AUTHENTISIERUNG

IST DER DATENZUGRIFF GESICHERT?

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.

Eine Hauptursache für Hackerangriffe: gestohlene oder kompromittierte Passwörter

MÖGLICHE GEFAHREN

- Weitergabe und unberechtigtes Nutzen von fremden Passwörtern.
- Abfangen von internen Passwörtern.
- Cyberangriff auf Passwörter zum Zweck der Spionage / Manipulation.

BEISPIELE

RISIKEN FÜR **HANDEL**

- Verlust von Einnahmen
- Verlust von Daten
- Vertrauensverlust
- Regressansprüche
- Bedrohung der Existenz

RISIKEN FÜR **FERTIGUNG**

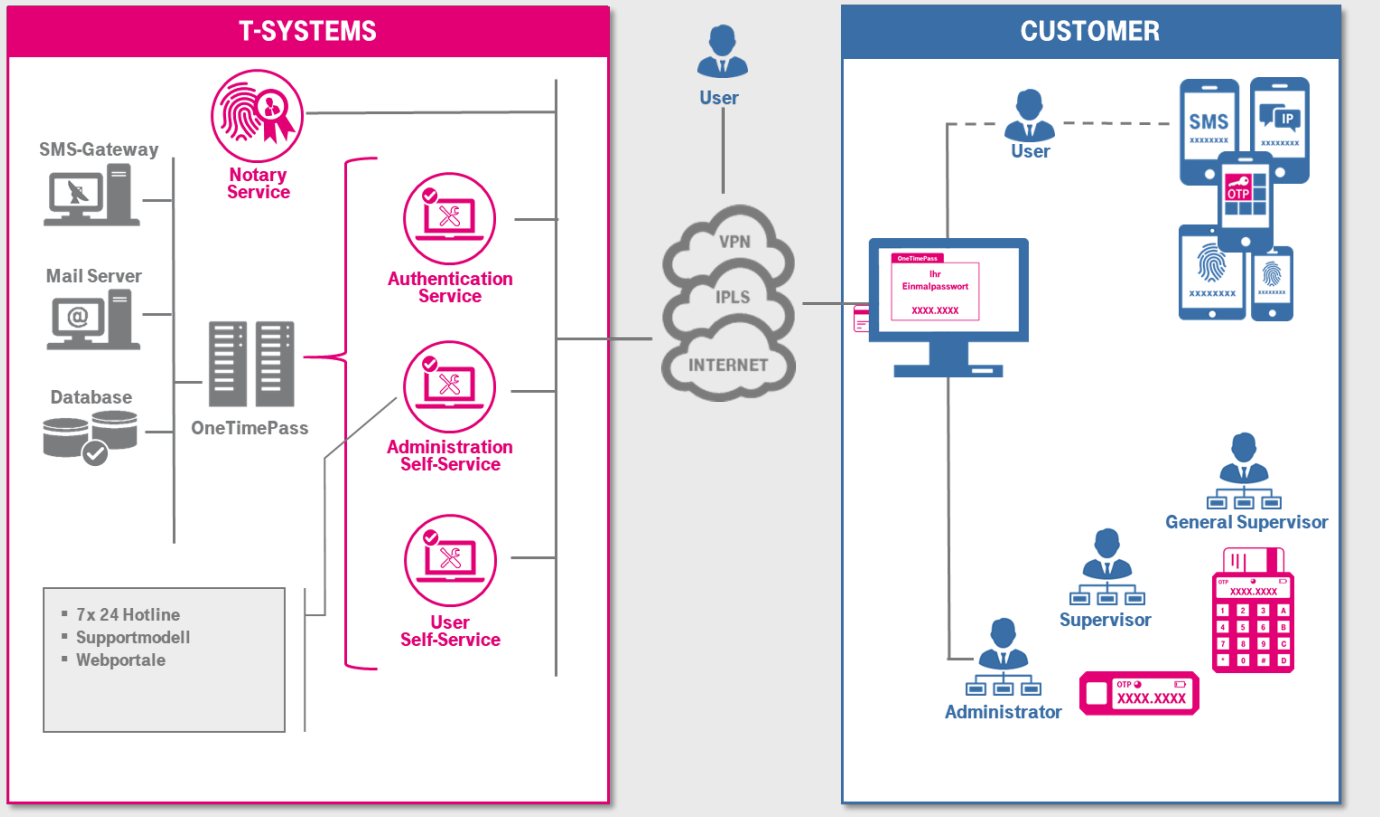
- Systemverfügbarkeit
- Produktionsstörung
- Qualitätsverlust
- Sabotage
- Diebstahl von Patenten und Know-How

RISIKEN FÜR **DIENSTLEISTUNG**

- Serviceausfall
- Datenmanipulation
- Ausspähung von Daten
- Verstöße gegen gesetzliche Vorgaben
- Regressansprüche

DIE LÖSUNG

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



TELESEC ONE TIME PASS

VORTEILE AUF EINEN BLICK

- Starke 2-Faktor-Authentifizierung
- Hoch -sicher, -verfügbar, -performant und –skalierbar
  (Betrieb im Telekom Trust Center)
- Eigene Benutzerverwaltung
- Verschiedene Token zur Auswahl
  (IP-Token, SMS-Token, Hardware-Token, Biometrische-Token, Smart-Token, FIDO-Token)
- Verschiedene Applikationsschnittstellen
  (RADIUS, SOAP (SAML ab neuem Release))

LEISTUNGEN:

Betriebsmodell

- OTP-Compact
  < 100 Nutzer
- OTP Advanced
  ab 100 Nutzer
  (inkl. Advanced Groups)
- Mandanten- und Resellerfähig

Service

Service-Modell
- 5x12h für Support-Anfragen
- 7x24h Störungshotline
- Internet-Serviceportal
- Downloadbereich, FAQ, News

Optional

- Anbindung per Internet, IPsec-VPN oder MPLS
- SmartToken (App)
- Hardware-Token
- SMS-Token
- Smartcard/Kartenleser
- (IP-Token ab neuem Release)

V02

INTERESSE?

Vertrauen Sie dem führenden Anbieter von Sicherheitslösungen.

Kontakt:

T-Systems International GmbH
security-info@t-systems.com
www.t-systems.de/security