



Etablierte Multi-User-Technologie

HR Campus AG verwaltet Passwörter und vertrauliche Informationen effektiv und sicher.

Die HR-Services der HR Campus AG decken alle Aspekte des Human Capital Managements ab: Von der strategischen Managementberatung über die Implementierung marktführender HR-Lösungen bis hin zu umfassenden Cloud Services für die Saläradministration, das Dokumenten- oder Talentmanagement. Gegründet 1998, betreut das Unternehmen mit Sitz in Dübendorf derzeit über 500 Kunden und kann auf 5.000 erfolgreich realisierte Projekte zurückblicken. Den Status als erster zertifizierter Reselling- und Beratungspartner von SAP in der Schweiz unterstreichen offizielle Zertifizierungen: z. B. SAP Gold Partner, SAP Recognized Expertise in HCM sowie SAP Recognized Expertise in HR Cloud Solutions.



*Daniel Burgener
Chief Technology Officer
HR Campus AG*

Vertrauen als Basis für Zusammenarbeit

Mit 95 erfahrenen Mitarbeitern ist HR Campus in der Lage, Kunden bei jeder Aufgabe durch hochkompetente Spezialisten zu unterstützen. Unter den Klienten finden sich KMUs genauso wie grosse Unternehmen und Banken. Insbesondere für letztere gelten höchste Compliance für Windows 7 Standards, die seitens des Dienstleisters ebenfalls erfüllt werden müssen. Schliesslich arbeiten dessen Berater und Teams oftmals mit sensiblen Informationen. Ein entsprechendes Sicherheitskonzept ist daher unerlässlich. Dies gilt nicht nur für das Netzwerk bei HR Campus selbst, sondern auch für die Sicherheit von Passwörtern, mit denen interne User auf die Datenbanken im Business Center zugreifen.

Schon seit Längerem war auf Notebooks und Smartphones der HR Campus User die Open Source-Software KeePass Password Safe als Stand-alone-Lösung installiert. Eine interne Richtlinie verpflichtete zu deren Nutzung, konnte jedoch nicht in jedem Fall verhindern, dass Passwörter in den Applikationen selbst gespeichert oder auf Notizzetteln abgelegt wurden. Was der IT-Abteilung zudem Kopferbrechen bereitete, war ein mögliches Worst-Case-Szenario: Ohne zentrale Steuerung über einen Password Server bestand ein höheres Risiko, dass Password Files, vertrauliche Informationen oder gar Zugangsdaten zu Kundensystemen durch einen ausscheidenden Mitarbeiter missbräuchlich kopiert werden.

“Wir haben nach einem Password Server gesucht, mit dem wir Zugriff und Aktivitäten auf privilegierte Konten schützen, verwalten, automatisieren und protokollieren können.”



Pleasant Password Server

Stressfrei. Unkompliziert. Effizient und zeitsparend.



Hauptsitz der HR Campus AG in Dübendorf

Zentral ist besser als lokal

Um künftig eine zentrale Steuerung des Benutzerzugriffs zu realisieren, suchte Projektleiter Stefan Jurt, System Engineer in der IT-Abteilung von HR Campus, nach einer server-basierten Lösung, die sowohl im internen Netz als auch über das Web gleichermaßen sicher arbeitet: „Wir haben uns fünf Lösungen angesehen, zwei teilweise installiert und uns dann mit guten Gründen für Pleasant Password Server entschieden.“

Ausschlaggebend für ihn war zum einen, dass die User mit KeePass bereits vertraut waren und mit der benutzerfreundlichen Oberfläche gut zurecht kommen. Zum anderen bietet Pleasant Password Server zu überschaubaren Kosten genau die Funktionalitäten, die tatsächlich gebraucht werden. „Weniger komplex als andere Produkte lässt er sich einfach konfigurieren und bietet ausreichende Sicherheit durch SSL-geschützte Verbindungen“, so Stefan Jurt.

Weniger Risiken, mehr Produktivität

Trotz des hohen Sicherheitsstandards müssen sich User jetzt nur noch ein Master Password merken, wobei der Administrator die volle Kontrolle besitzt. Die von ihm in Abstimmung mit dem jeweiligen Teamleiter sowie dem Security Officer zugewiesenen hierarchischen Benutzerrollen steuern automatisch den Zugriff auf Passwörter und vertrauliche Daten. Alle Prozesse sind strukturiert, dokumentiert und damit nachvollziehbar. Und das in Echtzeit.

Kosteneffiziente Dauerlizenz mit Support

Bis zur Einführung der neuen Password Management-Lösung vergingen drei Monate. Nicht etwa weil Pleasant Password Server aufwändig zu installieren und konfigurieren wäre – dafür genügte lediglich ein Tag. Neben der Erstellung eines detaillierten Sicherheitskonzeptes nahm man sich bei HR Campus zuvor allerdings die Zeit einer sorgfältigen Evaluation, Umsetzung und

Übergabe. Speziell die Berücksichtigung rechtlicher Sicherheitsaspekte in Abstimmung mit dem Security Officer und die teamweise durchgeführten Mitarbeiter-schulungen haben sich ausgezahlt. „Die gewachsene Akzeptanz bei den Usern freut mich ganz besonders“, betont IT-Leiter Daniel Burgener. Mitverantwortlich dafür mag die integrierte Pleasant Password App zur mobilen Kontaktdatenabfrage sein. Wichtiger für ihn ganz persönlich ist sicher der Produktivitätsgewinn und der geleistete First-Level-Support.



™ Pleasant Password Server ist eine Marke von Pleasant Solutions.

© Microsoft Windows ist eine eingetragene Marke der Microsoft Corporation.

1 KeePass ist eine OSI-zertifizierte Open Source-Lösung.