

Donnerstag, 27. September 2018

**TAKENET GmbH präsentiert**

**PASSWORD**  **SAFE**  
by MATESO

**TAKENET GmbH**

**Herr Peter Schöner**  
**Herr Andreas Hübner**

## IT – Servicepartner in Mainfranken

### AN20

Alfred-Nobel-Straße 20  
97080 Würzburg

40 Mitarbeiter, seit 2000



IT-Fullservice, Outsourcing,  
Rechenzentrumsbetrieb,  
Infrastruktur, Virtualisierung  
IT-Solutions



SAP Basis / SAP Technology  
SAP ERP, SAP All-in-One,  
SAP Business One

seit 2003: ISO 9001 (QM)  
seit 2008: ISO/IEC 27001 (Sicherheit)

# ENTERPRISE PASSWORD MANAGEMENT

mit Password Safe and Repository

Passwort  
vergessen?

## Die Fakten sprechen für Password Safe

- **Über 2.500.000 Anwender weltweit arbeiten mit Password Safe**
- **10.000+ Firmenkunden**
- **Marktführer im DACH Raum**
- **19 der Top 30 Dax-Unternehmen vertrauen bereits auf unser Produkt**
- **IT-Security Software – made in Germany**



TeleTrust Quality Seal  
[www.teletrust.de/itsmig](http://www.teletrust.de/itsmig)

## Sicherheitsüberprüfung



„Die SySS GmbH bewertet das Sicherheitsniveau der getesteten Softwareanwendung Password Safe and Repository 8 als sehr hoch.

Die Vertraulichkeit sensibler Daten wie Passwörter und Dokumente wird dabei durch sichere kryptografische Verfahren und einen eingeschränkten Zugriff auf entsprechendes Schlüsselmaterial gewährleistet.

Bezüglich der Schutzziele Integrität und Verfügbarkeit konnte die SySS GmbH keine Schwachstellen finden...“

**Sebastian Schreiber**  
Geschäftsführer der SySS GmbH



**Sind Ihre Passwörter sicher?**

**Wie geht Ihr Unternehmen mit  
Firmen-Passwörtern um?**

## Sicherheit vs. Bequemlichkeit

**56%** nutzen das gleiche Passwort beruflich wie privat

**20%** geben ihr Passwort an Mitarbeiter weiter

# Frau Müller aus der Buchhaltung kündigt ...

**Jetzt sollten Sie nicht  
in Panik geraten.**

Ab 25. Mai 2018  
gilt die neue  
**Datenschutz-  
grundverordnung.**

---

**DSGVO**  
Sorgen Sie jetzt für  
mehr digitale  
Sicherheit.

## Alptraum Datendiebstahl

**1 von 7** Mitarbeitern würde sein Passwort an Dritte verkaufen

**1 von 5** Personen wurden bereits Opfer einer Datenpanne

**Mögliche Konsequenz: irreparabler finanzieller oder Imageschaden möglich**

## Schlechte Passwörter

zu **79%** besteht ein Passwort aus persönlichen Angaben

**100%** Risiko – bei leicht zu merkenden Passwörtern

**123456** das meist benutzte Passwort

**W!bCym5** das Passwort ist in unter 10 Stunden errechnet

➤ <https://checkdeinpasswort.de/>

# WIE SICHER IST MEIN PASSWORT?

**Probiere verschiedene Passwörter aus!**

⚠ Aus Sicherheitsgründen sollten Sie niemals Ihre echten Passwörter eingeben.



„CheckDeinPasswort.de speichert keinerlei Daten und ist für Benutzer unbedenklich.“

RA Kai Schütze, Fachanwalt für IT-Recht

## Identische Passwörter

Durchschnittlich werden nur **3** unterschiedliche Passwörter verwendet

zu **23%** Wird die Zahl **1** an ein Passwort angehängt

# ➤ <https://wpengine.com/unmasked/>

"I'll Add a Number to Make it More Secure."

