BUNDESRECHTSANWALTSKAMMER

beA Digital. Einfach. Sicher.

beA – sicher
Die Sicherheitsarchitektur des beA

Rechtsanwalt Christopher Brosch, Rechtsanwältin Peggy Fiebig, BRAK, Berlin

Berlin, 03.06.2015

Auf Grund des durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten in die BRAO eingefügten § 31a richtet die Bundesrechtsanwaltskammer zum 1. Januar 2016 für jeden Rechtsanwalt und jede Rechtsanwältin ein besonderes elektronisches Anwaltspostfach (beA) ein. Spätestens im Jahr 2022 verpflichtet das Gesetz überdies auch zur aktiven Nutzung des elektronischen Rechtsverkehrs. Entsprechend den gesetzlichen Voraussetzungen wurde das beA mit einem besonders hohen Sicherheitsstandard entwickelt: Die Nachrichtenübertragung und auch das Postfach selbst sind gegen unbefugte Zugriffe geschützt.

Die Enthüllungen von Edward Snowden über die Aktivitäten verschiedener Geheimdienste, Berichte über Computerspionage im Deutschen Bundestag und auch die neuen Pläne zur Einführung einer Vorratsdatenspeicherung haben zu Fragen im Hinblick auf die Sicherheit elektronischer Kommunikation geführt. Nachfolgend soll daher ein Überblick über die Sicherheitsarchitektur des beA gegeben werden.

Ende-zu-Ende-Verschlüsselung

Entscheidend für die Vertraulichkeit der Übertragung von Nachrichteninhalten im beA ist eine durchgehende („Ende-zu-Ende“) Verschlüsselung – vom Webbrowser bzw. der Kanzleisoftware des Absenders bis zur Entschlüsselung durch den Empfänger. So gibt es keine Zwischenstationen, in denen die Nachrichten im Klartext vorliegen.

Verschlüsselt werden die zu übertragenden Nachrichten durch eine Kombination aus einem symmetrischen und einem asymmetrischen Verschlüsselungsverfahren. Beim symmetrischen Verfahren erfolgen Ver- und Entschlüsselung mit ein und demselben Schlüssel, der nicht öffentlich gemacht und deshalb auch nicht ungeschützt dem Empfänger übertragen werden darf. Bei der asymmetrischen Verschlüsselung dagegen werden zwei Schlüssel – ein öffentlicher und ein privater – benötigt. Mit dem öffentlichen Schlüssel wird verschlüsselt, mit dem privaten entschlüsselt.

Da asymmetrische Verschlüsselungsverfahren erheblich mehr Rechenleistung benötigen und dadurch deutlich langsamer sind, wird beim beA die Nachricht selbst symmetrisch verschlüsselt, und lediglich der dazu verwendete Nachrichtenschlüssel wird asymmetrisch chiffriert.

Die Entschlüsselung der Nachrichten erfolgt dann direkt auf dem Computer des Empfängers. Von dieser Ende-zu-Ende-Verschlüsselung ausgenommen sind lediglich einzelne für den Nachrichtentransport erforderliche Metadaten wie die Angabe des Absender- und des

Empfängerpostfachs. Aber auch diese Informationen werden bei der Übertragung durch das Internet mit einer Transportverschlüsselung geschützt und in verschlüsselten Datenbanken abgelegt.

Sichere Rechteverwaltung

Zur Abbildung einer Kanzleiorganisation aus mehreren Rechtsanwälten sowie Mitarbeitern stellt das beA eine umfassende Rechteverwaltung zur Verfügung, die es dem Postfachinhaber u.a. ermöglicht, anderen Personen Zugriff auf Nachrichten in seinem Postfach zu gewähren. Hierfür kommt ein sogenanntes Hardware Security Modul (HSM) zur Anwendung. Ein HSM ist ein Gerät, das nur spezielle, vorab definierte kryptographische Funktionen ausführen kann und das gegen jede Art der Manipulation sowie gegen Abhören geschützt ist.

Durch das HSM wird der verschlüsselte Nachrichtenschlüssel nach Prüfung der Berechtigung für einen Leser – Mitarbeiter oder Postfachinhaber – „umgeschlüsselt"; dieser kann ihn anschließend mit seinem privaten Schlüssel entschlüsseln und mit dem nun im Klartext vorliegenden Nachrichtenschlüssel die Nachricht entschlüsseln. Durch Einsatz des HSM kann eine Nachricht im beA mehreren Personen zum Lesen bereitgestellt werden, ohne dass sie zu irgendeinem Zeitpunkt unverschlüsselt im System vorliegt. Die Standorte der beA-Rechenzentren einschließlich der HSM befinden sich in Deutschland – der genaue Ort wird als eine weitere Sicherheitsmaßnahme nicht öffentlich genannt.

Sicherer als Post und Fax

Es lohnt sich, im Vergleich zu der Nachrichtenübermittlung im beA einen kurzen Blick auf die anderen Kommunikationswege mit der Justiz, die bisher zur Verfügung stehen, zu richten: Ein gewöhnliches Telefax wird unverschlüsselt über öffentliche Telefonnetze übertragen; eine Kenntnisnahme Dritter kann daher nicht ausgeschlossen werden. Das Öffnen eines Briefes durch Dritte hinterlässt in der Regel zwar Spuren – einen Schutz gegen ein unbefugtes Lesen bietet der Papierbrief jedoch nicht. Absolute Vertraulichkeit ist nur schwer zu erreichen. Das gilt auch für das beA. Doch so viel steht fest: Gegenüber der Kommunikation mittels Telefax oder Brief bedeutet das beA einen gewaltigen Sprung nach vorn.

