T SECURITY

Magenta Security OneTimePass.ID

Starke 2-Faktor Authentifizierung aus dem Telekom Trust Center

Authentisierung - Ist der Datenzugriff gesichert?

Eine Hauptursache für Hackerangriffe sind gestohlene oder kompromittierte Passwörter.

Nutzerkonten und sensible Daten in Unternehmen werden durch Passwörter geschützt. Gleichzeitig stellen diese ein Sicherheitsrisiko dar, sobald sie in die falschen Hände geraten. Laut dem „Data Breach Investigations Report 2022“ von Verizon sind 80% aller Datenschutzverletzungen in Unternehmen auf kompromittierte Anmeldedaten zurückzuführen.

Es betrifft alle Unternehmen, egal welcher Größe oder Branche

Cyber-Kriminelle beschränken sich dabei nicht nur auf große Unternehmen einer Branche. Für kleine und mittelständische Unternehmen ist das Risiko, Opfer einer Cyber-Attacke zu werden, laut BSI sogar höher als bei großen Unternehmen. Laut aktuellem „Data Breach Investigations Report“ mussten 61% aller kleinen Unternehmen Datenschutzverletzungen verzeichnen. Mehr und mehr Unternehmen erlauben externen den Zugriff auf das Unternehmensnetz. Außendienst-Mitarbeiter oder Kunden greifen auf persönliche Daten, wichtige Dokumente oder andere Informationen zu.

Häufig sind statische Passwörter der Schlüssel zu Ihren Systemen und damit auch zu kritischen Unternehmens- und Kundendaten. Eine schwache Authentisierung kann im Zusammenhang mit einem Sicherheitsvorfall erhebliche Auswirkungen auf Unternehmen haben.

Die Telekom setzt auf sichere 2-Faktor-Authentisierung:

Diese sorgt dafür, dass nur von Ihnen dazu berechtigte Nutzer mit dynamischen Einmal-Passwörtern Zugriff bekommen. Verwalten Sie die Berechtigungen und entscheiden Sie selbst darüber, welche 2-Faktor-Authentifizierungsmethode Ihre Nutzer anwenden.

Vorteile

- Starke 2-Faktor-Authentifizierung
- Hochsicher, -verfügbar, -performant und -skalierbar (Betrieb im Telekom Trust Center)
- Eigene, separate Benutzerverwaltung
- Verschiedene Token zur Auswahl (SmartToken (App), Hardware-Token, SMS-Token und weitere)
- Verschiedene Applikationsschnittstellen (RADIUS, SOAP, SAML, REST)

Schlüsselmerkmale

- Erhöhte Sicherheit gegen Cyber-Attacken
- Schwer angreifbar
- Einfache Prozesse
- Eliminierung schwacher, leicht zugänglicher Passwörter
- Wegfall komplizierter Passwort-Richtlinien und Passwortwechsel

Connecting your world.

Lösungsangebot für Magenta Security OneTimePass.ID

Wann zu verwenden?

OneTimePass.ID ist grundsätzlich von Ihnen zu verwenden, wenn Sie den Zugriff auf Ihr Netzwerk / ihre geschlossenen Benutzergruppen durch eine starke 2FA schützen möchten.

Welcher Support wird angeboten?

- Support-Hotline (DE/EN): Montag – Freitag, 7–19 Uhr
- Störungsannahme: 24/7
- Internet-Serviceportal, Downloadbereich, FAQ

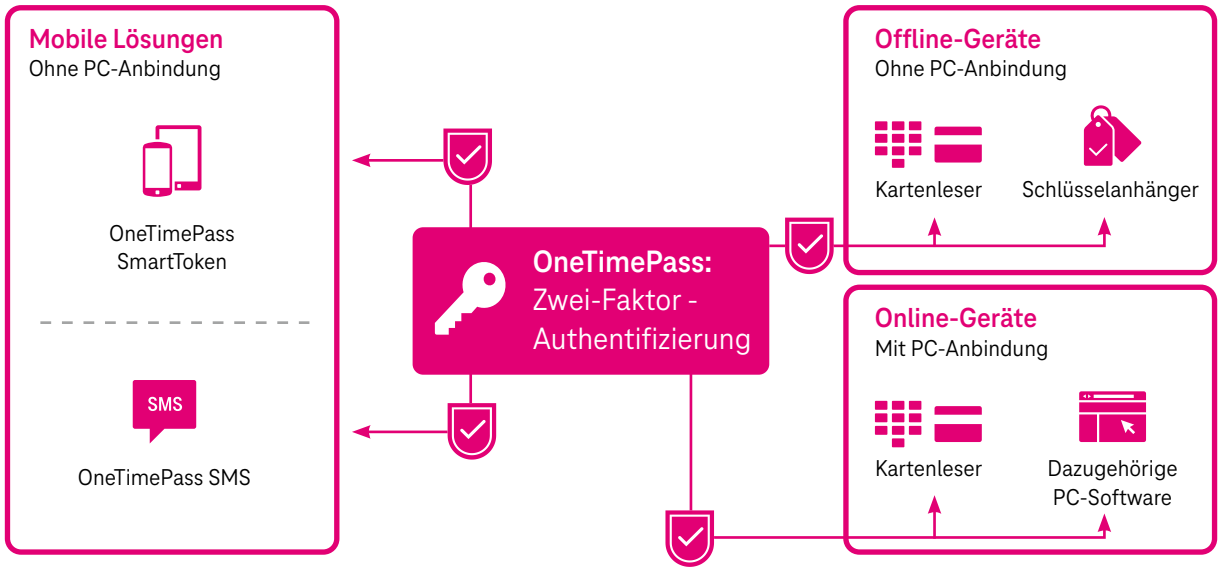
Was ist inbegriffen?

- Bereitstellung des Service inkl. Unterstützung bei Ersteinrichtung
- Optional Schulungen

Wie viel kostet es?

- Einrichtungspreis: 900,- €
- Monatlich ab 50,- €
- Min. 12 Monate Vertragslaufzeit

Alle Preise zzgl. gesetzlicher Mehrwertsteuer.



OneTimePass.ID? Höchster und umfassender Schutz!

Vergessene Passwörter und zeitraubendes Zurücksetzen verlorener Log-in-Daten sind mit OneTimePass.ID Vergangenheit. Die Lösung ersetzt statische Passwortsysteme durch dynamische Einmalpasswörter. Das Ergebnis: steigende Sicherheit und nur noch eine PIN merken.

Connecting your world.

Kontakt
Persönlicher Ansprechpartner
Freecall: 0800 33 04444
E-Mail: security@telekom.de
Web: security.telekom.de

Herausgeber
Deutsche Telekom Security GmbH
Bonner Talweg 100
53113 Bonn