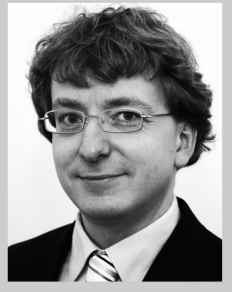
Das doppelte Versagen der BRAK beim beA



RA Matthias Bergt, Berlin

Nein, ein Informatikstudium braucht es hier wirklich nicht. Es reicht etwas gesunder Menschenverstand, um zu sehen: Das besondere elektronische Anwaltspostfach (beA), wegen schwerer Sicherheitsprobleme seit Weihnachten vom Netz, darf in seiner aktuellen Form nie wieder online gehen. Und vor einem Neustart muss sich grundlegend etwas ändern. Technisch. Rechtlich. Kommunikativ. Denn die Bundesrechtsanwaltskammer (BRAK) hat nicht nur technisch versagt, sondern auch im Umgang mit den Fehlern des beA.

Das Wichtigste ist: Der Schutz des Anwaltsgeheimnisses darf nicht mehr in der Hand von mehr oder offensichtlich eher weniger kompetenten IT-Dienstleistern liegen – das beA muss Open Source werden. Dazu gehören ein Bug-Bounty-Programm mit Belohnungen für die Meldung von Sicherheitslücken und ein professionelles vollständiges White-Box-Sicherheits-Audit.

Doch der erste Grundfehler des beA liegt schon darin, einer berufsständischen Vertretung wie der BRAK nicht nur den Betrieb, sondern sogar die Entwicklung eines komplexen und hohen Sicherheitsanforderungen unterliegenden Systems zu überantworten. An solchen Projekten scheitern ganz andere – aber Juristen können ja alles.

Der zweite Grundfehler war offensichtlich die Auswahl der IT-Partner: Um zu erkennen, dass das beA in seinem aktuellen System-Design nicht sicher sein kann, braucht man ebenfalls kein Informatikstudium. IT-Basiswissen und eine grobe Systembeschreibung reichen: Verschlüsselung im Browser ist nur so sicher wie die Website sicher und der Betreiber vertrauenswürdig ist. Und wenn man, wie das beA, einen lokalen WWW-Proxy mit öffentlichem Zertifikat zwischenschaltet, ist das System broken by design.

Dennoch hat der IT-Dienstleister so ein schon im Ansatz unsicheres System gebaut und in Betrieb genommen. Berücksichtigt man, dass der Hersteller auf das wegen Sicherheitsproblemen gesperrte offizielle Zertifikat mit einer hochgefährlichen Bastel-Lösung reagiert hat, die mit keiner IT-Policy vereinbar ist, stellt sich sogar die Frage, ob wirklich nur grobe Unfähigkeit vorliegt – oder ob hier nicht gar vorsätzlich Schrott geliefert wurde, in der Erwartung, es werde schon niemand merken. Ging ja offenbar schon beim Sicherheits-Audit so: Zwar hält die BRAK auch hier fast alles geheim, und das, was sie dazu sagt, ist allenfalls mit großem Wohlwollen noch als missverständlich zu bezeichnen – aber klar scheint jedenfalls, dass es der Hersteller war, der das Audit beauftragt hat und dafür gesorgt hat, dass der Auditor gar nicht so genau hinschauen kann.

Letzteres führt zum dritten Grundfehler: der Kommunikation. Sicherheitsprobleme zu vertuschen, indem ein gesperrtes Zertifikat als „abgelaufen“ bezeichnet wird und das beA als wegen „vereinzelter Verbindungsprobleme“ abgeschaltet, geht gar nicht. Zwar scheint es, dass die BRAK tatsächlich einfach keinen Schimmer hatte, was beim beA IT-technisch los ist, und vom Dienstleister an der Nase herumgeführt wurde. Doch auch nachdem ihr das ganze Ausmaß des Desasters bekannt war, blieb die BRAK beim Abwiegeln und Vertuschen. Vertrauen in den beA-Betreiber? Wird schwierig.

Aber gerade das unbedingte Vertrauen in die technische Sicherheit des beA und die Integrität des Betreibers ist unabdingbar. Das beginnt mit dem Vertrauen darein, dass die beA-Software keine Sicherheitslücken in die Anwalts-Rechner reißt – woran aktuell erhebliche Zweifel bestehen, liefert der beA-Client doch hoffnungslos veraltete Software-Bestandteile mit – und geht über eine sichere Umsetzung der Verschlüsselungs- und Signaturfunktionen bis zu einer sicheren Gestaltung und vertrauenswürdigen Handhabung des Hardware-Sicherheits-Moduls im Rechenzentrum. Dieses Hardware-Sicherheits-Modul, das bislang nicht im öffentlichen Fokus stand, hat es nämlich auch noch mal in sich: Hier liegen die privaten Schlüssel aller Anwälte. Wer Zugriff auf das Hardware-Sicherheits-Modul hat, befugt oder unbefugt, kann also jede beA-Nachricht lesen. Anders als immer auch von der BRAK öffentlich behauptet, gibt es beim beA eben keine Ende-zu-Ende-Verschlüsselung: Zwar bleibt die Nachricht an sich verschlüsselt gespeichert, aber das beA kann umschlüsseln, um dem Vertreter oder Sekretariat des Anwalts auch rückwirkend Zugriff auf die Nachrichten geben zu können. Zudem konnte die BRAK bisher nicht erklären, wie der private Schlüssel auf die beA-Karte des Anwalts kommt und die Kopie ins Hardware-Sicherheits-Modul im Rechenzentrum. Auch hier sind Angriffe denkbar.

Das beA braucht absolute Transparenz – von Client über Server und Schnittstellen bis hin zu Hard- und Software von beA-Karte und Hardware-Sicherheits-Modul im Rechenzentrum. Und in der Kommunikation. Ob das mit dem aktuellen BRAK-Präsidium und den aktuellen IT-Partnern gelingt? Das darf man getrost bezweifeln. Auch ohne Informatikstudium.