Orientierungshilfe

zum datenschutzgerechten Anschluss an Internet und Online-Banking
bei Gerichtsvollzieherinnen und Gerichtsvollziehern

November 2004

Arbeitskreis „Technische und organisatorische Datenschutzfragen“
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Gerichtsvollzieherinnen und Gerichtsvollziehern wollen vermehrt das Internet und moderne Kommunikationsdienste nutzen. Dabei ist jedoch zu bedenken, dass IT-Systeme mit einem Internet-Anschluss von außen angreifbar werden. Gerichtsvollzieherinnen und Gerichtsvollzieher sind gesetzlich verpflichtet, sich gegen solche Gefahren und möglichen Angriffe zu schützen. Hierfür ist eine sichere Trennung von lokalen Rechnern und externen Systemen erforderlich. Für diese Trennung bieten sich folgende Alternativen an:

- **Installation einer Firewall**
  Diese technische Einrichtung trennt das externe Netzwerk von der lokalen Installation. Hierfür sind jedoch erhebliche Aufwendungen in Hard- und Software erforderlich. Darüber hinaus erfordert der Einsatz von Firewall-Technik umfangreiche Kenntnisse und Erfahrungen in der Installation, Wartung und Pflege die eingesetzten Hard- und Software. Weiter sind wirksame Absicherungen gegen unerwünschte Kommunikationsinhalte zu treffen. Neben der Firewall sind ergänzende Sicherheitsmaßnahmen erforderlich. Beispielsweise sollten für die Sachbearbeitung und für die Internet-Nutzung getrennte Benutzerkonten verwendet werden.

- **Verwendung eines Einzelplatzsystems**
  solche Einzelplatzsysteme sind zu empfehlen, wenn eine aufwendige Sicherungstechnik die Finanzen und die Kenntnisse der Gerichtsvollzieherinnen und Gerichtsvollzieher übersteigt Es könneneinfache und preiswerte Personalcomputer eingesetzt werden, weil bei diesen Systemen in der Regel ausschließlich die Internetverbindung hergestellt wird, um beispielsweise Online-Banking zu nutzen. Auch bei einem Internet-PC mit dieser eingeschränkten Verwendung ist eine Grundsicherung erforderlich.[1] Dazu gehört auch die Installation und Konfiguration einer Personal-Firewall.

Was ist bei einem Anschluss an das Internet zu beachten?

- Wählen Sie einen vertrauenswürdigen Access-Provider.
- Halten Sie Zugangskennung und das zugehörige Passwort geheim.
- Speichern Sie die Zugangskennung und das zugehörige Passwort nicht auf dem Rechner ab.
- Nutzen Sie möglichst sichere Browser und Mail-Programme.
- Konfigurieren Sie Browser und Mail-Programme richtig.[2]
- Speichern Sie keine Nutz(er)daten auf dem Internet-Zugangssystem.
- Speichern Sie keine sensiblen personenbezogenen Daten unter der Kennung, mit der Sie im Internet surfen.

[1] BSI-Grundschutzhandbuch unter: *http://www.bsi.bund.de/gshb/deutsch/menue.htm*
[2] PC-Selbsttest unter: *http://www.lfd.niedersachsen.de/master/0,,C27776_N13210_L20_D0_I560,00.html*

Was sollten Sie beim E-Mail-Dienst beachten?

- Um das unbefugte Lesen und Verändern der E-Mail-Inhalte zu verhindern, sollten Sie eine Verschlüsselungssoftware, z. B. PGP oder GnuPG, einsetzen. Beachten Sie, dass sensible personenbezogene Daten per E-Mail nur in verschlüsselter Form übertragen werden dürfen.

- Damit Ihre E-Mail auf dem Weg zum Empfänger nicht unbemerkt gelöscht oder verloren geht, sollten Sie mit dem Empfänger eine Empfangsbestätigung vereinbaren.

