

PASSWORD SAFE

IT-Security im Finanzsektor

In den vergangenen Jahren ist das Risiko von Cyberangriffen auf die Wirtschaft und damit auch auf den Finanzsektor erheblich gestiegen. Die Gründe hierfür liegen auf der Hand. Zum einen die Digitalisierung unserer Wirtschaft sowie die zunehmende Vernetzung der Unternehmen, durch die neue Einfallstore für Hacker entstehen. Zum anderen finden Angreifer immer neue, professionellere Wege, um Unternehmen anzugreifen. Deshalb überrascht es auch nicht, dass Cyberattacken gegenwärtig als das größte operationelle Risiko für den Finanzsektor gelten.



Um vor allem die IT-Sicherheit in kritischen Infrastrukturen zu optimieren, hat die BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) bereits 2006 in einem Rundschreiben die Mindestanforderungen für das Risikomanagement (MaRisk) von Banken festgelegt. Banken und andere Finanzinstitute müssen deshalb den Normen wie BaFin nach AT 4.3.1 Tz.2, AT 7.2 Tz, ISO 27001, MaRisk nach BTO Tz. 9, SOX, PCI Standard, BAIT und FINMA erfüllen. Die Institute sollen ein Mindestmaß an Sicherheit gewährleisten und so vor Cyberattacken und den daraus resultierenden negativen Folgen geschützt werden. Password Safe hilft deinem Unternehmen, sicherheitsrelevante Anforderungen zu erfüllen und dabei gleichzeitig die Sicherheit der Zugangsdaten merklich zu erhöhen.



Optimiere jetzt die IT-Sicherheit in deinem Unternehmen. Unternehmensweit sichere Passwörter sind eins der besten Mittel gegen Cyberangriffe. Arbeite mit dem Marktführer im Bereich Password Management zusammen – wir haben die Expertise, um auch dein Institut gegen Cyberangriffe abzusichern!

Große Finanzdienstleister sind zudem gesetzlich dazu verpflichtet, sensible Daten in einer sicheren Umgebung zu speichern. Password Safe wird ausschließlich auf unternehmenseigenen Servern Self-Hosted betrieben. Im Vergleich zu SaaS-Lösungen und der Speicherung der Daten in einer Public Cloud hat das lokale Hosting im Unternehmen den Vorteil, dass alle Informationen rechtssicher am Unternehmensstandort wie beispielsweise in Deutschland gespeichert werden und die Server im Vergleich zu großen Cloud-Anbietern seltener Ziel von Hackerangriffen werden.



Auf Nummer sicher gehen

Gerade im Finanzsektor mit schätzungsweise dreimal mehr Cyberangriffen als in anderen Wirtschaftssektoren ist hoher Passwort-Schutz enorm wichtig. Bei Großunternehmen besteht allein auf Grund der hohen Mitarbeiterzahl das Problem, alle Zugänge, Passwörter und Apps abzusichern. Wenn Mitarbeitende ihren Login mit „Neumann1964!“ schützen, haben Hacker ein leichtes Spiel, Passwörter zu knacken.

Zum Schutz der Banken veröffentlicht die BaFin regelmäßig einen Katalog mit Anforderungen an die IT. Password Safe bietet zahlreiche Features, um die Informationssicherheit zu erhöhen und den Anforderungen der BaFin gerecht zu werden.

BaFin: „Durch Maßnahmen wie der Richtlinien zur Wahlsicherer Passwörter ist die Umgehung der Vorgaben der Berechtigungskonzepte vorzubeugen.“

Mit Password Safe ist „Neumann1964!“ passé: Mitarbeitende können sich in Sekundenschnelle automatisch anmelden – ohne überhaupt das Passwort zu kennen, da alle Passwörter sicher in der Software verwaltet werden. Für die Erstellung sicherer Passwörter steht ein Passwort-Generator zur Seite: Mit nur einem Klick können komplexe Passwörter generiert werden, an denen sich Hacker die Zähne ausbeißen. Zudem kann die IT individuelle Passwort-Richtlinien erstellen, die Schutz gegen zu leichte Passwörter bieten. Durch die Funktion Password Reset können Passwörter automatisch von der IT ereignis- oder zeitbasiert ausgetauscht werden.

