Starke Authentifizierung beim Beraterfrontend

Mit digitalen Zertifikaten zu einer sicher(er)en Alternative zu Nutzername/Passwort

Christoph Becker

Zugriff auf schützenswerte Daten sollen nur die NutzerInnen erhalten, die ihre Identität hinreichend beweisen können und denen zuvor entsprechende Zugriffsrechte eingeräumt wurden. IT-Systeme für die zentrale elektronische Verwaltung von Nutzerdaten (Identitätsmanagementsystem) unterliegen dabei einem besonderen Schutz, da hierin eine Vielzahl personenbezogener Daten verarbeitet werden. Aufgrund der weitreichenden Zugriffsberechtigungen sind die Nutzerkonten der KIM-BeraterInnen bevorzugte Angriffsziele. Der notwendigen Konsequenz bei der korrekten Gestaltung und dem verantwortungsvollen Gebrauch von Zugangsdaten kommt daher eine entscheidende Rolle zu, wenn es darum geht, unbefugtes Lesen, Kopieren, Verändern oder Löschen der Daten zu verhindern.
Doch der De-Facto-Standard einer Nutzername-Passwort-Kombination zur Anmeldung an IT-Diensten birgt in der Praxis bekanntermaßen die Gefahr, dass Angreifer über verschiedene Wege versuchen können, an die Passwörter der privilegierten Nutzerkonten zu gelangen. Aus diesem Grund wird empfohlen, bei besonders schützenswerten Zugängen eine zweite Barriere neben dem Passwort einzurichten (Zwei-Faktor-Authentifizierung).
Als zweiter Faktor eignen sich persönliche digitale Zertifikate, die die KIM-BeraterInnen seit Ende Oktober 2016 zusätzlich zum persönlichen Passwort bei der Anmeldung am Identitätsmanagementsystem aka Beraterfrontend benötigen. Ein digitales Zertifikat meint eine Datei, die bestimmte Angaben über den Inhaber (z.B. seinen Namen, die Zugehörigkeit zur Universität Konstanz und seine E-Mail-Adresse) bestätigt und durch kryptografische Verfahren für IT-Systeme nachprüfbar macht.

Diese Zertifikat-Passwort-Kombination kompensiert dabei entscheidende Nachteile des klassischen, passwortbasierten Verfahrens: Zum einen genügt das Erraten oder Ablauschen des Passwortes oder das Stehlen des Zertifikats allein noch nicht, um unautorisiert auf den Datenbestand zugreifen zu können. Das heißt, wenn einer der Faktoren fehlt, wird der Zugang verweigert. Zum anderen haben (im Gegensatz zu selbst gewählten Passwörtern) alle Nutzerzertifikate ein gleichmäßiges, sehr hohes Sicherheitsniveau.
Hat der Nutzer[1] das Zertifikat wie empfohlen auf einer speziellen Hardware-Komponente (Krypto-Token) gespeichert, ist es optimal geschützt. Er hat so, analog zu physikalischen Zutrittssystemen, seinen „Schlüssel“ direkt in der Hand und der Verlust wird ihm i. d. R. auffallen. Doch selbst bei Diebstahl oder Verlust des Tokens wird die unautorisierte Verwendung des Zertifikats durch ein weiteres persönliches Passwort verhindert.

1 Wegen der besseren Lesbarkeit wurde in diesem Absatz auf eine gendergerechte Schreibweise verzichtet.