GPA-Mitteilung 1/2010

Az. 049.00

15.01.2010

Einsatz von ADV-Verfahren in Eigenregie

Ausgangslage

Durch den mittlerweile als Standard im Arbeitsleben zu bezeichnenden PC am Arbeitsplatz und der damit verbundenen Vernetzung innerhalb der Verwaltung, betreibt heute nahezu jede Kommune ein eigenes „kleines Rechenzentrum". Die Kommune muss sich hierbei bewusst sein, dass sie bei dieser **Inhouse-Verarbeitung** (Server-/Rechnerstandort im Hause) erheblichen Gefährdungen ausgesetzt ist (z.B. durch höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen, Risiken von außen über Internet usw.).

Werden hierbei **ADV-Verfahren zur Abwicklung von Finanzvorgängen** eingesetzt, so hat die Verwaltung in Eigenregie sicherzustellen, dass in das Verfahren nicht unbefugt eingegriffen werden kann, die gespeicherten Daten nicht verloren gehen, nicht unbefugt verändert werden und die Daten während der Aufbewahrungsfristen jederzeit ausgedruckt werden können (§§ 11 Abs. 1 und 23 Abs. 2 GemKVO). Dies gilt sowohl für autonome Verfahren, als auch für solche, die über ein Regionales Rechenzentrum (RRZ) beschafft worden sind, aber bei der Gemeinde auf dem eigenen Rechner eingesetzt werden. Auch ist die Gemeindekasse so einzurichten, dass die Datenverarbeitungssysteme nicht unbefugt benutzt werden können (§ 5 Abs. 1 Nr. 3 GemKVO). Im Übrigen sind die Anforderungen der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme - GoBS (insbesondere Kapitel 5, Datensicherheit) zu beachten.

Dabei gilt es aber nicht nur, die unmittelbar finanzwirksamen Programme zu betrachten, sondern auch die **sonstigen Datenbestände** (z.B. Systeme für die geografische Informationsverarbeitung, digitale Archivierungssysteme, Datenbanken usw.) zu berücksichtigen, da auch sie Werte darstellen, die ausreichend geschützt werden müssen. In den Ge-

schäftsberichten 1994/1995 und 2008 (jeweils im Abschnitt 3.4) ist auf die Notwendigkeiten entsprechender Maßnahmen bereits ausführlich eingegangen worden.

Maßnahmen zur Daten- und Programmsicherheit, Risikoanalyse

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen ausführlichen Maßnahmenkatalog zur Daten- und Programmsicherheit (**IT-Grundschutzkatalog**) erarbeitet (www.bsi.bund.de). Auf der dortigen Homepage stehen eine Vielzahl von weiteren Informationen zum Download zur Verfügung (z.B. ein Leitfaden zur Informationssicherheit).

Um die Verwaltungen zu sensibilisieren und den Einstieg in die durchaus komplexe Materie zu erleichtern, sind auf dieser Grundlage sowie eigener Erfahrungen aus der Prüfung wesentliche Fragen herausgearbeitet worden, die sich gerade auch beim Einsatz von Finanzsoftware in Eigenregie stellen. Der in der Anlage zusammengestellte Fragenkatalog soll der Verwaltung zunächst als Grundlage für eine **Grobanalyse** der bestehenden Maßnahmen zur Daten- und Programmsicherheit dienen. Er erhebt bewusst nicht den Anspruch auf Vollständigkeit, sondern zeigt einzelne Risikobereiche auf. Diese müssen dann unter Berücksichtigung der **örtlichen Risikoeinschätzung** und **Hinzuziehung weiterer Informationen** (z.B. aus dem IT-Grundschutzkatalog) vertieft untersucht bzw. ergänzt werden.

In den nachfolgenden Schritten sind die **erforderlichen individuellen Schutzmaßnahmen** aus der Risikoanalyse abzuleiten und umzusetzen sowie in einem Sicherheitskonzept darzustellen (zu dokumentieren).

Anlage
Fragenkatalog Daten- und Programmsicherheit

gpa Baden-Württemberg

Fragestellungen/Maßnahmen	Sachstand, Risikobeurteilung
1 Organisatorische und personelle Maßnahmen	
1.1 Sind Regelungen zum Programmeinsatz vorhanden?	
• Regelungen zum Einsatz neuer Programmversionen (z.B. Austesten der neuen Funktionalitäten in einem Testsystem).	
• Regelungen zur Änderung von Parameterdateien (wer darf was, wie ist zu dokumentieren, wann ist die freigebende Stelle einzuschalten); z.B. Aussteuerung von Schnittstellenparametern.	
• Regelungen zur Eigenprogrammierung (soweit diese erfolgt); wer darf eine Programmierung (z.B. Programmänderungen) vornehmen, wie ist diese auszutesten, zu dokumentieren usw.	
1.2 Bestehen Vorgaben zu den Verarbeitungsprozessen?	
• Definition von finanzrelevanten (buchungsrelevanten) Abläufen mit Festlegen der Reihenfolge (z.B. welche Programmreihenfolge ist beim Mahnen einzuhalten).	
1.3 Bestehen Regelungen zum Passwortgebrauch?	
• Mindestlänge (z.B. 8 Zeichen), keine Trivialpasswörter („Passwort“, „geheim“ usw.), Sperrung nach einer bestimmten Anzahl von Fehlversuchen.	
• Regelungen zur Geheimhaltung der Passwörter.	
1.4 Welche Maßnahmen sind für einen „Notfall“ getroffen?	
• Ausreichende Personalstärke für den Rechner- bzw. Netzwerkbetrieb (mind. 2 Personen wegen Vertretung), ggf. auch Unterstützung durch Externe.	
• Aufbewahrung wichtiger Passwörter (z.B. Administratorpasswort) für den Urlaubs- und Vertretungsfall (an einem sicheren Ort).	
• Durchführung regelmäßiger Brandschutzbegehungen, ggf. Bestellung eines Brandschutzbeauftragten, Datensicherheitsbeauftragten.	
• Durchführung regelmäßiger Notfallübungen (Datenwiederherstellung).	
1.5 Sind sonstige allgemeine Regelungen zur Daten- und Programmsicherheit vorhanden?	
• Regelung des Zutritts über eine Schlüsselverwaltung.	
• Regelungen, die geschlossene Fenster, Türen (nach Dienstschluss) einfordern.	

