gpa Baden-Württemberg
Kommunale Prüfung und Beratung

GPA-Mitteilung 13/2006

Az. 912.15

01.12.2006

Sicherheitsanforderungen beim Online-Banking

Die Kommunen nutzen zunehmend die von Kreditinstituten angebotenen Möglichkeiten zur Abwicklung des unbaren Zahlungsverkehrs über „elektronische" Zahlungsverfahren (Online-Banking). Dabei ist vor allem für die Zahlungen über das Internet die notwendige Kassensicherheit zu gewährleisten. Das kommunale Kassenrecht enthält zwar keine besonderen Regelungen für das Online-Banking (Abwicklung von Bank- bzw. Zahlungsgeschäften über PC, Laptop oder z.B. auch Smartphones), dennoch sind nachfolgende Sicherheitsaspekte zu beachten.

Grundsatz der Einheitskasse

Durch § 93 GemO ist die Organisationsfreiheit der Gemeinden gesetzlich dahingehend beschränkt, dass grundsätzlich sämtliche Kassengeschäfte bei der Gemeindekasse abzuwickeln sind. Weitere verbindliche Rahmenvorgaben zur Aufbau- und Ablauforganisation der Gemeindekasse enthält die Gemeindekassenverordnung (GemKVO), für deren Umsetzung entsprechend den örtlichen individuellen Verhältnissen und Verantwortlichkeiten eine Dienstanweisung empfohlen wird (örtliche Dienstanweisung für die Gemeindekasse). Die Abwicklung des (baren und) unbaren Zahlungsverkehrs gehört auch bei Nutzung des Online-Banking zum Kernbereich der Kassengeschäfte mit einer strikten Bindung dieser Aufgaben an die Kassenbediensteten (§ 93 Abs. 1 GemO; § 1 Abs. 1 i.V. mit § 12 Abs. 2 GemKVO).

Zugangsschutz

Dem Grundsatz der Kassensicherheit (§ 5 Abs. 1 GemKVO) kommt bei der Gemeindekasse besondere Bedeutung zu. Die Abwicklung des (unbaren) Zahlungsverkehrs muss deshalb so gestaltet sein, dass über die zu diesem Zweck von ihr zu verwaltenden Konten keine

Gemeindeprüfungsanstalt Baden-Württemberg
76133 Karlsruhe · Hoffstraße. 1a · Telefon 0721 / 8 50 05 - 0
70193 Stuttgart · Klopstockstraße 35 · Telefon 0711 / 6 36 71 - 0

Unbefugten verfügen oder auf diese zugreifen können. Das bedeutet, dass die für das Online-Banking eingesetzte Hard- und Software mit einem wirksamen Zugangsschutz versehen sein muss. Anregungen und Informationen hierzu bietet z.B. der IT-Grundschutz-Katalog des Bundesamts für Sicherheit in der Informationstechnik (Teil M4 Maßnahmenkatalog Hardware und Software).[1]

„Vier-Augen-Prinzip“

Beim Zahlungsverkehr ist als wesentlicher Sicherheitsaspekt das Vier-Augen-Prinzip in Form der Doppelunterschrift bzw. entsprechender elektronischer Signaturen vorgeschrieben (§ 5 Abs. 2 GemKVO). Elektronische Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die der Authentifizierung dienen (z.B. ein elektronischer Doppelunterschriftersatz in Form zweiter Geheimnummern als Unterschriftssurrogat zweier[!] Bediensteter oder elektronische Unterschriften mittels jeweils zweier Unterschriftsdisketten). Damit ist nicht ausschließlich ein Verfahren nach dem Signaturgesetz vorgeschrieben. Vielmehr geht es allgemein um einen elektronischen Unterschriftsersatz, der in jedem Einzelfall auch noch nachträglich eine eindeutige und unverwechselbare Identifizierung des jeweils Handelnden ermöglichen muss. Dieser Ansatz kommt gerade bei der Abwicklung von Kassengeschäften per Online-Banking z.B. mit PIN/TAN-Autorisierung zum Tragen. Bei diesem besonderen Verfahren sind für den Zugang zum Konto neben der Konto- oder Kundennummer die geheime PIN (Personal Identification Number) und für Transaktionen (z.B. Überweisungen) zusätzlich eine TAN (Transaktionsnummer) anzugeben. Die Forderung nach einer Doppelunterschrift bzw. entsprechenden Surrogaten richtet sich als Konsequenz des Grundsatzes der Einheitskasse ausdrücklich an Kassenbedienstete. Ist die Gemeindekasse nicht ständig mit zwei Bediensteten besetzt, spricht gerade bei Abwicklung des Zahlungsverkehrs per Online-Banking nichts dagegen, zur Sicherstellung des Vier-Augen-Prinzips auch „Nichtkassenbedienstete“ heranzuziehen. Ein Alleinzugriff von Nichtkassenbediensteten ist aber stets auszuschließen (z.B. des Bürgermeisters oder des Fachbediensteten für das Finanzwesen).

