Original-URL des Artikels: https://www.golem.de/news/bea-das-anwaltspostfach-kommt-mit-sicherheitsluecken-1809-136346.html
Veröffentlicht: 03.09.2018 10:00 **Kurz-URL:** https://glm.io/136346

BeA

Das Anwaltspostfach kommt mit Sicherheitslücken

Das besondere elektronische Anwaltspostfach (BeA) soll am heutigen Montag wieder starten. Es war seit Dezember vergangenen Jahres aufgrund zahlreicher Sicherheitslücken offline. Nach wie vor sind viele Fragen in Sachen Sicherheit ungeklärt.

Nachdem es acht Monate offline war, soll das besondere elektronische Anwaltspostfach (BeA) heute wieder online gehen. Doch weiterhin gibt es ungeklärte Fragen in Sachen Sicherheit. Das BeA ist ein System der Bundesrechtsanwaltskammer (Brak), über das Rechtsanwälte und Justizbehörden verschlüsselt miteinander kommunizieren können. Eigentlich war vorgesehen, dass Anwälte ab Januar 2018 darüber ihre Nachrichten empfangen müssen. Doch daraus wurde nichts. Aufgrund schwerwiegender Sicherheitslücken wurde das BeA am 23. Dezember abgeschaltet.

Als Reaktion auf die zahlreichen Sicherheitslücken hat die Brak die Firma Secunet beauftragt, die Sicherheit des BeA zu prüfen. Inzwischen wurde ein Gutachten als Ergebnis dieser Prüfung veröffentlicht, an vielen Stellen bleibt es jedoch vage. Sowohl Secunet als auch die Brak verweigern Auskünfte über die Details der Sicherheitslücken.

Im Gutachten von Secunet werden die gefundenen Schwachstellen in verschiedene Risikokategorien eingeteilt. Die schwersten Lücken wurden als Kategorie A oder als *"betriebsverhindernde"* Probleme bezeichnet. In einem zusammen mit dem Gutachten veröffentlichten Begleitschreiben kündigte die Brak an, das BeA werde nur wieder online gehen, wenn Secunet bestätige, dass alle Probleme der Kategorie A behoben seien.

Betriebsbehindernde Sicherheitslücke bleibt bestehen

Eine dieser Lücken - im Secunet-Gutachten unter Punkt 5.4.1 zu finden - ist jedoch nach wie vor nicht geschlossen, da dies ohne eine grundlegende Änderung der Softwarearchitektur des BeA nicht möglich ist. Das BeA ist als Javascript-basierte Webanwendung realisiert. Die Webanwendung wird von einem Server der Brak - erreichbar unter bea-brak.de - geladen und kommuniziert dann mit der sogenannten Client Security, einer Software auf dem lokalen PC.

Das Problem bei dieser Konstruktion: Ein Angreifer, der Zugriff auf den Server der Brak hat, könnte jederzeit eine andere Anwendung ausliefern und beispielsweise den Javascript-Code so ändern, dass er den entschlüsselten Inhalt der Nachrichten an Dritte weiterleitet.

Das bedeutet letztendlich, dass ein Innentäter jederzeit Zugriff auf verschlüsselte Nachrichten erlangen kann, wenn er gezielt einen BeA-Nutzer angreifen will. Damit erübrigen sich auch alle bisherigen Diskussionen über die Frage der Sicherheit des Hardware-Sicherheitsmoduls (HSM) und einer möglichen Ende-zu-Ende-Verschlüsselung, um die es viel Streit gab und zu der auch noch eine Klage läuft.

Verhindern ließe sich ein solcher Angriff nur, wenn die Anwendung komplett lokal laufen würde. Doch eine solche Änderung ist nicht vorgenommen worden und wäre in dem kurzen Zeitraum wohl auch nicht umsetzbar gewesen. Trotzdem hat laut Aussage der Brak Secunet dem BeA nun seinen Segen gegeben. Auf

mehrfache Nachfragen von Golem.de konnte die Brak nicht erklären, wie sie dieses grundlegende Problem beheben will.

In einer Pressemitteilung dazu heißt es: *"Hinsichtlich der Schwachstelle 5.4.1 erklärt Secunet, dass man sich durch ein zusätzliches Quelltext-Audit davon überzeugt habe, dass zu keiner Zeit Zugriff auf den Klartext der vertraulichen Nachrichtenanhänge bestand. Die Schwachstelle stellt nach Auffassung von Secunet in dieser Form kein Hindernis mehr für eine Wiederinbetriebnahme des BeA dar."*

Brak sieht Lücke als behoben an, kann aber nicht erklären, warum

Was diese Erklärung aussagen soll, bleibt unklar. Ein Quelltext-Audit ist hier irrelevant, da das Angriffsszenario ja davon ausgeht, dass ein Angreifer den Code jederzeit verändern kann. Wir haben mehrfach vergeblich versucht, von der Brak eine Erklärung dafür zu erhalten, warum sie dort davon ausgeht, dass dieses Problem behoben ist.

Kurz vor Inbetriebnahme des BeA sah sich die Rechtsanwaltskammer jedoch nicht in der Lage, Fragen zur Technik des BeA zu beantworten. *"Inhaltlich brauche ich für Ihre Antwort Input aus unserer Technik-Abteilung"*, schrieb uns die Pressesprecherin der Brak, Stephanie Beyrich, auf Anfrage. *"Sie werden verstehen, dass derzeit alle dortigen Mitarbeiter mit den Vorbereitungen für die Wiederinbetriebnahme ausgelastet sind. Ich habe nochmals an Ihr Anliegen erinnert, rechne aber nicht damit, dass in dieser Woche eine Antwort möglich sein wird."*

Veraltete Verschlüsselung in OSCI

Doch das ist längst nicht das einzige Problem. Ende Juli hat die Frankfurter Allgemeine Zeitung (FAZ) berichtet, dass es beim Schließen einer Lücke in der Verschlüsselung wohl ein Koordinierungsproblem mit dem EGVP gibt. Das EGVP ist ein älteres Justiz-Kommunikationssystem, das mit dem BeA über den OSCI-Standard kommunizieren kann.

