Schlüsselverwaltung – Grundsätze und Lebenszyklus

Ziel

Schlüsselverwaltung umfasst die gesamte Lebensdauer kryptografischer Schlüssel: Planung, Erzeugung, Ausgabe, Verwendung, Sicherung, Rotation, Sperrung und Löschung.

Trennung nach Zweck

Schlüssel sollten möglichst nicht gleichzeitig für voneinander unabhängige Zwecke eingesetzt werden. Für unterschiedliche Geräte und automatisierte Dienste sind getrennte Zugangsschlüssel sinnvoll. So kann ein einzelner kompromittierter Schlüssel gezielt entzogen werden.

Aufbewahrung

Private Schlüssel und symmetrische Schlüssel gehören in geschützte Speicherbereiche. Berechtigungen, Passphrasen, Hardware-Sicherheitsschlüssel und verschlüsselte Sicherungen sind geeignete Schutzmaßnahmen. Öffentliche Schlüssel dürfen verteilt werden, müssen aber korrekt zugeordnet sein.

Sicherung und Wiederherstellung

Unersetzliche Entschlüsselungsschlüssel, Recovery-Informationen und erforderliche Passphrasen müssen unabhängig gesichert werden. Eine Sicherung gilt erst dann als zuverlässig, wenn eine Wiederherstellung erfolgreich getestet wurde. Bei automatisierten Diensten ist zusätzlich der sichere Neustart nach einem Ausfall zu planen.

Rotation

Ein geplanter Schlüsselwechsel sollte überlappend erfolgen: neuen Schlüssel erzeugen, Berechtigungen verteilen, Funktion prüfen, alten Schlüssel entfernen. Bei Verschlüsselung muss geklärt werden, ob alte Daten mit dem bisherigen Schlüssel weiter entschlüsselt werden müssen.

Kompromittierung

Bei Verdacht auf Offenlegung: Schlüssel sperren oder Zugriffsrechte entfernen, Ersatzschlüssel

erzeugen, betroffene Systeme prüfen, Zertifikate gegebenenfalls widerrufen und nötigenfalls Daten neu verschlüsseln. Zeitpunkt und Umfang des Vorfalls dokumentieren.

Regelmäßige Prüfung

- Welche Schlüssel werden tatsächlich noch benötigt?
- Sind Besitzer und Zweck eindeutig?
- Sind Sicherung und Wiederherstellung geprüft?
- Sind abgelaufene Zertifikate und ungenutzte Zugänge entfernt?
- Ist die eingesetzte Kryptografie weiterhin angemessen?

Dokumentation

Ein Schlüsselkataster kann Metadaten, Zuständigkeiten und Prüftermine erfassen. Geheimnisse selbst gehören nicht in ein allgemein zugängliches Kataster.

Zurück zur Übersicht

From:
https://wiki.bluegnu.de/ - **wiki**

Permanent link:
https://wiki.bluegnu.de/doku.php/open:it:secure:schluesselverwaltung

Last update: **2026/11/15 16:36**