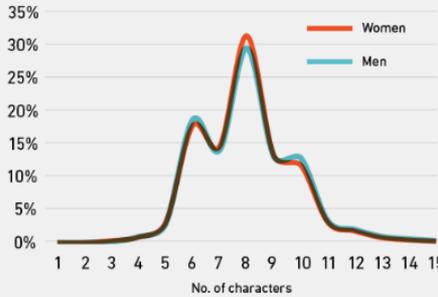
Most Used Numbers (0-99) at the End of 420,000 Passwords



The 20th Most Used Key Walk in 10 Million Passwords



Breakdown of 485,000 Passwords' Length

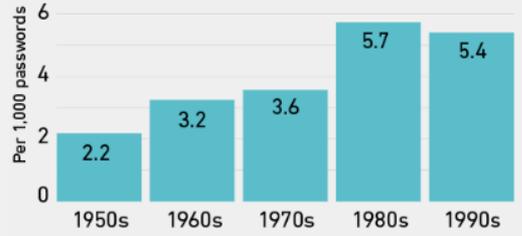


The 20 Most Common Keyboard Patterns in 10 Million Passwords



 Position: Agent to the stars Password: <b>clydek</b> Entropy: 12.2 Crack Time: 0.2 seconds	 Position: Former Senior Password: <b>s3ash311 (seashell)</b> Entropy: 15.6 Crack Time: 2.5 seconds	 Position: Director Password: <b>indiana</b> Entropy: 9.8 Crack Time: 0.04 seconds
 Position: On-air Correspondent Password: <b>ballet</b> Entropy: 12.2 Crack Time: 0.24 seconds	 Position: Journalist Password: <b>raven639</b> Entropy: 19.4 Crack Time: 34 seconds	 Position: Senior Engineer Password: <b>ez1422</b> Entropy: 23.6 Crack Time: 12 minutes
 Position: Editor Password: <b>shagwell</b> Entropy: 16.8 Crack Time: 5.8 seconds	 Position: Division Chief Password: <b>lincoln</b> Entropy: 10.9 Crack Time: 0.09 seconds	 Position: Editor Password: <b>dgnco</b> Entropy: 22.0 Crack Time: 5 minutes
 Position: Senior Director Password: <b>wuxi6969</b> Entropy: 21.9 Crack Time: 5 minutes	 Position: Software Engineer Password: <b>muffins</b> Entropy: 12.3 Crack Time: 0.2 seconds	 Position: Senior Manager Password: <b>123456</b> Entropy: 1.0 Crack Time: 0 seconds
 Position: Digital Reporter Password: <b>blah11</b> Entropy: 14.7 Crack Time: 1.3 seconds	 Position: Manager Password: <b>b0j1k0</b> Entropy: 27.8 Crack Time: 5 hours	 Position: Editor Password: <b>kellymistry</b> Entropy: 14.2 Crack Time: 0.9 seconds

