Passwörter erfreulich sicher

So einfach sichert die digital guru GmbH & Co. KG die Daten und Dokumente ihrer Kunden.

Je mehr Applikationen und Devices genutzt werden, desto mehr Passwörter werden vergeben. Das Speichern von Passwörtern in den Applikationen oder, schlimmer noch, auf den üblichen Notizzetteln, unterminiert die Sicherheit. Ein Passwort-Server löst das Problem. Ein erster Erfahrungsbericht des deutschen Softwareunternehmens digital guru GmbH & Co. KG mit Pleasant Passwort Server.

Es ist schon paradox. Je sicherer ein Passwort ist, desto komplexer ist es – und desto eher sind die Nutzer geneigt, das jeweilige Passwort entweder in der betreffenden Applikation zu speichern – oder, schlimmer noch, irgendwo in einer Textdatei oder auf einem Zettel zu notieren. Das Problem potenziert sich noch, je mehr Applikationen und verschiedene Geräte – PCs, Laptops, Tablet und Smartphones – verwendet werden.

Sicherheitslücken wachsen unbeobachtet

Die Konsequenz ist offensichtlich – die Sicherheit wird schleichend unterminiert. Das sieht auch Hildebrand Müller, Geschäftsführer des Softwareunternehmens digital guru in Osnabrück so: „Aus Gründen der Sicherheit ist es wirklich problematisch, die Passwörter auf den Rechnern oder mobilen Endgeräten der Mitarbeiter abzulegen.“

Hildebrand Müller
Geschäftsführer digital guru

„Aus Gründen der Sicherheit ist es problematisch, Passwörter auf Rechnern oder mobilen Endgeräten der Mitarbeiter abzulegen.“

Software für höchste Kundenzufriedenheit

Das Credo von digital guru ist, Software zu entwickeln, die problemlos funktioniert und Menschen dabei hilft, ihre Arbeit schneller, transparenter und einfach besser zu bewerkstelligen.

Die Produktpalette umfasst die Software GREYHOUND mit den Modulen CRM, DMS und Max – eine professionelle Komplettlösung für die Verwaltung sämtlicher Kommunikations- und Informationsprozesse in Unternehmen. Die Lösung wird von einer Vielzahl bekannter Unternehmen eingesetzt, darunter dress-for-less, babymarkt.de, billiger.de und viele mehr.

GREYHOUND® The Teamwork Company

Kunde: digital guru GmbH & Co. KG, Osnabrück

Branche: Software

Dazu Hildebrand Müller: „Wir müssen und wollen natürlich dafür sorgen, dass sowohl unsere als auch die Unterlagen unserer Kunden auf unseren Rechnern und Endgeräten nachhaltig geschützt sind. Wir haben uns daher schon früh mit der Absicherung von Passwörtern befasst.“

Keypass als solide Basis

Initial setzte digital guru auf Keepass Password Safe, eine Open Source-Software für die Verwaltung von Passwörtern. Keepass ist praktisch für alle Windows-Versionen sowie für Linux und Mac verfügbar. Darüber hinaus haben Drittanbieter Keepass Ports für Android und iOS Smartphones und Tablets, Windows Phone und andere Systeme entwickelt. Damit kann Keepass plattformübergreifend eingesetzt werden, eine wichtige Voraussetzung für die nachhaltige Steigerung der Sicherheit.

Keepass ist allerdings nur auf einzelnen Geräten nutzbar und kann seine Vorteile weder im Netzwerk noch über das Web ausspielen. Genau das war aber die Zielsetzung von digital guru. Dazu Hildebrand Müller: „Wir beschäftigen derzeit zwölf Mitarbeiterinnen und Mitarbeiter. Diese arbeiten abteilungsübergreifend, zudem sind wir dezentral organisiert. Das stellt hohe Anforderungen an die Sicherheit.“

Server-basierte Lösung, bezahlbar und sicher

Daher suchte Müller nach einer server-basierten Lösung für das Passwortmanagement, die im internen Netz als auch über das Web gleichermaßen schnell und sicher arbeitet. Hildebrand Müller erläutert: „Wir haben uns

Der Firmensitz der digital guru GmbH & Co. KG in Osnabrück

fünf Lösungen angesehen, zwei testweise installiert und uns dann für Pleasant Password Server entschieden“.

Hildebrand Müller fasst die wesentlichen Argumente für die Entscheidung für Pleasant Password Server zusammen – neben der Geschwindigkeit die komfortable Benutzeroberfläche, die Unterstützung von TCP/IP, die direkte Unterstützung von Keepass und letztlich die überschaubaren Kosten.

Zudem erfüllt Pleasant Password Server die von digital guru definierten Anforderungen an die Flexibilität und Leistungsfähigkeit. Das System bietet hohe Sicherheit gegen externe und interne Bedrohungen, ist in allen Lebenslagen schnell und verlässlich und unterstützt Windows, Macintosh sowie Android und iOS. Und das Beste: Trotz des hohen Sicherheitsstandards müssen sich die Nutzer nur noch ein Master-Passwort merken – und das führt aufgrund geringerem Supportaufkommen und vereinfachter Administration zu deutlichen Zeit- und Kosteneinsparungen.

Kostenlose Testversion gleich herunterladen von:
www.passwortserver.de
www.passwortserver.ch
www.passwortserver.at

[1] KeePass ist eine OSI-zertifizierte Open- Source-Lösung