- Vergewissern Sie sich beim Absender von E-Mails mit angehängten, ausführbaren Dateien (z. B. *.exe, *.bat, *.com, *.vbs, *.scr), ob die Dateien tatsächlich von ihm stammen.

- Wenn Sie sichergehen möchten, dass auch der angegebene Absender wirklich der Verfasser der E-Mail ist und dass keine Veränderung oder Verfälschung am Inhalt oder Absender vorgenommen wurde, dann verwenden Sie eine digitale Signatur.

- Beachten Sie, dass bei den meisten E-Mail-Programmen gelöschte E-Mails zunächst in einen „Papierkorb“ verschoben und erst beim Leeren dieses Papierkorbs endgültig gelöscht werden. Deshalb sollten Sie Ihren E-Mail-Papierkorb regelmäßig leeren.

- Geben Sie Ihre E-Mail-Adresse nicht an jeden weiter. Damit verringern Sie die Gefahr, dass Sie mit Spam-E-Mail belästigt werden.

- Virenwarnungen mit der Aufforderung, sie weiter zu versenden, sollten Sie ungeöffnet löschen und nicht den „gutgemeinten“ Anweisungen folgen.

Wie schützen Sie sich an Ihrem APC vor einen Virenbefall?

- Um einen Virenbefall an Ihrem Arbeitsplatz-PC zu verhindern, sind alle Disketten, CD-ROMs oder andere Datenträger, die Sie für Ihren Aufgabenbereich benötigen, auf Virenbefall zu überprüfen.

- Suspekte E-Mail, z. B. mit einer offensichtlich unsinnigen Betreffzeile, sollten Sie sofort ungeöffnet löschen, auch wenn die Absenderadressen Ihnen bekannt sind.

- Sie sollten auch misstrauisch werden, wenn Betreffzeilen Wörter wie happy, fun usw. enthalten.

- E-Mails sollten Sie immer mit einem aktuellen Virenschutzprogramm überprüfen bzw. vom Administrator prüfen lassen.

- Nutzen Sie für den Internetzugang und die Mailfunktion möglichst keine Kennung, die über Administratorrechte verfügt.

Was ist bei Online-Banking besonderes zu beachten?

Online-Banking-Dienste werden in unterschiedlicher Ausprägung angeboten; sowohl als traditionelle PIN/TAN Variante als auch in der Form der HBCI-Abwicklung. Im Hinblick auf eine höchstmögliche Sicherheit wird der HBCI-Standard (Home Banking Computer Interface) unter Verwendung einer Chipkarte und eines Lesegerätes der Klasse 3 empfohlen. Im Folgenden finden Sie einige wesentliche Hinweise zu einem datenschutzgerechten Umgang mit Online-Banking:

- Die Gerichtsvollzieherin bzw. der Gerichtsvollzieher ist für die ordnungsgemäße Erledigung der Dienstgeschäfte bei der Anwendung des Online-Banking verantwortlich.
- Die für die Zugangsberechtigung und Auftragsfreigabe erforderliche Persönliche Identifikations-Nummer (PIN) darf nur dem verfügungsberechtigten Gerichtsvollzieher und seiner nach § 49 Nr. 2 GVO buchführungsberechtigten Bürohilfe bekannt sein.
- Chipkarte und PIN hat der Gerichtsvollzieher stets getrennt voneinander und sicher aufzubewahren, so dass sie anderen Personen nicht zugänglich sind. Die PIN darf nicht im IT-System hinterlegt werden. Sie sollte in regelmäßigen Abständen geändert werden.
- Die Chipkarte darf nur solange in das Lesegerät eingelegt werden wie der HBCI-Dialog geführt wird. Bei Verdacht auf Missbrauch ist der Zugang sofort zu sperren.
- Es ist technisch sicherzustellen, dass nach Absenden der Daten keine Veränderungen bei einzelnen Überweisungen vorgenommen werden können, beispielsweise durch Zugangs- und Zugriffskontrolle.
- Speichern Sie keine PIN und TAN auf dem Rechner.