WHITEPAPER

IT-Sicherheit dank Open Source

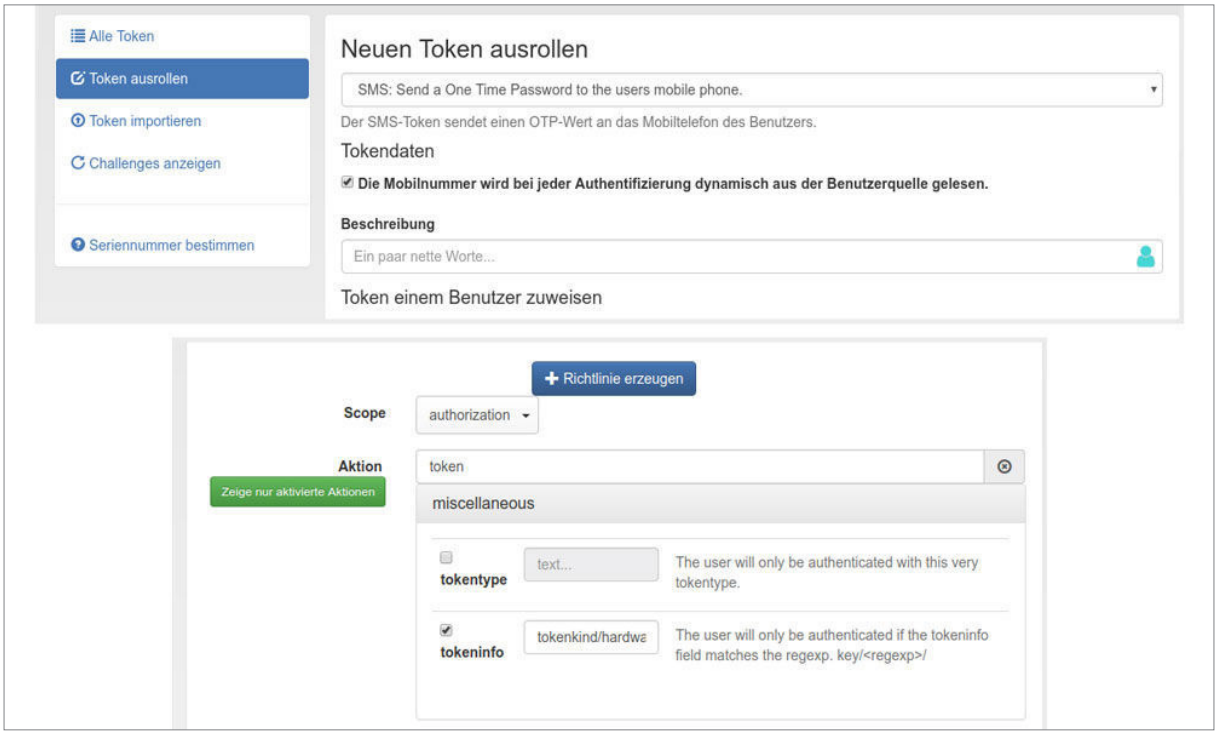
Eine Zwei-Faktor-Authentifizierung gilt als effektives Verfahren, den Zugang zur Krankenhaus-IT zu schützen. Oft kommt dabei eine kommerzielle Software zum Einsatz, die nicht selten mit weniger Kontrolle und höheren Gesamtkosten einhergeht. Manchmal droht zudem der Fall einzutreten, dass eine gekaufte Software plötzlich nicht mehr weiterentwickelt wird. Das Klinikum Hanau nahm so einen Fall zum Anlass, künftig auf die quelloffene 2-Faktor-Authentifizierungslösung „privacyIDEA“ zu setzen.

