

SSH-Keys (Ed25519) erzeugen & installieren, passwortlose Anmeldung einrichten, installieren auf UDMP

YouTube Video: W-1S3aVXjNU

Video-Details

- **Kanal:** Navigio - Jürgen Barth
- **Dauer:** 24:05
- **Upload:** 16.09.2020
- **Kategorie:** Science & Technology
- **Tags:** unifi, ubiquiti

AI Model: openai-gpt-4o-mini

Zusammenfassung

HAUPTTHEMA

In diesem Video wird erklärt, wie man SSH-Schlüsselpaare erzeugt, diese austauscht und praktisch anwendet, insbesondere auf einem Unified Device.

KERNPUNKTE

- **Schlüsseltypen:** Es werden vier Schlüsseltypen vorgestellt – DSA (unsicher), RSA (veraltet, verwenden von 3072 oder 4096 Bit empfohlen), ECDSA (fragwürdig) und Ed25519 (empfohlen wegen Sicherheit und Geschwindigkeit).
- **Erzeugung unter Windows:** Die Nutzung des Programms PuTTY wird beschrieben, um SSH-Schlüsselpaare zu erzeugen. Die Schritte umfassen die Erstellung des Schlüssels und die sichere Speicherung.
- **Erzeugung unter Unix/Linux/Mac:** Der Prozess zur Erstellung von SSH-Schlüsseln wird ebenfalls erläutert, wobei das Programm `ssh-keygen` verwendet wird.
- **Schlüsselübertragung:** Es wird gezeigt, wie man den öffentlichen Schlüssel auf den Zielsystem überträgt und die Authentifizierung ohne Passwort einrichtet.
- **Konfiguration:** Die Konfiguration der SSH-Dateien zur Deaktivierung der Passwortanmeldung und zur Sicherstellung der Sicherheit wird demonstriert.
- **Praktischer Einsatz:** Ein praktisches Beispiel zeigt, wie SSH-Schlüssel auf einem Unified Device verwendet werden, wobei die sicherheitsrelevanten Aspekte hervorgehoben werden.

FAZIT/POSITION

Das Video bietet eine umfassende Anleitung zur sicheren Handhabung von SSH-Schlüsseln für eine effektive und sichere Authentifizierung. Es wird betont, dass eine sorgfältige Verwaltung der Schlüssel entscheidend ist, da der Verlust oder Diebstahl erhebliche Sicherheitsrisiken darstellen kann.