Trennungen von Anordnung und Vollzug

Durch die (personelle) Trennung von Anordnung und Vollzug (§ 6 Abs. 3 GemKVO; keine Kassenanordnung durch Kassenbedienstete) wird ein hohes Maß an Sicherheit in der Ab-

[1] Internet-Adresse: http://www.bsi.de.

wicklung der Geldgeschäfte bzw. des Zahlungsverkehrs erreicht (z.B. Ausschluss von „Selbstanweisungen“ und „Selbstauszahlungen“). Dem dient auch der grundsätzliche Ausschluss der Kassenbediensteten von der Feststellungsbefugnis (§ 10 Abs. 3 GemKVO). Bei ausschließlicher Kenntnis der PIN (quasi als „Hauptzugang“ zum Geschäftskonto der Gemeindekasse) durch Kassenbedienstete sind die vorgenannten Trennungsvorgaben und Sicherheitsaspekte wirksam umgesetzt. Eine zusätzliche Sicherheit kann ggf. noch dadurch erreicht werden, dass kassenintern die Bereiche Buchführung und Zahlungsverkehr getrennt werden (s. frühere Nr. 4 VwV-GemKVO zu § 5)[1]. Abgesehen davon sollte durch gelegentliche Änderungen der PIN (z.B. anlässlich von Vertretungsfällen) die Kassensicherheit erhöht werden. Bei einem Personalwechsel sollte die PIN auf jeden Fall geändert werden. Die für den Vertretungsfall im Online-Banking eingerichteten Einzelberechtigungen sind ebenfalls stets an den o.g. Sicherheitsaspekten auszurichten.

Sicherheit des Übertragungswegs

Eine Gefahr zufälliger oder absichtlicher Verfälschung der Daten besteht im Zusammenhang mit dem Übertragungsweg im Internet von der Kasse zum Kreditinstitut. Auf die unterschiedlichen Sicherheitsstandards (und evtl. Risikozuweisungen) in den Geschäftsbedingungen der Kreditinstitute ist vorab zu achten. Hierzu wird auch auf die Information „Online-Banking-Sicherheit“ des Bundesverbandes Deutscher Banken (6. Aufl. Berlin, Sept. 2006) verwiesen.[2] Online-Banking wird in Deutschland fast nur noch über das Internet angeboten. Hierfür wird als Online-Banking-Standard auf FinTS (Financial Transaction-Services) bzw. HBCI (Home Banking Computer Interface) aufgebaut. FinTS bzw. HBCI bietet verschiedene Möglichkeiten der Authentisierung. Die Absicherung erfolgt meist über das PIN/TAN-System. Eine Alternative ist die Absicherung des Online-Banking über eine Chipkarte. Diese Methode gewährleistet einen sehr hohen Sicherheitsstandard, denn es wird sowohl die Kundenidentifizierung abgesichert als auch die Übertragung der Daten[3].

---

[1] In einem Kassenrechtsentwurf zum NKHR BW wird dieser Trennungsaspekt übrigens wieder aufgegriffen.

[2] Internetadresse: http://www.Bankenverband.de.

[3] Vgl. dazu Band 10 der Schriftenreihe zur IT-Sicherheit [Sicherheitsaspekte bei Electronic Commerce] des Bundesamts für Sicherheit in der Informationstechnik (abrufbar unter http://www.bsi.de).

Zusammenfassung

Das Kassenrecht enthält für Sicherheitsfragen im Zusammenhang mit der Zahlungsabwicklung per Online-Banking zwar nur allgemein gehaltene Vorschriften. Sie sind aber zur Gewährleistung der Kassensicherheit beim Einsatz unterschiedlichster Zahlungsverkehrsvarianten und –techniken geeignet, wenn sie **entsprechend eingehalten** werden. Dies hat die Kommune in eigener Verantwortung sicherzustellen.

SG 30/2