ReTests der beA-Client-Security Schwachstellen zu Abschnitt 3.5.4 und 5.4.1 aus dem Gutachten vom 18.6.2018

Kapitel 3.5.4, S. 36 - Veraltete Softwareelemente

Die in der beA-Client-Security (Release 3.1.3.8) verwendeten Drittbibliotheken wurden im Internet auf Schwachstellen hin recherchiert. Hierbei zeigte sich, dass die meisten in der beA-Client-Security genutzten Drittbibliotheken in der aktuellsten Version genutzt werden. Für einzelne Drittbibliotheken existieren bereits wieder neuere Versionen. Deren zeitnahe Einbindung ist jedoch bei einem kurzen Update-Zyklus im Entwicklungsprozess nicht immer realistisch umsetzbar. Für einige der Softwarebibliotheken wurden auch in der aktuellsten Version Schwachstellen gefunden, deren Ausnutzbarkeit im Kontext der beA-Anwendung eingeschätzt wurde. Hier konnten keine kritischen Schwachstellen mit Bedrohung für den beA-Client-Security identifiziert werden. Bei der Prüfung der identifizierten potentiellen Schwachstellen handelt es nach Abstimmungen mit den Hersteller um „False-Positive"-Schwachstellen, da beispielsweise Fehler in der Beschreibung vorlagen oder die betroffenen Bibliotheken nicht verwendet werden.

Somit konnten in der neuen von der BRAK übermittelten beA-Client-Security zu den in der Anwendungsoberfläche aufgeführten verwendeten Drittbibliotheken als auch in einer Betrachtung der tatsächlichen *.jar Dateien (Source-Code) keine sicherheitsrelevanten Schwachstellen identifiziert werden, welche eine Bedrohung für die beA-Client Security oder den Anwalts-PC darstellen. Bei den identifizierten potentiellen Schwachstellen handelt es sich nach Informationen durch den Hersteller um „False-Positive"-Schwachstellen, da beispielsweiße Fehler in der Beschreibung vorlagen. Aus Sicht von secunet unter Betrachtung der Softwareaktualität, kann die beA-Client-Security Release 3.1.3.8 wieder zum Download durch die BRAK bereitgestellt werden.

Kapitel 5.4.1, S. 80 - Verwendung von JavaScript

Dem Gutachter ist mitgeteilt worden, dass die im Gutachten dargestellte Schwachstelle in Abschnitt 5.4.1, die Verwendung von JavaScript zur Steuerung der beA-Client-Security, entgegen der Aussagen im Feinkonzept zur beA-Client-Security, einem Angreifer nicht die Anhänge einer Nachricht im Klartext preisgeben kann. Anhänge werden nur im Ciphertext an die beA-Anwendung übergeben oder von ihr übernommen. Bei der Verschlüsselung wird der Klartext eines Anhangs nur innerhalb der beA-Client-Security von der Festplatte gelesen, verarbeitet und in verschlüsselter Form an die beA-Anwendung übertragen. Bei der Entschlüsselung eines Anhangs wird ebenfalls der Klartext nur innerhalb der beA-Client-Security ermittelt und als Datei auf dem Anwalts-PC abgelegt.

Es besteht noch die Gefährdung, dass ein Angreifer einem Versender eine simulierte beA-Client-Security-GUI anbietet, und dann die Upload-Funktionalität des Browsers nutzt, um den Klartext einer Datei an ein gewünschtes Ziel zu übertragen. Dieser Angriff würde aber rasch bemerkt werden, da die so „versendete“ Nachricht im beA-System nicht auftaucht, was auch der Versender zeitnah feststellen kann. Unter anderem deswegen wird weiter an der Forderung eines wirksamen Integritätsschutz der JavaScript-Seiten festgehalten.

Der Gutachter hat sich per Quelltext-Audit der beA-Client-Security in der Version 3.1.3.8 davon überzeugt, dass diese Angaben zutreffen und an keiner Stelle Antworten an das beA-System oder die JavaScript-Komponente generiert werden, die Anhänge im Klartext enthalten. Nur der eigentliche Nachrichtentext (fachlich gesehen das Anschreiben an den Adressaten) wird im Klartext mittelbar in die JavaScript-Komponente übermittelt bzw. mit ihrer Hilfe erzeugt (Texteingabemaske).

Die beA-Client-Security verwendet beim Versenden auch einen eigenen Auswahldialog für die Bestimmung der verschlüsselt zu versendenden Dateianhänge, der in dieser Form nicht von JavaScript nachgebildet werden kann. Dem Nutzer kann der Angreifer hier nicht durch böswilliges JavaScript eine Verwendung der beA-Client-Security vortäuschen und dann auf die ausgewählten Dateien über eine Browserfunktion zugreifen, um sie auf ein Ziel seiner Wahl im Klartext hochzuladen.

Die BRAK stuft den Schutzbedarf dieses begleitenden Nachrichtentextes hinsichtlich Vertraulichkeit aus fachlicher Sicht als deutlich geringer ein als den Schutzbedarf der Anhänge. Das führt dazu, dass aus fachlicher Sicht der mögliche Schaden auch bei massenhafter Kompromittierung dieser Begleittexte nicht mehr als hohe, sondern nur noch als mittlere Bedrohung eingestuft wird. Das Risiko dieser Schwachstelle wird dadurch von Kategorie A auf Kategorie B geändert. Die Schwachstelle stellt in dieser Form kein Hindernis mehr für eine Wiederinbetriebnahme des beA dar. Die weitere Bearbeitung der Schwachstelle wird gemäß den Hinweisen und Anforderungen des Gutachters zum Integritätsschutz der JavaScript-Seiten erfolgen.

Hinsichtlich der Schwachstelle 5.4.1 wurde durch den Quelltext-Audit festgestellt, dass zu keiner Zeit Zugriff auf den Klartext der vertraulichen Nachrichtenanhänge besteht. Darüber hinaus wurde festgestellt, dass durch den von der BRAK kommunizierten neuen Schutzbedarf des Nachrichtentextes, die hier genannte Schwachstelle in dieser Form kein Hindernis mehr für eine Wiederinbetriebnahme des beA darstellt.