Um den Zugang zu kritischen Informationen wie Patienten- und Mitarbeiterdaten zu schützen, gilt die Authentifizierung mit zwei Faktoren als eine der effektivsten und am schwersten zu hackenden Verfahren. Deren wichtigstes Merkmal ist die Anmeldung eines Nutzers durch zwei voneinander unabhängige Komponenten für einen zweifelsfreien Identitätsnachweis, z.B. durch ein Passwort in Verbindung mit einem externen Token (Schlüssel), der einen zufälligen Code generiert.

Das Klinikum Hanau nutzte in den vergangenen Jahren eine lizenzierte – sogenannte proprietäre – Authentifizierungslösung eines kommerziellen Herstellers. Dieser entschied sich Anfang 2018, den Support für die Software einzustellen. In der Folge wurden keine Updates mehr entwickelt und die Software wurde langfristig unbrauchbar. Durch den geschützten Code hatte die IT-Abteilung zudem keine Möglichkeit, die Software selbst weiterzuentwickeln oder anzupassen. Darüber hinaus wurde vom Hersteller die Ausgabe weiterer Tokens eingestellt. Neue Benutzer konnten nicht mehr in das bestehende System aufgenommen werden. Der Zwei-Faktor-Authentifizierung des Klinikums fehlte plötzlich der zweite Faktor.

Beim Umstieg bestanden im wesentlichen zwei Hauptanforderungen: Ein unterbrechungsfreier Übergang sowie die Möglichkeit, künftig flexibel neue Authentifizierungstoken hinzufügen zu können. Bei der Suche nach einer passenden Lösung fiel die Wahl des Klinikums Hanau auf die 2-Faktor-Authentifizierung privacyIDEA, deren Abrechnungsmodell keine Lizenzierung jedes einzelnen Nutzers vorsieht, sondern ein gestaffeltes Service Level Agreement, bei dem der Preis nicht sofort mit jedem neuen Nutzer ansteigt.

Durch die sogenannte „sanfte Migration” der NetKnights GmbH, die die quelloffene Lösung entwickelte, kann das Backend, in dem die Authentifizierungsanfragen bearbeitet werden, in wenigen Minuten ausgetauscht und angepasst werden, ohne dass die Nutzer irgendetwas davon bemerken. Außerdem erhalten nur jene Nutzer neue Token, die nach dem Wechsel auf das neue System hinzukommen. Alte Schlüssel bleiben weiter aktiv, was zusätzliche Kosten spart. Wer ein neues Authentifizierungsgerät in Betrieb nimmt, muss sich nur noch mit dem neuen Gerät anmelden – ohne weitere notwendige Schritte und mit minimalem Aufwand.



Mit Open-Source-Lösungen wie „privacyIDEA“ können neue Nutzer flexibel hinzugefügt werden, ohne dass höhere Lizenzgebühren anfallen.

„Mit dem Wechsel zu einer Open-Source-basierten Lösung haben wir nachhaltig einen Vendor-Lock-In vermieden. Das verständliche Support-Modell der NetKnights GmbH ermöglicht uns außerdem eine langfristige Planungssicherheit“, resümiert Hüseyin Gökceoglu, als IT-Leiter hauptverantwortlich für die Umsetzung des Projektes.

Mit privacyIDEA lässt sich – zusammenfassend gesagt – eine ansonsten langwierige und arbeitsintensive Umstellung auf ein neues System maximal vereinfachen. Und die IT-Sicherheit langfristig in die eigenen Hände nehmen.

Cornelius Kölbel, Gründer und Geschäftsführer der NetKnights GmbH: „Gerade für Krankenhäuser, die mit sensiblen, personenbezogenen Daten arbeiten, kann eine auf offenem Quellcode basierende Lösung eine gute Alternative sein. Die Krankenhaus-IT erhält damit langfristig die volle Kontrolle über sämtliche Daten, Accounts und Logins und macht sich damit unabhängig von kommerziellen Herstellern.“

NetKnights GmbH, Ludwig-Erhard-Str. 12,
D-34131 Kassel, +49 561 3166 797,
info@netknights.it, www.netknights.it