Use of 'Love' in Passwords By Decade of Birth



# Ihr Admin hat alles im Griff.

**Muss er auch direkten Zugriff  
auf alles haben?**

Ab 25. Mai 2018  
gilt die neue  
**Datenschutz-  
grundverordnung.**

---

**DSGVO**  
Sorgen Sie jetzt für  
mehr digitale  
Sicherheit.

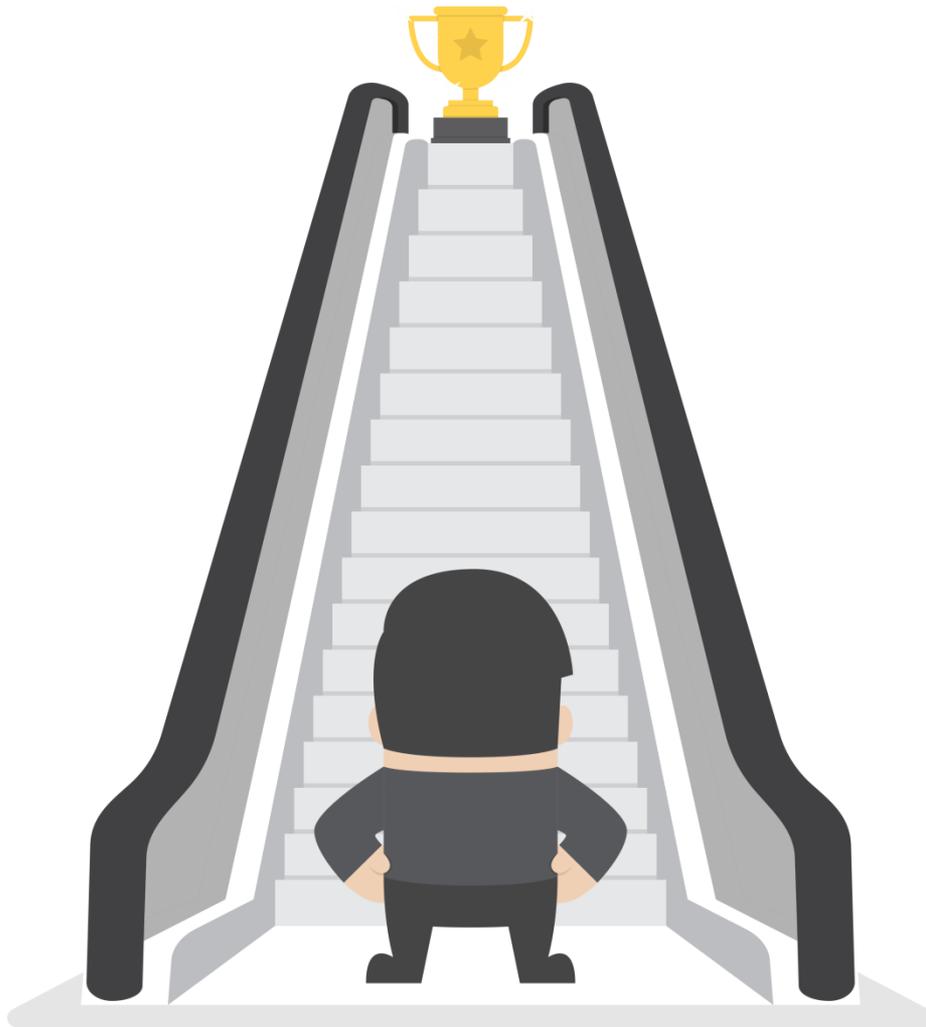
## Vorsicht vor Cyberattacken



## SERVICEACCOUNTS & CO.

- Service Accounts oder auch administrative Zugänge sind eine Schwachstelle der IT
- Mehrfachverwendung des Passworts oder erstellen von Passwörtern nach einem Muster
- Unsichere Weitergabe der Zugangsdaten via unverschlüsselter E-Mail, Zettel oder Chat.

## Herausforderungen



- **BSI-IT-Sicherheitsgesetz:**  
neue Vorgaben für Betreiber kritischer Infrastrukturen  
(KRITIS – Schutz kritischer Infrastrukturen)
- **BSI IT-Grundschutz-Kataloge, Maßnahmenkataloge, insb.**
  - M 2.11 Regelung des Passwortgebrauchs
  - M 4.306 Umgang mit Passwort-Speicher-Tools
- **ISO/IEC 27001, normativer Anhang A.11**  
Zugangskontrolle,  
insb. A.11.3.1 Passwortverwendung  
(praxisnäher in der Umsetzung)
- **EU-Datenschutzgrundverordnung (EU-DSGVO),**  
insb. Art. 32 (gilt ab 25. Mai 2018)

## Argumente für Password Safe



- Hohe Verschlüsselung der Passwörter
- Zentrale Datenbank
- Entdecken und verwalten privilegierter Accounts inkl. Password Reset
- Verschlüsselte Kommunikation zwischen Client und Server
- Rechteverwaltung bis auf Datensatzebene
- Active Directory Integration und Authentifizierung
- Zwei Faktor Authentifizierung (z.B.: OTP, PKI, Zertifikate, ...)
- Speichern von Dateien/Anhängen zu Passwörtern (Lizenzen, PDF's, ...)
- Detaillierte Protokollierung (Log) – revisionssicher
- Datensatzversionierung Freigabe-System (Mehr-Augen-Prinzip)
- Automatische Eintragung (SSO) via Agent/Browser Addons
- Sichtsperrung für Passwörter (autom. Anmeldung ohne Passwort zu sehen)
- Terminal Server/Citrix fähig
- Einfaches Handling und benutzerfreundlich
- Offline Verfügbarkeit
- Mobiler Zugriff (Web Client)
- Automatisches Backup
- uvm.

