Wie sicher ist das beA?

Das besondere elektronische Anwaltspostfach (beA) aus Sicht der IT-Sicherheit

Kurz vor den Weihnachtsfeiertagen des vergangenen Jahres musste die Bundesrechtsanwaltskammer das beA wegen Sicherheitsproblemen vom Netz nehmen. Hintergrund war, dass der IT-Sicherheitsexperte Markus Drenger vom Chaos Computer Club an den privaten Schlüssel eines Zertifikats aus der beA-Client-Software gelangt war. Dieses musste daraufhin von der zuständigen Registrierungsstelle aufgrund der selbst auferlegten Richtlinien zurückgezogen werden. Den Richtlinien zufolge müssen Zertifikate, deren privater Schlüssel nicht mehr im alleinigen Besitz des Inhabers ist, widerrufen werden. Als kurzfristige Problembehebung tauschte die BRAK daraufhin das Zertifikat aus und veröffentlichte die Empfehlung, ein selbstsigniertes Zertifikat des Dienstleisters und beA-Entwicklers Atos zu installieren. Durch dieses Vorgehen sollte verhindert werden, dass ein neues Zertifikat noch einmal widerrufen wird. Das zugrundeliegende Problem, dass ein globaler, privater Schlüssel mit dem beA-Client an alle Nutzer verteilt wurde, wurde jedoch nicht gelöst. Zu allem Übel handelte es sich bei dem selbstsignierten Zertifikat um ein sog. Root-Zertifikat. Dieses ermöglicht es dem Inhaber des privaten Schlüssels, also jedem Nutzer des beA-Clients, beliebige weitere Zertifikate für Webseiten auszustellen. Ein Angreifer wäre damit unter anderem in der Lage gewesen, betroffenen Rechtsanwälten eigene, manipulierte Webseiten als vertrauenswürdig auszuweisen. Nachdem dieses massive Sicherheitsproblem bekannt wurde, zog die BRAK die Anleitung daher zurück und empfiehlt richtigerweise, allen Rechtsanwälten das Zertifikat schnellstmöglich zu deinstallieren. Ausgehend von diesen Vorgängen, die auch als "beAgate" bezeichnet werden, ist allgemein eine Debatte über die IT-Sicherheit des beA entbrannt. Dabei geht es längst nicht mehr alleine um die geschilderte Problematik um das Zertifikat, sondern auch um grundsätzliche Fragen der beA-Architektur, wie u.a. die Sicherheit der Ende-zu-Ende-Verschlüsselung.

Der Vortrag beleuchtet ausgehend von den Vorfällen rund um den Widerruf des Zertifikats der beA Client-Security die IT-Sicherheit des beA. In diesem Rahmen sollen zunächst die Vorgänge rund um die Weihnachtsfeiertage kritisch aufgearbeitet werden. Daran anknüpfend wird der Vortrag der Frage nachgehen, ob und inwieweit weitere Sicherheitsrisiken beim beA bestehen.

Referenten:

Stefan Hessel (Dipl.-Jur.) ist akademischer Mitarbeiter bei der juris-Stifungsprofessur für Rechtsinformatik und dem Center for IT-Security, Privacy and Accountability (CISPA) an der Universität des Saarlandes. Außerdem ist Stefan Hessel Geschäftsführer der Defendo GbR – Möllers & Hessel, die Unternehmen in IT-Sicherheitsfragen berät.

Weitere Informationen: stefan.legalinf.de und www.defendo.it

Frederik Möllers (M.Sc.) ist wissenschaftlicher Mitarbeiter bei der juris-Stiftungsprofessur für Rechtsinformatik und dem Center for IT-Security, Privacy and Accountability (CISPA) an der Universität des Saarlandes. Er ist ebenfalls Geschäftsführer der Defendo GbR – Möllers & Hessel, die Unternehmen in IT-Sicherheitsfragen berät.

Weitere Informationen: frederik.legalinf.de und www.defendo.it