Festplattenverschlüsselung mit Yubikey - verwaltet mit LinOTP

Cornelius Kölbel
cornelius.koelbel@lsexperts.de
http://www.lsexperts.de

Chemnitzer Linuxtage 2014 (März 2014)

Zusammenfassung

Spätestens seit Snowdens Enthüllungen sollte es jedem klar sein, dass man sich über den Schutz seiner Daten Gedanken machen muss. Verschlüsselung ist hier das Mittel der Wahl. Doch auch ein starker Verschlüsselungsalgorithmus ist nicht stärker als ein schwaches Passwort. Deswegen betrachten wir in diesem Vortrag die Möglichkeit, die Verschlüsselung mit einer Zweifaktor-Authentisierung zu schützen. Die mit LUKS verschlüsselte Festplatte wird erst mit der Eingabe eines starken Passwortes und dem Besitz eines Yubikeys aufgeschlossen. Die Verwaltung dieser Yubikeys erfolgt mit LinOTP.

LUKS (Linux Unified Key Setup)[1] ist eine Erweiterung des Device Mappers dm-crypt und in allen gängigen Linuxdistributionen als Verschlüsselungslösung der Festplatte vertreten.

[1] http://code.google.com/p/cryptsetup/

LUKS arbeitet mit Keyslots, die vereinfacht gesagt den mit einem Passwort verschlüsselten Verschlüsselungskey enthalten. Nach Eingabe des Passwortes kann der Verschlüsselungskey entschlüsselt und damit auf die gesamte verschlüsselte Festplatte zugegriffen werden.

Die Sicherheit der Daten hängt hier also lediglich an einem hoffentlich starken Passwort.

Dieser Vortrag zeigt, wie man mit einem Yubikey[2] zusätzlich zum Passwort einen zweiten Faktor (den Besitz des Yubikeys) einführen kann, so dass die Festplatte nur noch mit dem Wissen um das Passwort und dem Besitz des Yubikeys aufgeschlossen werden kann. Hierzu soll der Challenge-Response-Modus des Yubikeys verwendet werden, da man hierbei zum einen ohne authentisierendes Backend auskommt und außerdem es nicht nötig ist, die Taste auf dem Yubikey zu drücken. Es existieren bereits Ansätze solcher Lösungen im Internet[3]. Yubico selber bietet hierzu ebenfalls eine Implementierungsempfehlung[4] an, die bisher aber von keinem Hersteller umgesetzt wurde.

Schließlich wird in diesem Vortrag vorgestellt, wie mit dem Zwei-Faktor-Authentisierungs-Backend LinOTP[5] die Yubikeys für die Authentisierung in der LUKS-Boot-Phase ausgerollt und verwaltet werden können. Die Möglichkeit, Yubikeys, die zum Booten des Rechners benötigt werden, zentral auszurollen und zu verwalten, erleichtert nun die Nutzung einer solchen Lösung für einen größeren Benutzerkreis und hilft bei der Implementierung im Unternehmensumfeld.

Der Vortrag richtet sich sowohl an Privatanwender und Dienstleister als auch an kleine und große Unternehmen, die Ihre Datensicherheit verbessern wollen.

---

[2] http://yubico.com

[3] https://github.com/tfheen/ykfde

[4] http://static.yubico.com/var/uploads/pdfs/YubiKey Integration for Full Disk Encryption with Pre-Boot Authentication.pdf

[5] http://linotp.org