## Die Lösung: Password Safe!

The screenshot displays the Password Safe - Enterprise Plus (8.5.0.14896) application window. The interface is divided into several sections:

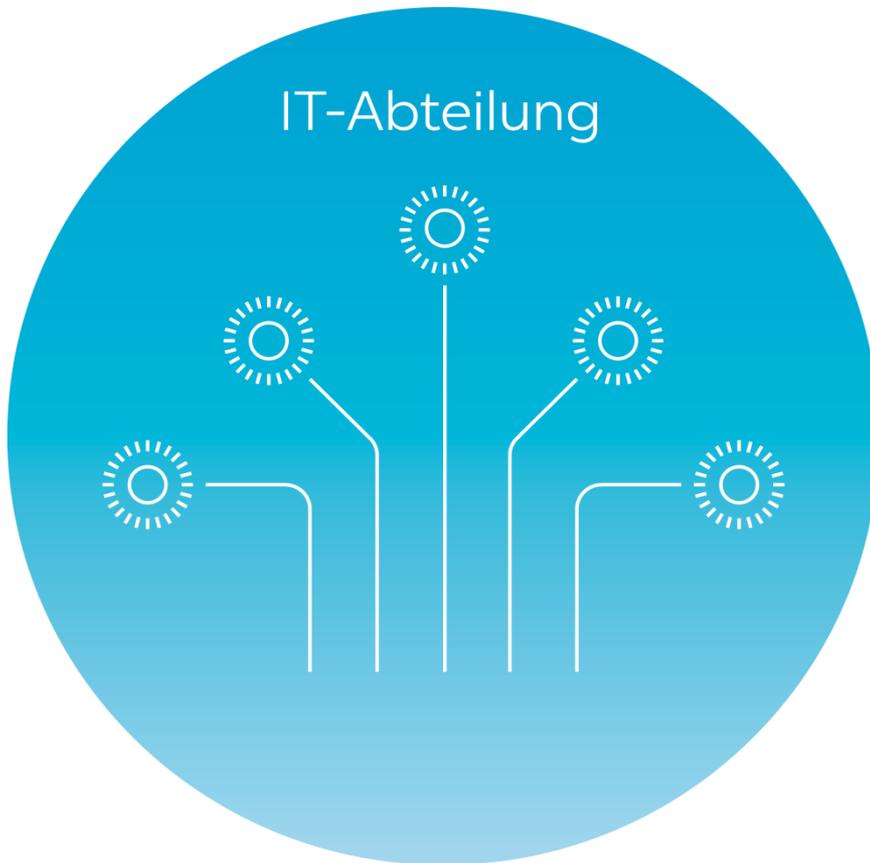
- Top Bar:** Includes a search bar labeled "Schnellsuche (Strg+Q)" and a title bar with window controls.
- Menu Bar:** Contains "START", "ANSICHT", and "FILTER".
- Toolbar:** Features various icons for actions like "Öffnen", "Löschen", "Aufdecken", "Benachrichtigungen", "Duplizieren", "Verschieben", "Berechtigungen", "Schnellansicht", "Siegel", "Sichtschutz", "Benutzername", "Passwort", "Internetseite", "Internetseite öffnen", "Externe Links erzeugen", "Export", "Historie", "Drucken", "Formular wechseln", and "Einstellungen".
- Left Panel (Filter Struktur):** Shows a search field and a list of filters, currently displaying "admin".
- Main Content Area:**
  - admin x** (tab)
  - Alle Favoriten** (header)
  - TakeNet GmbH** (entry) with a yellow status indicator and date "21.09.2018".
  - Webpasswort** (sub-entry) with a yellow background.
  - Webpasswort Details:**
    - Beschreibung:** TakeNet GmbH
    - Benutzername:** passwordsafe
    - Passwort:** Masked with dots, status "Gut"
    - Internetadresse:** https://www.takenet.de
    - Bemerkung:** Empty text area
    - Gültig bis:** Empty date field
  - Administrator, TakeNet (admin)** (user info)
- Bottom Bar:** Includes navigation links: "Passwörter", "Dokumente", "Organisationsstruktur", "Rollen", "Formulare", "Benachrichtigungen", "Logbuch", and a menu icon.