Fragestellungen/Maßnahmen	Sachstand, Risikobeurteilung
• Regelungen bzw. Vereinbarungen zur Telearbeit (falls vorhanden).	
• Nutzungsverbot nicht freigegebener Hard- und Software (z.B. privater USB-Stick, Spiele, usw.).	
• Aus- und Weiterbildung des Personals im Bereich Informationstechnik und Sicherheit (Schulungskonzept).	
• Archivierungskonzept (mit Angaben wie lange die Daten im DV-System aufbewahrt werden, ob sie nach einem bestimmten Zeitraum „ausgelagert" werden - z.B. Ausdruck, Mikrofiche, CD-ROM - und wie insgesamt sichergestellt wird, dass die gesetzlichen Aufbewahrungsfristen eingehalten werden).	
• Löschkonzept (wie lange werden welche Daten im DV-System vorgehalten).	
2 Technische und bauliche Maßnahmen	
2.1 Sind der Rechner- bzw. Netzwerkbetrieb sowie die Anwendung ausreichend sicher und die Zugriffskontrollen ausreichend?	
• Protokollführung der Zugriffe, der Fehlversuche und unerlaubten Zugriffsversuche (Betriebssystem- bzw. Anwendungsebene).	
• Einsatz von Virenschutzprogrammen und einer Firewall.	
2.2 Ist ein Datensicherungskonzept vorhanden?	
• Regelmäßige Datensicherungen; welche Daten (alle oder nur Teile davon), werden wann (z.B. automatisiert nachts) auf welche Datenträger (z.B. Bänder) gesichert; Durchführen von Tages-, Monats- und Jahressicherungen (3-Generationenprinzip).	
• Auslagern von Datenbeständen.	
2.3 Werden der Rechnerraum, das Datenträgerarchiv usw. speziell geschützt?	
• Der Rechnerraum sollte nicht für jeden erkennbar (z.B. keine Beschilderung) und nicht für jedermann zu erreichen sein (z.B. nicht neben dem Bürgerbüro).	
• Verwendung „besonderer" (stabiler) Schließzylinder, Sicherheitsschlösser, installierte Sicherheitstüren (Feuer- und Rauchschutztüren), Sicherheitsfenster (nicht einfach auszuhebeln), Scheiben aus Spezialglas / Gitter vor Fenster, Rolladensicherungen, Schutzschrank für Datenträger, spezielle (zusätzliche) Sicherung des Rechnerraums / Archivs (z.B. Ausweisleser).	
• Keine Lagerung brennbarer Materialien.	
• Überwachung der Temperatur und Luftfeuchtigkeit, vorhandene Klimaanlage.	
• Schutz vor Spannungsabfall, unterbrechungsfreie Stromversorgung (USV), regelmäßiger Test und Wartung der USV, vorhandener Überspannungsschutz.	

Fragestellungen/Maßnahmen	Sachstand, Risikobeurteilung
• Besteht eine erhöhte Gefahrenlage für die Rechnerausstattung durch Ver- und Entsorgungsleitungen in oder in der Nähe des Rechnerraums (Wasserrohrbruch, Abwasserrückstau)?	
2.4 Werden regelmäßig „Wartungsarbeiten“ an Programmen durchgeführt?	
• Dokumentation der Wartungsarbeiten (wer hat wann, welche Updates zum Betriebssystem, zur Anwendungssoftware eingespielt).	
• Sichere Fernwartungszugänge (falls vorhanden), z.B. über Kennwort und Callback (automatischer Rückruf).	
2.5 Ist bei Schulungen, Besprechungen usw. gewährleistet, dass Unberechtigte keinen Zugriff auf sensible Daten erhalten?	
• Räumliche Abtrennung des Schulungsbereichs, kein Zugriff vom Schulungs-PC (o.ä.) auf das (gesamte) interne Netz oder das Internet.	
• Sichere Konfiguration der Rechner (kein Administratorzugang, kein Zugriff auf Diskettenlaufwerk, USB-Anschluss, usw.).	
2.6 Sind Sensoren für bestimmte Gefahren installiert (Gefahrenmeldeanlage)?	
• Automatische Feuermelder, Rauchmelder, Wassermelder, Einbruchmelder.	
2.7 Sind die Ver- und Entsorgungsleitungen ausreichend gesichert?	
• Lagepläne von Ver- und Entsorgungsleitungen.	
• Physische Sicherung von Kabeln (Kabelschächte durch Schloss, Verlegung unter Putz), gekennzeichnete Kabel (Art, Nutzung, usw.).	