Intelligente und sichere Lösungen für Finanzinstitute

Password Safe unterstützt dich mit einer individuell auf dein Unternehmen zugeschnittenen Passwortverwaltungslösung, egal ob für eine Filiale oder mehrere Standorte. Unabhängig davon, ob es sich um verzweigte Berechtigungsstrukturen für Banken oder um das zentrale Password Management in sonstigen Finanzeinrichtungen handelt: Vertraue auf unsere umfangreiche Erfahrung in der IT-Security-Branche!



Durch mehrere Augen Prozesse absichern

Das Mehr-Augen-Prinzip steht in der Finanzbranche an der Tagesordnung. Aktivitäten oder Prozesse werden von mindestens zwei Personen freigegeben, was gegen Manipulation und Missbrauch absichert. Wieso dieses Prinzip nicht auch auf den Umgang mit Passwörtern anwenden?

BaFin: „Änderungen [...] von Berechtigungen [...] sind nachvollziehbar und auswertbar zu dokumentieren.“

Die in Password Safe integrierte Siegelfunktion stellt sicher, dass der Zugriff auf ein Passwort erst von einer oder mehreren Rollen genehmigt werden muss. Erst durch erteilte Freigabe können Personen auf Passwörter und Accounts zugreifen. Wenn Passwörter mit einem zusätzlichen Sichtschutz kombiniert werden, können Mitarbeitende die Passwörter nur verschlüsselt zum Login verwenden, jedoch nicht im Klartext sehen. So bleiben Passwörter auch bei Spionage und Social Engineering Attacken sicher. Wenn Mitarbeitende das Unternehmen verlassen, müssen zudem Passwörter von geteilten Accounts nicht ausgetauscht werden.

Alle Handlungen und Freigaben in Password Safe werden zudem dokumentiert, revisions sicher im Logbuch gespeichert und können in Form von Berichten exportiert werden. So besteht hoher Passwort-Schutz und hohe Nachvollziehbarkeit für Audits.

Den Zugriff auf Passwörter von überall sicher gewährleisten

In Banken arbeiten Kundenbetreuer an unterschiedlichen Terminals, müssen häufig ihren Standort wechseln und sich jedes Mal erneut im System einloggen. Zusätzlich arbeiten sie oftmals an diversen Standorten im In- und Ausland. Da vor allem Finanzinstitute digital eng vernetzt sind, darf Sicherheit nicht lokal von Filiale zu Filiale gedacht werden.

Die skalierbare Architektur von Password Safe ermöglicht sicheres und schnelles Zugreifen auf Zugangsdaten in Password Safe von jedem Standort aus. Durch die Anbindung mehrerer Server bleibt die Performance gleichbleibend gut. Im Falle eines Ausfalls bleiben die Daten durch SQL-Clustering und -Cluster-Replikation sicher.

Schnell und sicher anmelden

Für mehr Sicherheit bei der Anmeldung an Password Safe kann ein zweiter Faktor hinzugefügt werden. So wird jeder einzelne Login doppelt abgesichert und die Identität kann durch eine Smartcard oder die Abfrage biometrischer Merkmale zweifelsfrei sichergestellt werden. Gleichzeitig ermöglicht Password Safe als Identity Provider auch die passwortlose Anmeldung an Anwendungen. Der Login an Password Safe selbst kann somit durch die Kombination eines Masterpasswortes mit einem FIDO-2-konformen Token oder einer Smartcard passwortlos erfolgen.

