Überblick: privacyIDEA

privacyIDEA ist ein Open Source-Projekt (AGPLv3) zur starken Authentifizierung. Es hat seine Wurzeln in der Zwei-Faktor-Authentifizierung mittels Einmal-Passwörtern (OTP). Als zentrales System greift es auf bestehende Benutzerdatenbanken (LDAP, AD, SQL, Flat file, SCIM) zu und kann für all diese Benutzer Authenisierungs-Devices als zweiten Faktor verwalten. Beliebige Applikationen wie VPN, Webseiten, Desktop-Login u.v.m. können über entsprechende Schnittstellen (REST, RADIUS, SAML, PAM...) an privacyIDEA angebunden werden. Der Benutzer kann sich nun mit seinen zentral verwalteten zwei Faktoren an diesen Applikationen anmelden.

Innovation

Zwar ist mit OATH (HOTP/TOTP) ein Standard geschaffen, über den OTP-Token diverser Hersteller austauschbar sein sollen, doch unterstützen kommerzielle Hersteller wie SafeNet oder Vasco mit ihrer Management-Software (SafeNet Authentication Manager, Vasco Identikey) vor allem ihre eigenen Hardware. Weiterhin versuchen Hersteller die Kunden dadurch zu binden, dass Authentifizierung nicht mehr on-premise sondern als Service in der Cloud angeboten wird. Eine Nutzung anderer Authentisierungs-Devices, einer anderen Anmelde-Technologie oder eine Migration zu einem anderen Anbieter ist nicht mehr möglich.

privacyIDEA gibt dem Unternehmen die **Kontrolle zurück**. Es ist dafür gemacht, on-premise betrieben zu werden und kann Authentisierungs-Token beliebiger Hersteller in jeglicher Kombination verwalten. Außerdem ermöglicht es leichte Migrationen zu privacyIDEA hin – und wenn gewünscht – auch wieder von privacyIDEA weg. Ein Vendor Lock-In ist somit verhindert.

privacyIDEA geht den Schritt von einem reinen OTP-Server hin zur **Verwaltungsinstanz für jegliche Authentifizierungsinformationen**. So können heute schon SSH-Keys zentral verwaltet und X.509-Zertifikate ausgestellt werden. Eine Offline-OTP-Anmeldung an Clients ist möglich. privacyIDEA verwaltet Yubikeys, um mit diesen als zweiten Faktor LUKS verschlüsselte Notebooks zu booten.

In Zukunft wird die Unterstützung des Nitrokey als Open-Hardware Authentisierungs-Device folgen. Die Verwaltung von Smartcards oder Verschlüsselungskeys ist denkbar.

Über den Namen privacyIDEA

Mit privacyIDEA können Authentifizierungsinformationen für Benutzer verwaltet werden, um die Benutzer zu identifizieren (**ID**). Neben der reinen Authentifizierung können innerhalb von privacyIDEA auch Zugangsregeln definiert werden (Autorisierung). Ein digital signiertes Audit Log ermöglicht den Einblick in alle durchgeführten Aktionen → Authentifizierung, Autorisierung, Audit (**3A**) → **ID3A**.

Auch im Bereich der Authentifizierung ist seit geraumer Zeit zu beobachten, dass immer mehr Cloud-Dienste genutzt werden und der Authentifizierungsprozess für die Unternehmen intransparenter wird. Gleichzeit werden wie bei RSA SecurID oder FIDO U2F-Devices vorinitialisierte Geräte verwendet, bei denen der Hersteller das geheime Schlüsselmaterial geliefert hat und ggf. noch weiterhin besitzt. privacyIDEA unterstützt aber auch diverse Geräte, bei denen der Anwender oder das Unternehmen selber das Schlüsselmaterial erzeugt (**privacy**). → **privacyID3A**.

Nutzen für die Anwender

Der prinzipielle Nutzen besteht in der Sicherung der Zugänge und Daten durch die Verwendung eines flexiblen, zweiten Faktors. privacyIDEA ist ein Lösung, die sich an größere Benutzergruppen wendet. Daher kann der Nutzen für die Organisation selber und die Endanwender betrachtet werden.

