ins Multi-Faktor-ID

Authentisierung durch Abgleich von „Wissen“ und „Besitz“.

Einfach und sicher.

Per App oder Token.

Statische Passwörter alleine bieten keine ausreichende Sicherheit, um Ihre IT-Infrastruktur vor ungewollten Zugriffen zu schützen. Eine Zwei-Faktor-Authentisierung mit der INS Multi-Faktor-ID ist hingegen die einfache und sichere Lösung. Dabei erfolgt die Anmeldung an Ihren Systemen nicht nur über ein statisches Passwort, sondern zusätzlich über eine Kombination aus einer PIN („Wissen“, 1. Faktor) und einem sich laufend ändernden Code, der Ihnen auf einem separaten Gerät (App oder Token) angezeigt wird („Besitz“, 2. Faktor).

ins Multi-Faktor-ID bietet Ihnen u.a.

- Unterstützt alle gängigen 2FA-Apps (IOS, Android)
- Anbindung z.B. über **Windows Credential Provider**, Radius und Netscaler
- Äußerst geringe Ausfallzeiten durch **Hochverfügbarkeit (99,8%)** und Loadbalancing
- Hosting in deutschem **Tier 3+ Rechenzentrum**
- Nutzung als **Self Service** oder **Managed Service**
- **Pay per use**: mtl. Lizenzpreis pro Nutzer
- **Kostengünstige Hardware-Token** verfügbar
- Sichere Übermittlung via HTTPS

Insbesondere für sicherheitskritische Anwendungsbereiche, aber auch für webbasierte Dienste, wird die Zwei-Faktor-Authentisierung vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) dringend empfohlen.

Die ins Multi-Faktor-ID stellt eine kostengünstige und sichere Lösung als Alternative zu Lösungen wie z.B. RSA dar, die wir Ihnen gerne detailliert präsentieren.

So funktioniert es:

Beim Zugriff auf eine geschützte Ressource, etwa eine Web-Benutzeroberfläche oder die Windows-Anmeldung, wird der Anwender zur Eingabe des Passcodes aufgefordert. Der Passcode basiert auf zwei Komponenten: der PIN, die bei der Einrichtung durch das Multi-Faktor-ID-System generiert wurde und dem Code, der für den Anmeldeversuch vom Authentifizierungstoken bzw. der App des Anwenders generiert wurde. Der Token-generator generiert alle 30 Sekunden einen neuen Sicherheitstoken in Form einer sechsstelligen Zahl, die nach dem gleichen Algorithmus auf dem entsprechenden Host, dessen Zugang mit diesem Token gesichert ist, ebenfalls generiert wird. Unser MFID-System berechnet, welche Nummer das Token zum aktuellen Zeitpunkt anzeigen soll, vergleicht sie mit den Angaben des Anwenders und entscheidet über Freigabe bzw. Verweigerung des Zugriffs.

Vereinbaren Sie mit uns einen Termin für ein kostenloses Erstgespräch, in dem wir Ihre konkreten Anforderungen besprechen und Ihnen die unterschiedlichen Möglichkeiten aufzeigen.

Zertifizierte Sicherheit, auf die Sie sich verlassen können:
INS ist zertifiziert nach **ISO 9001:2015** und **ISO/IEC 27001:2013**.