

PASSWORD SAFE

... und der Betriebsrat

INFORMATIONEN FÜR DEN BETRIEBSRAT



Zugriffskontrolle

Verhindern sie den Zugriff durch Unbefugte – durch Speicherung der Passwörter von Datenverarbeitungssystemen in Password Safe. Zugriff auf die Passwörter erhalten nur berechtigte Mitarbeiter! Der Zugang zu Password Safe kann dabei mittels Multi-Faktor-Authentifizierung doppelt abgesichert werden.



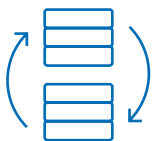
Kontrolle über Passwörter

Legen Sie gezielt fest, welche Mitarbeiter Zugriff auf welche Passwörter erhalten: Erstellen Sie ein entsprechendes Rechtekonzept in Password Safe und weisen sie die Zugriffsrechte den Mitarbeitern entsprechend ihrer Berechtigung/Rolle zu. Dank Sichtschutz können die Passwörter nicht eingesehen werden. Besonders sensible Passwörter können auch einem Freigabeprozess unterliegen. Erst nach Freigabe durch berechtigte Personen können diese dann verwendet werden.



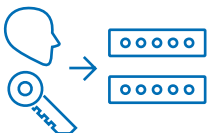
Eingabekontrolle

„Welcher Mitarbeiter hat wann welches Passwort verwendet?“ Nutzen Sie das Logbuch, um alle Vorgänge nachvollziehen zu können. Besser vorsorgen: Bei Bedarf warnt Sie das System auch automatisch bei ungewöhnlichem Verhalten, damit Sie frühzeitig reagieren können.



Verfügbarkeitskontrolle

Dank SQL Clustering sind die Datenbank und damit auch die Passwörter stets verfügbar. Fällt ein System aus, wird das zweite aktiviert. Verwenden Sie zudem mehrere Anwendungsserver, sodass bei einem Serverausfall die Mitarbeiter weiterhin Zugriff auf ihre Passwörter erhalten. Mithilfe von automatischen Backups werden alle in Password Safe hinterlegten Benutzer und Passwörter sowie konfigurierten Rollen und Berechtigungen gesichert.



Keine Speicherung personenbezogener Daten

Zur Verwendung von Password Safe bedarf es lediglich eines Benutzernamens und eines Passworts. Weitere Daten sind optional.



Datenschutz

Jeder Benutzer sieht nur die Daten, auf die er berechtigt ist. Das betrifft auch die Einträge im Logbuch. Diese können auch regelmäßig automatisch gelöscht werden.