# Password Safe - Keyfeatures

- **Zentrale Team-Datenbank**
- **SSO Agent mit Browser Add-On**
- **Offline Zugriff und Webclient**
- **Sichtschutz**
- **Vier-Augen-Prinzip (Siegel)**
- **Zwei-Faktor Authentifizierung**
- **Passwort Reset**
- **Kein Open Source – Made in Germany!**
- **u.v.m**



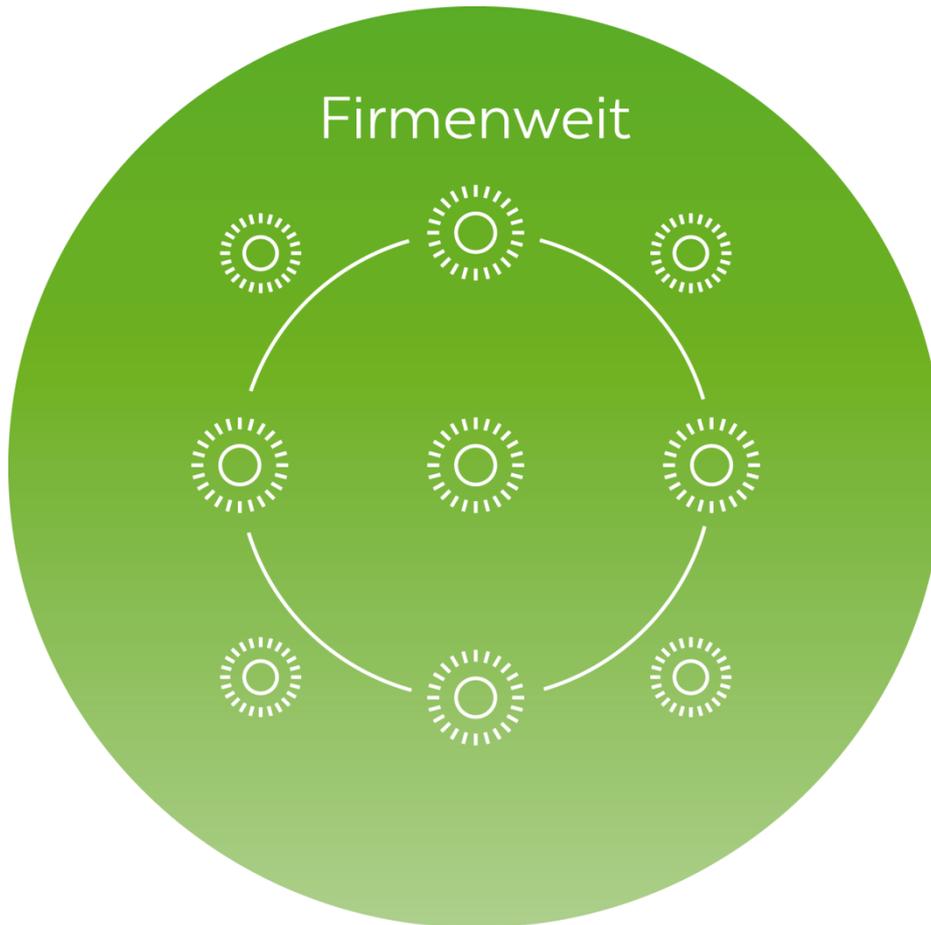
## Einsatzszenario – IT-Abteilung



**Die Arbeit der System-Administratoren ist bedeutender Sicherheitsfaktor und ein hochsensibles Aufgabengebiet.**

- **Verwaltung von Systemen mit etlichen Passwörtern**
- **Häufiger Login zur Konfiguration auf div. Systeme notwendig**
- **Dokumentation von Systemen und komplexen Strukturen**
- **Berechtigungskonzept für Zugriff auf Systeme**
- **Protokollierung des Zugriffs**