Administratoren, Helpdesk und die Organisation

Im Gegensatz zu herkömmlichen OTP-Lösungen ist privacyIDEA durch seine REST-API in Workflows integrierbar, anpassbar und automatisierbar. Die Arbeit der Administratoren und Helpdesk-Mitarbeiter wird dadurch erheblich erleichtert. Bestehende Token können i.d.R. weiterverwendet werden.

Authentisierungs-Devices unterschiedlicher Hersteller können nebeneinander verwendet werden. Dies ist für

Cornelius Kölbel, cornelius.koelbel@netknights.it +49 561 3166797

unterschiedliche Benutzergruppen interessant oder wenn sich die Organisation über Ländergrenzen hinweg erstreckt und keine zentrale Beschaffung möglich ist.

Hilfe finden der Administrator in der ausführlichen öffentlichen Dokumentation, in der Google Group oder durch Abschluss eines professionellen SLAs.

Endanwender

Wenn der Administrator dies zulässt, kann der Endanwender das Gerät oder die Authentisierungsmethode wählen, die am besten zu ihm passt. In einem aufgeräumten, sehr einfach gestaltetem Web Interface kann der Endanwender die von dem Administrator freigeschalteten Aufgaben selbst durchführen.

Technischer Hintergrund

privacyIDEA ist eine Web-Applikation und kommuniziert über eine REST-API. Für unterschiedliche Applikationen stehen Plugins zur Verfügung. Basierend auf dem Python-Framework „Flask“ ermöglicht es sehr schnelle Entwicklungszyklen.

Das Projekt privacyIDEA nutzt konsequent Github und andere freie Dienste, um Transparenz und zuverlässigen Code zu gewährleisten (Travis-CI, Circle-CI, Codecov, QuantifiedCode...). Durch die komplette Transparenz des Entwicklungsprozesses auch zwischen einzelnen Releases zeichnet es sich auch gegenüber anderen Lösungen aus.

Durch die konsequente Nutzung von Python-typischen Programmier-Strukturen wie bspw. „Decorators“, wird eine verhältnismäßig kleine Code-Basis erreicht (17.500 Zeilen des Servers), die die Entwicklung und Pflege nachhaltig erleichtert.

Reifegrad

privacyIDEA ist ein Fork von LinOTP, das seit 2010 verfügbar ist. In 2014 erfuhr privacyIDEA ein Rewrite, so dass es nun auf modernen Technologien wie dem Flask-Framework und AngularJS basiert. Durch den Rewrite konnte wie oben erwähnt die Code-Basis bei größerer Funktionalität mehr als halbiert werden. privacyIDEA ist produktiv einsetzbar. Es wird u.a. von Anwendern in U.S.A., U.K., Deutschland, Italien, Russland, Australien produktiv im Unternehmensumfeld betrieben. Die bekannte größte Installation mit 35.000 Benutzern an einer deutschen Universität befindet sich gerade in der Pilot-Phase.

Links und Beispiele

Projektlinks

Projektwebseite: https://privacyIDEA.org

Github-Repository: https://github.com/privacyidea/privacyidea

Ausführliche Dokumentation: http://privacyidea.readthedocs.io/en/latest/

Google Group: https://groups.google.com/forum/#!forum/privacyidea

FAQs: http://privacyidea.readthedocs.io/en/latest/faq/index.html

Beispiele

Anwendungsszenarien wie

- Zugriff für Außendienstmitarbeiter https://netknights.it/loesungen/aussendienstmitarbeiter/,
- Anmeldung am Windows-PC https://netknights.it/loesungen/sichere-anmeldung-am-windows-pc/,
- Kundenportal https://netknights.it/loesungen/sicherer-zugriff-ihrer-kunden/,
- SSH-Key-Management https://netknights.it/loesungen/sichere-administration-der-serverfarm/,
- Online-Banking https://netknights.it/loesungen/modernes-online-banking/,
- Leichte Migration https://netknights.it/einfacher-umstieg-von-proprietaerem-otp-system-nach-offenem-privacyidea/.

Cornelius Kölbel, cornelius.koelbel@netknights.it +49 561 3166797