Keycloak und privacyIDEA

Chemnitzer Linux-Tage 2020

Cornelius Kölbel <cornelius.koelbel@netknights.it>

2FA und Single Sign-On

Keycloak ist ein Single Sign-On Identity Provider. Web-Anwendungen können über die Protokolle SAML oder OpenID Connect an Keycloak angebunden werden, um ein Single Sign-On bei der Benutzeranmeldung zu realisieren.[1]

Die Anmeldung mit Single Sing-On wird für den Benutzer einfacher, für die IT-Sicherheit aber auch problematischer. Ist die eine Anmeldung überwunden, so hat ein potentieller Angreifer Zugriff auf alle angebundenen Applikationen. Eine Zwei-Faktor-Authentifizierung ist hier also das Mittel der Wahl.

Die Stärken von dedizierten Systemen

Auch wenn Keycloak bereits eine integrierte 2FA-Funktionalität mitbringt, empfiehlt es sich, einen Blick auf einen Ansatz zu werfen, der über die Möglichkeiten, die Keycloak bietet, hinausgeht.

Genau wie Keycloak haben auch andere Applikationen wie ownCloud, Nextcloud, FreeIPA, Django, Wordpress u.v.m. bereits Zwei-Faktor-Funktionen mit an Bord. Doch gerade in Setups mit größeren Benutzerzahlen bietet ein dediziertes Zwei-Faktor-System gegenüber integrierten Lösungen entscheidende Vorteile.

Wie nicht zuletzt auch der Vortrag zum Telematik-Hack auf dem Chaos Communication Congress zeigte[2], ist es nicht nur entscheidend im Falle von Identitäten und Authentifizierung technisch sichere Umsetzungen zu haben, sondern auch einen organisatorische Sicherheit zu gewährleisten. So sind beispielsweise Workflows wie der initiale Rollout eines zweiten Faktors oder der Ersatz bei Verlust eines Authentifizierungsmerkmals entscheidend für die Gesamtsicherheit des Systems.

Ein professionelles Zwei-Faktor-Management-System wie privacyIDEA[3] ermöglicht es Organisationen und Unternehmen, solche Workflows genau auf ihre Bedürfnisse hin passend zu definieren.

[1] https://keycloak.org
[2] https://www.ccc.de/de/updates/2019/neue-schwachstellen-gesundheitsnetzwerk
[3] https://privacyidea.org

Setup von Keycloak und privacyIDEA

Mit Hilfe des *Keycloak PriacyIDEA Plugins*[4] kann Keycloak mit dem unternehmenstauglichen Zwei-Faktor-System "privacyIDEA" verbunden werden. Genau wie Keycloak läuft privacyIDEA on Premises an einem zentralen Ort im eigenen Netzwerk. Auf diese Weise stehen dem Administrator alle Management- und Workflow-Funktionen von privacyIDEA zur Verfügung, um die zweiten Faktoren der Benutzer zu verwalten. Darüber hinaus können auch alle verschiedene, von privacyIDEA unterstützte Token-Typen verwenden, wie Registrierungscodes, Yubikeys, U2F oder sogar die Authentifizierung über PUSH-Benachrichtigungen.

Über den Vortrag

In dem Vortrag auf den Chemnitzer Linuxtagen werden die Vorzüge von dedizierten 2FA-Systemen gegenüber intergrierten 2FA-Ansätzen erarbeiten. Nach einer kurzen Einführung in Keycloak und privacyIDEA, zeigen wir, welche Möglichkeiten sich konkret aus der Kombination von Keycloak mit dem flexiblen privacyIDEA ergeben. Schließlich lassen sich nicht nur die Logins besser absichern, sondern auch alle notwendigen Workflows einfach und robust abbilden.

[4] https://github.com/privacyidea/keycloak-provider