

Vortrag - Kurzpapier

Created Donnerstag 15 Dezember 2011

Über LinOTP

LinOTP ist eine innovative und flexible Lösung zur Zweifaktorauthentisierung.

LinOTP ist auf python und dem pylons web framework aufgebaut. Dank der modularen Architektur ist LinOTP herstellerunabhängig und unterstützt beliebige Authentisierungsprotokolle, Token und Datenbanken. LinOTP verwendet bevorzugt Einmalpasswörter, um die Sicherheit in Anmeldeverfahren zu erhöhen.

Wir werden tiefer in die Struktur von LinOTP einsteigen und die Funktionsweise durch praktische Anwendung (Rollout, Authentisierung, Einbindung in andere Applikation) näher kennenlernen und somit die Möglichkeiten für eine erhöhte Sicherheit bei Remote-Zugriffen, Server-Administrator oder Web-Portalen darlegen.

Benutzerdatenbanken

I.d.R. hat jedes Unternehmen und jede Organisation bereits eine Benutzerverwaltung. Dies will LinOTP auch nicht ändern, daher bindet sich LinOTP an bestehende Benutzerdatenbank an, ob auf diese schreibend zugreifen zu müssen. Die Anbindung erfolgt über Module. Zur Zeit sind Module für beliebige LDAP-Datenbanken, SQL-Datenbanken und Flatfile (/etc/passwd) vorhanden. Weitere Module ließen sich leicht hinzufügen. Diese Benutzerquellen können beliebig zu Realms kombiniert werden, worüber sich auch die Mandantenfähigkeit abbilden lässt.

Management

Das Management macht sich das Pylons Webframework zu Nutze. Um die Token im LinOTP zu managen, gibt es einen Command line client, einen Web Client und einen nativen GTK client, der auf Windows und auf Linux läuft.

Darüber hinaus lassen sich alle Managementfunktionen über eine einfache WebAPI ansprechen, so dass ebenso einzelne Funktionen in andere Applikationen -- bspw. bestehende Helpdesk-Portale -- eingebunden werden können.

Selfservice

In einem Selfservice Portal können Benutzer die vom Administrator

definierten Funktionen auf ihre eigenen Token ausführen.

Authentisierung

Auch die Authentisierung erfolgt über eine einfache WebAPI. Unterstützte Protokolle und Szenarien sind PAM, Radius, OpenID, SAML und auch LDAP BINDs mittels OTP. Die Liste ist leicht und beliebig erweiterbar.

Über den Vortrag

Dieser Vortrag wird sehr praxisnah durchgeführt. In verständlichen Überblicken holt er Neulinge in dem Themenbereich Zweifaktorauthentisierung ab und wird bei Bedarf in beliebige technische Tiefen abtauchen.

Hands on / Praxis-Vorführung

In diesem Vortrag wollen wir anhand von praktischen Beispielen das System kennenlernen. Hierzu werden diverse Token-Typen ausgerollt (wie Hardware-Token, SMS-Token oder Smartphone Apps) und diverse Workflows vorgestellt. (bspw. Benutzer verliert unterwegs seinen Token und ihm muss wieder remote Zugriff gewährt werden.)

Ebenso zeigen wir, wie schnell und einfach bestehende Anwendungen um eine Zeifaktorauthentisierung mit [LinOTP](#) erweitert werden können.

Nützliches Vorwissen

- Aufbau von URLs
- Linux-Basiswissen
- Basiswissen Programmierung
- Basiswissen LDAP
- Basiswissen SQL

Weiterführende Links

<http://lsexperts.de/linotp.html>

<http://linotp.org/>

<http://www.openauthentication.org/>

<https://www.ietf.org/rfc/rfc4226.txt>

<http://motp.sourceforge.net>