SOHO Radius für One-Time-Passwörter selbstgebaut

In diesem Vortrag wird praktisch vorgeführt, wie man aus einer Linux-Basis-Installation (CentOS 7.x) durch die Kombination von FreeRADIUS, oath-toolkit, google-authenticator und pam_oath einen OTP-Server baut.

Zunächst werden die zusätzlichen Pakete installiert, danach eine Ordnerstruktur für die Verwaltung der OTPs angelegt. FreeRADIUS ist mit ein paar Handgriffen bereit OTPs abzufragen und wir können die erfolgreiche Konfiguration bereits per Kommandozeile abfragen.

Ein paar simple Bash-Skripte erlauben die Administration des Servers von der Kommandozeile. Diese werden nun mit Webmin kombiniert bis eine tolle webbasierte Administrationsoberfläche entsteht, welche kinderleicht zu bedienen ist.

Das System kann folgende Tokentypen verwalten:

- sequenzbasierte HMAC OTPs
- zeitbasierte HMAC OTPs mit 30 sec. Intervall
- zeitbasierte HMAC OTPs mit 60 sec. Intervall
- Mobile-OTPs, zeitbasiert 10 sec. Intervall
- Mobile-OTPs, sequenzbasiert 10 sec. intervall

Es ist egal, ob die später eingesetzten Token dann Hardware-Token sind oder einfach nur die Software "Google-Authenticator" auf einem Smartphone.

Ein ähnlich konfiguriertes System läuft seit etwa 8 Jahren bei den Vortragenden produktiv und verwaltet ca. 2600 Hard- und Softwaretoken ohne Probleme. Dabei wird das System als 2. Faktor für die Authentisierung von VPN-Benutzern und den Zugriff auf ein Application-Portal verwendet.

Die Präsentation, samt allen Skripten wird spätestens am Tag des Vortrags unter https://bit.ly/2QNzQE8 bereitgestellt.