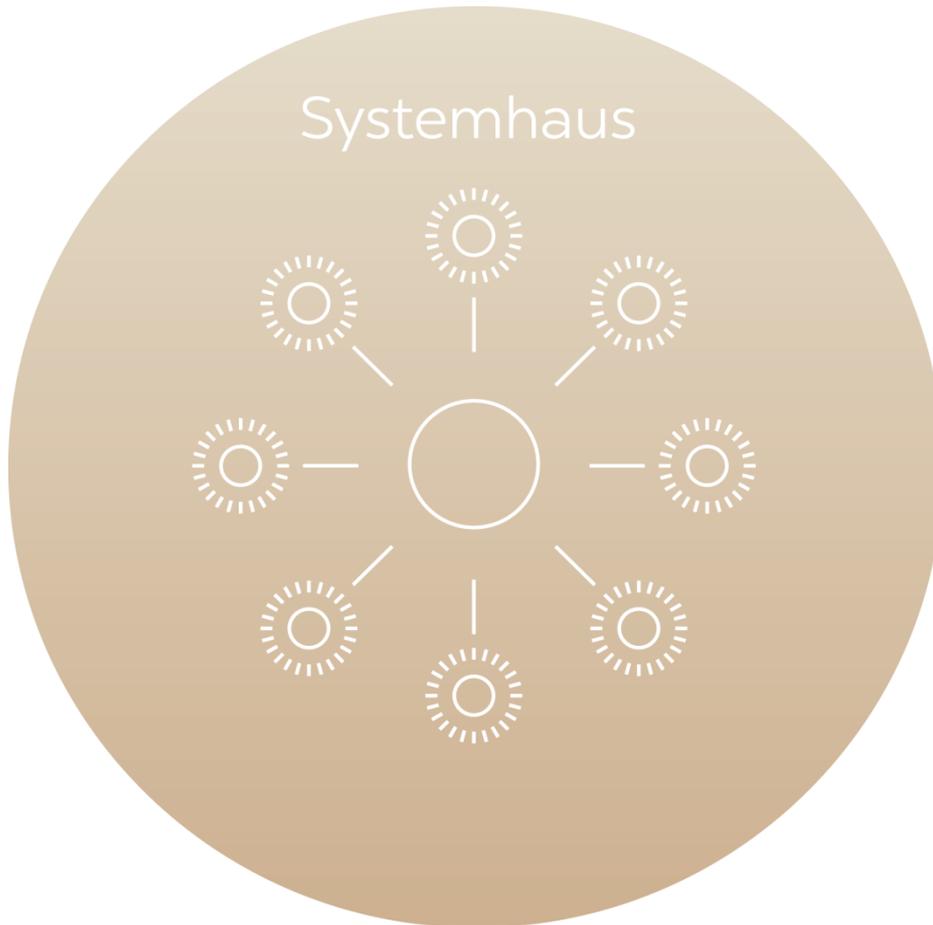
## Einsatzszenario – Firmenweite Einführung



Jeder Mitarbeiter muss sich zahlreiche Passwörter merken. Je komplexer die Systeme, desto größer die Herausforderung.

- **Ausschließliche Verwendung von sicheren Passwörtern**
- **Vermeidung von Passwörtern in unsicheren Medien**
- **Reduzierung der Password Resets durch zentrales Password Management und automatische Passwort Eintragung**
- **Rechteverwaltung zur Steuerung des Daten-Zugriffs**
- **Hochverfügbarkeit sorgt für eine niedrige Ausfallzeit**
- **Anpassung an Sicherheitsanforderungen des Unternehmens**

## Einsatzszenario – Systemhaus



**Datenverwaltung und auch die Datensicherheit sind hoch komplexe Gebiete von Systemhäusern. Es geht hierbei nicht nur um firmeneigene Daten, sondern auch um Kundendaten.**

- **Nachweisliche Datensicherheit für Firmenkunden**
- **Anpassbare Datenstruktur zur optimalen Verwaltung**
- **Kundendaten werden oft vor Ort zur Konfiguration oder Einrichtung benötigt**
- **Protokollierung jedes Zugriffs und auf Wunsch dem Kunden vorlegbar**
- **Rechtstruktur regelt Zugriff auf Daten und Kunden**

➤ <https://www.hallo-main-rhoen.de/> - 14.03.2016

## Cyberangriff: Trojaner erpresst Stadt Dettelbach



**PASSWORD SAFE**

VIELEN DANK

*Hochzeitstag  
nicht  
vergessen!*

## Ihre Ansprechpartner



**Peter Schöner**

**IT-Service Manager**

**E-Mail: [schoener@takenet.de](mailto:schoener@takenet.de)**

**Telefon: 0931 903 3109**