conpal LAN Crypt
Multi-Faktor-Authentifizierung mit dem
YubiKey Token

Der YubiKey ist ein Hardware-Authentifizierungsgerät von Yubico. Sie können sich das Gerät als einen winzigen Safe vorstellen, auf dem Anmeldeinformationen sicher und unabhängig von einem Computer gespeichert werden können. Es gibt ihn in den verschiedensten Größen: Von einem Token, der groß genug ist, um am Schlüsselbund getragen zu werden, bis hin zu den kleinsten Modellen, die kaum noch aus dem Gerät herausragen, in dessen USB-Anschluss sie eingesteckt sind. Der YubiKey benötigt weder eine Batterie noch Software, die auf dem Host-Gerät installiert werden müsste. Stecken Sie ihn einfach in einen USB-Port oder verbinden Sie ihn via NFC und schon sind Sie startklar.

Wie können Sie conpal LAN Crypt zusammen mit MFA nutzen?

conpal LAN Crypt ist eine client-seitige Verschlüsselungslösung, die Verschlüsselung auf Dateiebene bietet. Die leistungsstarke Schlüssel- und Richtlinienverwaltung unterstützt Daten mit unterschiedlichen Schlüsseln für geschäftliche, persönliche und gemeinsam genutzte Daten. Schlüssel, die einem bestimmten Benutzer zugewiesen sind, werden mit standardisierter privater Schlüsselkryptographie verschlüsselt. Nur derjenige Nutzer, der über den privaten Schlüssel verfügt, kann auf diese Schlüssel zugreifen, weswegen der Schutz dieses privaten Schlüssels von höchster Wichtigkeit ist. Der YubiKey Token ist dafür ideal: Durch seine Nutzung werden zwei separate Authentifizierungsfaktoren benötigt – Wissen und Besitz – und dadurch das generelle Sicherheitslevel deutlich erhöht.

Schutz aktivieren

1 Definieren Sie, welche Daten Sie schützen

Definieren sie in der Admin-Konsole von conpal LAN Crypt, welche Daten geschützt werden sollen und welcher Schlüssel verwendet werden soll. Eine einzige Regel reicht aus, um zu gewährleisten, dass alle Ihre Daten verschlüsselt sind. Definieren Sie zusätzliche Regeln mit unterschiedlichen Schlüsseln, wenn Sie Daten in bestimmten Ordnern freigeben möchten. Das ist alles, was Sie für den Moment brauchen. Sollten Sie mit dem Resultat nicht zufrieden sein, können Sie jederzeit die geschützten Bereiche nachjustieren, um sie so weiter an Ihre Bedürfnisse anzupassen.

2 Schlüssel an Benutzer zuweisen

Als nächstes weisen Sie den Benutzern die Richtlinien und die zugehörigen Verschlüsselungsschlüssel zu. Jeder Benutzer erhält sein eigenes persönliches Exemplar, das mit seinem eigenen persönlichen Schlüssel verschlüsselt ist. Persönliche Schlüssel sind für den Schutz vor unbefugtem Zugriff auf Daten unerlässlich. Aus diesem Grund muss der Zugang zu diesen Schlüsseln besonders gut gesichert sein. So wird sichergestellt, dass nur berechtigte Nutzer auf verschlüsselte Daten zugreifen können.

Bereitstellen des YubiKey Token

3 Bereitstellen des YubiKey Token

YubiKey Token sind eine perfekte Möglichkeit, persönliche Schlüssel sicher aufzubewahren. Um diese Funktion in conpal LAN Crypt nutzen zu können, muss der Token registriert und bereitgestellt werden. Dabei gibt es die Wahl zwischen einer zentralen Verwaltung - bei der Token direkt von der ausstellenden Authority (etwa einer PKI) mit den persönlichen Schlüsseln versehen werden – oder einer Selbstbedienungsoption, bei der der Benutzer seinen zuvor ausgegebenen persönlichen Schlüssel zum besseren Schutz auf den YubiKey-Token überträgt.

Aktivierung der Multi-Faktor-Authentisierung

4 Windows und Mac

Nach der Initialisierung ist die Verwendung des YubiKey-Tokens ganz einfach. Schließen Sie den Token an Ihr System an und schon können Sie loslegen. Sie müssen keine zusätzliche Software installieren oder Änderungen an Ihrer Konfiguration vornehmen. Sobald die Verbindung hergestellt ist, erkennt conpal LAN Crypt den Token automatisch und verwendet ihn zur Entschlüsselung des Benutzerprofils und der Verschlüsselungsschlüssel.

5 Multi-Faktor-Authentifizierung

Der Zugriff auf den persönlichen Schlüssel erfordert von nun an zwei Faktoren. Erstens muss der Nutzer den physischen Yubikey Token besitzen, zweitens muss er auch die Endbenutzer-PIN des Tokens kennen. Diese PIN wird für den Zugriff auf den persönlichen Schlüssel benötigt. Sobald der PIN erfolgreich eingegeben wurde, kann conpal LAN Crypt private Schlüsselfunktionen durchführen und die privaten Schlüssel des Nutzers entschlüsseln. Die Verwendung des YubiKey Token macht aus der conpal LAN Crypt Authentisierung eine 2FA (Two-Factor Authentication) mit den beiden Faktoren Wissen und Besitz.