Authentifizierung mit bi-Cube®

Unternehmen stehen heute unter dem Druck, die IT im Unternehmen sicherer und gemäß Compliance-Anforderungen zu gestalten. Dazu gehört auch die Absicherung von Anwendungen und Zugängen mit sicheren Authentifizierungsmethoden. bi-Cube bietet die Möglichkeit, sichere und gleichzeitig benutzerfreundliche Authentifizierungsverfahren einfach zu implementieren.

Starke Authentifizierungsmethoden erhöhen das Sicherheitsniveau

Für die Anmeldung an einem Arbeitsplatz oder für eine Anwendung muss der Benutzer nachweisen, dass er zur Nutzung autorisiert ist. bi-Cube bietet verschiedene Authentifizierungsverfahren an, die allein oder in Kombination genutzt werden können.

Ein hinreichend hohes Sicherheitsniveau lässt sich erzielen, wenn eine Kombination von Verfahren genutzt wird. Diese duale oder auch starke Authentifizierung geht davon aus, dass der Nutzer zwei unabhängige Informationen mitbringt, die jeweils seine Identität belegen.

Authentifizierung mittels Kennwort

bi-Cube bietet eine umfassende Kennwortverwaltung an, die Kennwortregeln und Kennwortwechsel automatisiert umsetzt. Mit der bi-Cube Single Sign-On Lösung werden gleichzeitig Sicherheit und Benutzerfreundlichkeit erhöht. Ohne ein Single Sign-On ist die Verwendung der Authentifizierung mittels Kennwort nur in Kombination mit anderen Verfahren empfehlenswert.

Der bi-Cube Secu Token zur sicheren und dualen Authentifizierung

Der Token ist verschlüsselt und mit einer begrenzten Lebensdauer belegt. In Verbindung mit der Länge und der Vielzahl der enthaltenen Prüfinformationen ist diese Authentifizierungsmethode unangreifbar.

Secu-Token auch mobil und mit Biometrie kombiniert

Der bi-Cube Secu-Token kann ohne großen Aufwand erzeugt und verteilt werden. Dies kann z.B. innerhalb des Firmensitzes durch einen berechtigten Administrator dezentral über das Web erfolgen. Somit ist diese sichere Authentifizierungsmethode auch in anderen Geschäftsstellen nutzbar.

Für ein noch höheres Sicherheitsniveau kann der Token zusätzlich mit dem Fingerabdruck des Benutzers abgesichert werden.

BI-CUBE AUTHENTIFIZIERUNGS-MÖGLICHKEITEN

- Kennwort
- Secu-Token
- Mobile Token
- SMS-Token
- Biometrie (Fingerabdruck)
- Speicher-/RFID-Karte
- Weitere Methoden (RADIUS)

DUALE AUTHENTIFIZIERUNG

Für ein hohes Sicherheitsniveau empfiehlt sich die Kombination von zwei Authentifizierungs-methoden, auch bei der Anmeldung am Arbeitsplatzrechner.

SINGLE SIGN-ON

Der Einsatz der bi-Cube Single Sign-On Lösung erhöht nicht nur die Sicherheit, sondern schafft auch eine hohe Benutzerzufriedenheit. Es lassen sich verschiedene Authentifizierungsmethoden in unser Single Sign-On integrieren.

Vor der Generierung des Tokens wird dann die biometrische Authentifizierung des Benutzers abgefragt. Analog funktioniert die Absicherung des Tokens mit einer PIN. Weiterhin kann der Secu-Token an einen bestimmten Speicherstick gebunden werden. Das macht es unmöglich, den Token von einem anderen Laufwerk aus zu generieren.

All diese Eigenschaften machen die Authentifizierung mit dem bi-Cube Secu-Token zu einer hochgradig sicheren Authentifizierungsmethode.

Mobil, sicher und bequem anmelden: Mit dem bi-Cube SMS-Token oder der App bi-Cube Mobile Token

Wird vom Benutzer im Rahmen einer dualen Authentifizierung neben dem Kennwort ein Token abgefragt, kann er diesen auf sein Mobilgerät anfordern. Der Token wird dann per SMS zugesandt.
Alternativ kann er sich über die bi-Cube Mobile Token App auf einem registrierten Gerät ganz bequem ein Mobile Token erstellen.
Der Einsatz dieser Lösungen spart dem Unternehmen zusätzliche Hardware, auf die der Token sonst verteilt werden müsste.

Biometrische Authentifizierung anhand des Fingerabdrucks über SSO

Die biometrische Authentifizierung anhand des Fingerabdrucks ist für die Anmeldung am Arbeitsplatzrechner und für die Absicherung sämtlicher über das bi-Cube Single Sign-On zur Verfügung stehenden Anwendungen einsetzbar. Sie bietet nicht nur eine hohe Sicherheitsstufe – sie ist auch für den Benutzer komfortabel zu handhaben. Voraussetzung für die Nutzung dieser Authentifizierungsmethode ist der Einsatz der entsprechenden Hardware. bi-Cube spricht dafür eine Vielzahl von unterschiedlichen Geräten an.

Komfortable Anmeldung am Arbeitsplatzrechner mit Speicher-/RFID-Karte

Weiterhin bietet bi-Cube die Möglichkeit, eine Speicher-/RFID Karte zur Authentifizierung zu nutzen. Mit Entfernen der Karte wird der Rechner gesperrt. Ist die Karte wieder im Slot, wird die Rechnersperrung aufgehoben. Eine Integration in bestehende RFID-Karten, die z.B. zum Bezahlen in der Firmenkantine genutzt werden, ist problemlos möglich.

Weitere Methoden

Das RADIUS-Protokoll ist ein bewährtes Mittel zur Authentifizierung. Deshalb stellt bi-Cube einen RADIUS-Server bereit, der mittels RADIUS-Protokoll von beliebigen Access-Control-Servern (z.B. Cisco) genutzt werden kann.

- bi-Cube bietet zahlreiche sichere Authentifizierungsmethoden
- Empfehlenswert ist die Kombination zweier Methoden
- Jede Authentifizierungsmethode lässt sich in das bi-Cube Single Sign-On integrieren

OEDIV SecuSys

SOFTWARE MADE IN GERMANY

bi-Cube ist eine Software „made in Germany“. Daraus ergibt sich nicht nur ein besonderer Qualitätsanspruch, sondern auch unsere Unabhängigkeit.

BEST PRACTICE

Durch jahrelange Projekterfahrung fließen in jede Softwarekomponente die Erfahrungen ein, die sich als „best practice“ bewährt haben. Dadurch sind Sie mit uns auf der sicheren Seite.

MEHR SICHERHEIT

bi-Cube schafft ein hohes Sicherheitsniveau und setzt Compliance konsequent um.

TRANSPARENZ

bi-Cube macht die Prozesse rund um die Verwaltung von Nutzern und Berechtigungen transparent.

Innovative Grundlagenforschung
Gefördert mit EFRE-Mitteln
EUROPÄISCHE UNION
Europäischer Fonds für Regionale Entwicklung

OEDIV SecuSys GmbH

Oldendorfer Str. 12
18147 Rostock

Tel: +49 381 37573-0
Fax: +49 381 37573-29
E-Mail: info@secusys.de
Web: www.secusys.de