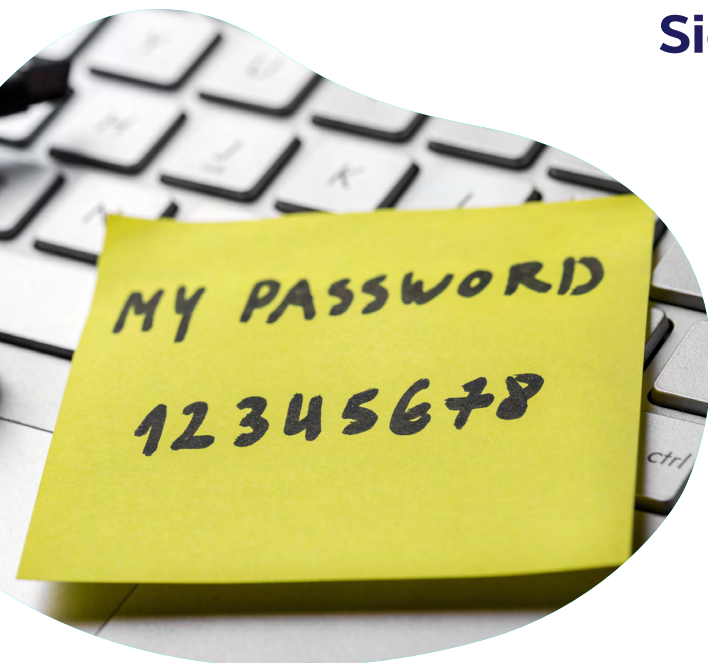


Vertrauen ist gut – Sicherheit besser

Ein häufiges Einfallstor für Cyberkriminelle ist der Mitarbeitende selbst, der entweder böswillig oder in Unwissenheit die Sicherheit des gesamten Unternehmens gefährdet. Um das Risiko möglichst gering zu halten, sollten Mitarbeitende gemäß dem Least-Knowledge-Principle nur Zugriff auf Daten haben, welche sie zum Arbeiten zwingend benötigen.

BaFin: „Das Berechtigungskonzept sollten nach dem Sparsamkeitskonzept funktionieren.“

Password Safe basiert auf diesem Sicherheitsansatz: Mitarbeitende haben nur Zugriff auf die Daten, Accounts und Passwörter, die zum effizienten Arbeiten unbedingt benötigt werden. Die Rechte werden rollenbasiert bestimmten Gruppen von Mitarbeitenden gewährt (RBAC) und können ebenso unkompliziert wieder entzogen werden.



Sicherheit ganzheitlich gedacht

Ein unsicheres oder auf einem Post-it notiertes Passwort genügt schon, um Hackern Zugang zu betrieblichen Geheimnissen zu gewähren. Gerade in der Finanzbranche ist es enorm wichtig, dass Mitarbeitende über alle Geräte und Anwendungen hinweg sichere Passwörter nutzen und verwalten können.

Mit Password Safe können die Verwaltung und der sichere Umgang mit Zugangsdaten unabhängig von der Größe der Finanzeinrichtung und der damit verbundenen Anzahl von Lizenzen gewährleistet werden. Password Safe verringert durch komplexe Passwörter und abgesicherte Zugänge das Risiko von Cyberattacken. Investiere heute noch in umfassenden Passwortschutz und sichere dir so die Kunden von morgen.

**Kontaktiere uns und lass dich dazu beraten,
inwiefern Password Safe die richtige
Lösung für dich ist!**

Warum Password Safe?



Erfahrung

MATESO hat sich seit **2006** auf professionelles Enterprise Password Management fokussiert. Über **21 der Top 40 DAX-Unternehmen** sowie **10.000 Unternehmenskunden** mit Millionen Anwendern vertrauen in puncto Passwort-Schutz bereits auf Password Safe.



Umfassender Schutz

Mit dem Einfluss von über **20 Jahren Markterfahrung** ist die Lösung ganzheitlich auf die individuellen Sicherheitsanforderungen und -bedürfnisse von Unternehmen zugeschnitten. Alle Passwörter werden ganzheitlich im **Password Life Cycle** geschützt – vom Erstellen bis hin zum Archivieren dieser.



Made in Germany

Als Mitglied der TeleTrust Initiative »**IT-Security Made in Germany**« steht MATESO für vertrauenswürdige IT-Sicherheitslösungen, die den Anforderungen des deutschen Datenschutzrechts genügen, **DSGVO-konform** genutzt werden können und keine versteckten Zugänge enthalten.

MATESO GmbH

Daimlerstraße 15, D-86356 Neusäß

Web: www.passwordsafe.com

E-mail: sales@passwordsafe.de

Tel: +49 821 74 77 87-0



MATESO
PASSWORD SAFE