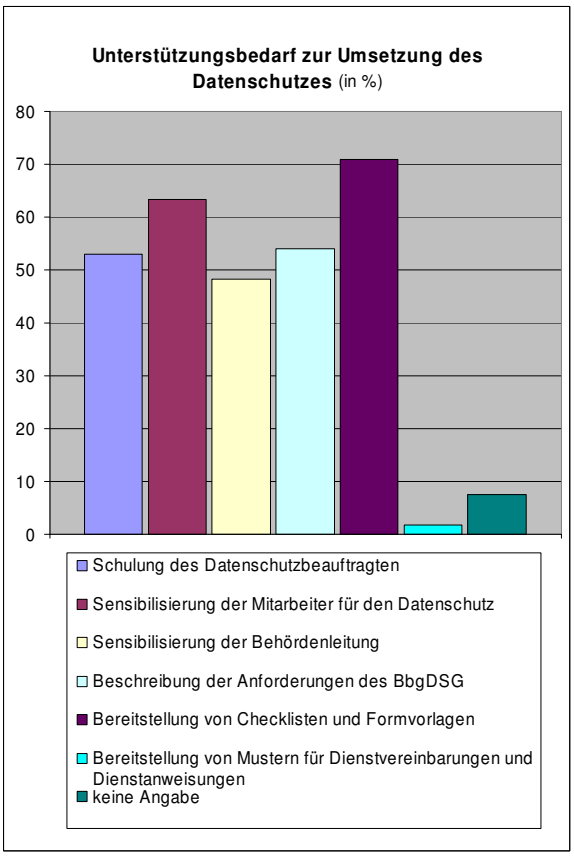






2.7 Handlungsbedarf

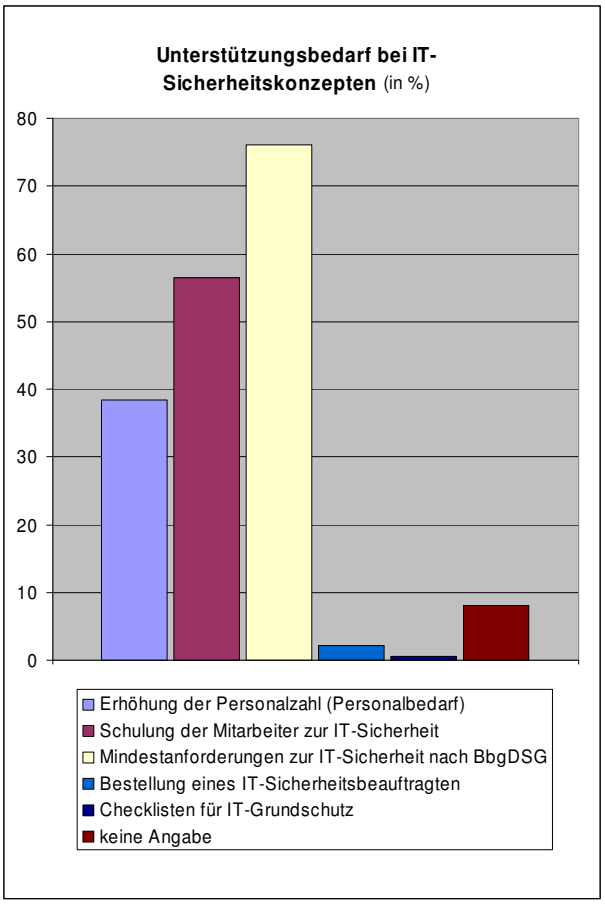
Wo sehen Sie erhöhten Handlungsbedarf für die Umsetzung des Datenschutzes?



Als Abschluss der Umfrage sollten die Kommunen Ihre Anregungen und Wünsche äußern, die zu einer Verbesserung des Datenschutzes führen können. Rund 70% sehen zentrale Vorgaben, die sich in Checklisten und Formvorlagen widerspiegeln, als ein wünschenswertes Hilfsmittel. Die Schulung und Sensibilisierung des Datenschutzbeauftragten (53%), der Mitarbeiter (65%) und auch der Behördenleitung (54%) werden als erforderlich angesehen.

Ableiten lässt sich, dass sich die Kommunen über die bestehenden Defizite bewusst sind, sie die notwendigen Schritte zur Verbesserung des Datenschutzes aber nicht allein umsetzen können.

Was ist aus Ihrer Sicht notwendig, um die Umsetzung eines IT-Sicherheitskonzeptes voranzutreiben?



Für die Umsetzung von IT-Sicherheitskonzepten erwarten die Kommunen zentrale Vorgaben (75%), vor allem dahingehend, was das Brandenburgische Datenschutzgesetz im Rahmen einer IT-Sicherheitsbetrachtung erwartet.

Dem IT-Sicherheitsbeauftragten (3%) wird kaum eine Bedeutung beigemessen.

Wie im Datenschutz wird ein Schwerpunkt zur Verbesserung der IT-Sicherheit bei der Schulung der Mitarbeiter (55%) gesehen.

3. Fazit

Die auf Basis der gesetzlichen Anforderungen durchgeführte Umfrage zeigt die bestehenden Mängel bei der Umsetzung des Brandenburgischen Datenschutzgesetzes auf. Die existierenden Vollzugsdefizite in vielen Bereichen der Kommunalverwaltung sind Ausdruck für die bestehende Unsicherheit bei der Umsetzung der gesetzlichen Datenschutzregelungen, aber auch der zunehmenden Aufgabenfülle der Verwaltung bei gleichzeitig knappen Ressourcen.

Die Landesbeauftragte beabsichtigt, die Kommunalverwaltungen bei der Behebung der Mängel durch Schulungen zu unterstützen und dabei mit der TUIV-AG (Kommunale Arbeitsgemeinschaft Technikunterstützte Informationsverarbeitung im Land Brandenburg), dem Brandenburgischen IT-Dienstleister, sowie dem Netzwerk SeSamBB (Security and Safety made in Berlin-Brandenburg e. V.) zu kooperieren. Die betroffenen Kommunen sind jedoch zunächst gehalten, ihre eigene Verantwortung zur Umsetzung des Datenschutzes wahrzunehmen. Synergieeffekte durch verwaltungsübergreifende Kooperationen sowie externe Unterstützung können insbesondere kleinen Verwaltungen helfen, fehlende Ressourcen zu kompensieren.