OSCI ist ein recht alter Standard, die letzte Version 1.2 wurde im Jahr 2002 veröffentlicht. Dementsprechend finden sich darin zahlreiche uralte Verschlüsselungsverfahren. Die Brak schwieg sich über Details des Problems aus, aber aus den bekannten Informationen lässt sich schließen, dass das System offenbar RSA im Padding-Modus PKCS #1 1.5 einsetzt und für einen sogenannten Bleichenbacher-Angriff verwundbar war.

Behoben werden sollte das durch einen Umstieg auf das modernere OAEP-Verfahren, doch diese Umstellung muss noch etwas warten, da ein gleichzeitiger Umstieg im EGVP stattfinden muss.

Das RSA-Padding-Verfahren ist nicht die einzige fragwürdige, veraltete Verschlüsselungskonstruktion in OSCI. Im originalen OSCI-Standard wird eine XML-Verschlüsselung mit dem sogenannten CBC-Modus beschrieben. Dies gilt eigentlich schon lange als unsicher, da CBC ein nicht authentifizierter Modus ist und Nachrichten somit nicht gegen Modifikation geschützt sind. Insbesondere stellt sich hier auch die Frage, ob OSCI und damit das BeA verwundbar für einen Angriff wie Efail wäre.

Optional lässt sich OSCI wohl inzwischen auch mit dem authentifizierten GCM-Verfahren verwenden. Daher hätten wir gerne gewusst, ob das BeA GCM bereits nutzt. Doch auch diese Frage hat uns das Brak nicht beantwortet.

BeA-Installer unter Linux stürzt ab

Einige Anwälte haben Golem.de berichtet, sie hätten Probleme mit der BeA-Installation mit Firefox und generell unter Linux gehabt. Diese Probleme betreffen offenbar nicht alle Anwender, wir konnten sie jedoch

in einem Test nachvollziehen.

Da das BeA mit einem lokalen HTTPS-Server kommuniziert, muss dafür ein Zertifikat im Browser installiert werden. In einem Test von uns mit einer frischen Windows- und Firefox-Installation wurde das Zertifikat dabei zwar im Windows-eigenen Zertifikatsspeicher abgelegt, nicht jedoch in Firefox - der Mozilla-Browser nutzt einen eigenen Zertifikatsspeicher.

Die Linux-Installation wird offiziell laut Brak nur unter der inzwischen schon über zwei Jahre alten Ubuntu-Version 16.04 unterstützt. Doch ein Test von uns bestätigte, was uns auch ein Anwalt mitteilte: Die Installationsroutine brach unter Ubuntu 16.04 mit einem Absturz ab.

Generell nicht unterstützt wird vom BeA Microsofts Edge-Browser. Den Anwendern von Edge empfiehlt die Brak, auf den inzwischen veralteten Internet Explorer zurückzugreifen. Gleichzeitig schreibt die Brak aber auch im Widerspruch dazu: *"Es wird empfohlen, immer die aktuelle Version der Browser zu verwenden, da von den Herstellern fortlaufend Sicherheitslücken geschlossen werden."*

BeA kommt mit veralteter Java-Version

Bei der Untersuchung der Probleme des Installers ist uns eine weitere Sache aufgefallen: Das Installationsprogramm ist offenbar schon länger nicht aktualisiert worden - die Dateien tragen ein Datum vom Februar 2018. Die BeA-Software selber wird dabei immer aktuell von einem Server aus dem Netz gezogen, doch falls auf dem System noch kein Java installiert ist, wird eine mit dem Installer mitgelieferte Version verwendet.

Das mitgelieferte Java trägt die Versionsnummer 1.8.0_161 und wurde im Januar veröffentlicht. Seither gab es mehrere Java-Sicherheitsupdates, das BeA läuft also mit einer Java-Version mit bekannten Sicherheitslücken.

Niemand muss mit dem BeA Nachrichten verschicken

Trotz Sicherheitslücken und Installationsproblemen: Für Rechtsanwälte gilt, dass sie das BeA ab sofort nutzen müssen. Zwischenzeitlich war diskutiert worden, ob man für eine Übergangsphase die Nutzungspflicht aussetzen kann, das lehnte das Justizministerium jedoch ab.

Allerdings gilt die Nutzungspflicht bislang nur passiv. Das bedeutet, dass Anwälte zwar übers BeA Nachrichten empfangen müssen, sie sind aber nicht verpflichtet, das System selbst zur aktiven Kommunikation zu nutzen. Die Gesellschaft für Freiheitsrechte, die zurzeit gegen das BeA klagt, empfiehlt daher: *"Die Gefahren für die Datensicherheit lassen sich auch bannen, indem einfach niemand das unsichere beA nutzt."* (hab)

Verwandte Artikel:
Bundesrechtsanwaltskammer: Sicherheitsgutachten zum Anwaltspostfach enttäuscht
(22.06.2018, https://glm.io/135104)
Ende-zu-Ende-Verschlüsselung: Klage gegen Anwaltspostfach eingereicht
(18.06.2018, https://glm.io/134984)
EGVP: Empfangsbestätigungen einer Klage sind verwertbar
(26.03.2018, https://glm.io/133520)
BeA: Secunet findet noch mehr Lücken im Anwaltspostfach
(29.03.2018, https://glm.io/133601)
Skype: Ende-zu-Ende-Verschlüsselung bei Skype ist verfügbar