Doppelt hält besser

Lediglich ein Schutz der Datenübertragung wäre nicht ausreichend zur Gewährleistung der Vertraulichkeit. Auch vor und nach Ende der Datenübertragung zwischen zwei Postfächern müssen unberechtigte Zugriffe auf das beA verhindert werden. Entsprechend der gesetzlichen Vorgaben ist für den Zugriff auf das beA eine sichere Anmeldung unter Verwendung zweier voneinander unabhängiger Sicherungsmittel erforderlich. Durch diese sogenannte Zwei-Faktor-Authentifizierung wird ein weit höheres Maß an Sicherheit erreicht als lediglich durch ein Passwort.

Vorgesehen ist, dass für jeden Zugriff auf das beA neben einer PIN (Wissen) entweder eine Chipkarte oder ein Softwarezertifikat (Besitz) verwendet werden muss. Dies gilt für Rechtsanwälte und – nach der Vergabe der entsprechenden Berechtigungen – für Mitarbeiter gleichermaßen. Für Rechtsanwälte bietet es sich an, eine Chipkarte mit Signaturfunktion zu erwerben, denn nur so ist nicht nur der Zugriff auf das Postfach, sondern auch der Versand von Nachrichten möglich: Das ERV-Gesetz sieht bis Ende 2017 vor, dass Dokumente, die elektronisch bei Gericht eingereicht werden, qualifiziert elektronisch signiert sein müssen. Ab 2018 entfällt dieses Erfordernis, wenn die Dokumente vom Rechtsanwalt selbst (nicht von einem Mitarbeiter oder Vertreter) aus seinem beA-Postfach versandt wurden. Auch hierfür ist dann für die Anmeldung eine Chipkarte erforderlich, ein Softwarezertifikat wird voraussichtlich nicht genügen.

Wo Anwalt draufsteht, ist Anwalt drin

Damit sichergestellt wird, dass nur Rechtsanwälte ein beA besitzen, ist eine von der BRAK herausgegebene beA-Karte erforderlich, die jeder Rechtsanwalt und jeder Rechtsanwältin aus diesem Grund erwerben muss (Näheres zum Bestellverfahren siehe gegenüberliegende Seite). Die Karte enthält die eindeutige Bezeichnung des Postfachs und wird dem Rechtsanwalt bzw. der Rechtsanwältin getrennt von der dazugehörigen PIN übermittelt. Nur so lässt sich eine sichere Zuordnung eines Postfachs zum jeweiligen Besitzer gewährleisten. Zugleich wird das Risiko eines Missbrauchs von Zugangsinformationen ausgeschlossen, denn nur die Benutzung von Karte und PIN ermöglichen den Zugriff auf ein Postfach. Selbst wenn eine Karte bei ihrem Versand abgefangen würde, fehlt die getrennt versandte PIN.

Das beA basiert auf einem sicheren Verzeichnisdienst, der von der Bundesrechtsanwaltskammer betrieben wird. Nur wer hier eingetragen ist, wird ein beA-Postfach erhalten. Gespeist wird der Verzeichnisdienst aus den elektronischen Registern der Rechtsanwaltskammern nach § 31 Absatz 1 BRAO. Diese Daten werden in einem sicheren Verfahren von den Rechtsanwaltskammern an die Bundesrechtsanwaltskammer übertragen – eine elektronische Signatur der Rechtsanwaltskammer schließt dabei Manipulationen bei der Übertragung aus.

Das beA ermöglicht eine Kommunikation nur mit definierten und in die Verzeichnisse eingetragenen Postfächern. Während bei der E-Mail-Kommunikation die angezeigte E-Mail-Adresse sowie der Name frei bestimmt werden können und man sich daher – sofern nicht zusätzlich eine qualifizierte elektronische Signatur verwendet wird – nie sicher sein kann, dass der Kommunikationspartner, Absender oder Empfänger einer Nachricht, der ist, der er zu sein scheint, gilt beim beA: Wo Anwalt drauf steht, ist auch Anwalt drin.

Geht nicht, gibt’s nicht

Für die anwaltliche Tätigkeit ist eine ununterbrochene Verfügbarkeit des beA-Systems von großer Bedeutung. Systemausfälle müssen verhindert werden und dürfen gerade auch kurz vor Ablauf eines Tages nicht vorkommen. Bereits bei der Konzeption wurde daher Wert darauf gelegt, dass technische Störungen, die sich nie vollständig ausschließen lassen werden, möglichst keine Auswirkungen auf den Betrieb des beA haben: Das beA-System wird in zwei örtlich getrennten Rechenzentren betrieben. An beiden Orten befindet sich dieselbe Hard- und Software. Eines der Rechenzentren dient dem aktiven Betrieb, eines dient der Ausfallsicherheit. Zusätzlich sind auch in jedem der beiden Rechenzentren Redundanzen vorhanden, die die Last und das Ausfallrisiko verteilen. So sind etwa an jedem der beiden Standorte zwei HSM installiert.

Ergebnis

Plakativ ausgedrückt: Das beA ist sicher. Die BRAK stellt jedem Rechtsanwalt und jeder Rechtsanwältin ein höchsten Anforderungen genügendes Kommunikationssystem zur Verfügung. Ein wesentlicher Baustein der IT-Sicherheit ist jedoch auch das Verhalten der Anwender. Die dargestellten Maßnahmen verlieren an Wert, wenn etwa unberechtigte Personen Zugriff auf beA-Karte und PIN haben oder das beA von einem Computer (etwas in einem öffentlichen Internetcafé) genutzt wird, bei dem das Vorhandensein von Viren und Spionagesoftware nicht ausgeschlossen werden kann.