Neuigkeiten, sicheres Login und allgemeine Sicherheitsaspekte zum Verhalten im Web

Buchungssystem für Ferienhäuser und Ferienwohnungen
Dieses Modul und seine Belegungspläne sind nun umfangreicher geworden und skalierbar, das bedeutet, dass ab sofort mehrere Objekte (bis zu 99) verwaltet und zur Anfrage/Buchung angeboten werden können.
Die Javascript-Engine
wurde überarbeite und erneuert.
Editor
Der im System integrierte Editor, der nicht nur bei der Seitenbearbeitung zum Einsatz kommt, wurde mit der neuesten Version versehen.
Login und Sicherheit
Neuerdings können die Zugangsdaten zum Adminbereich von "Pastos" wieder im Browser gespeichert werden. Das sollte allerdings nur genutzt werden, wenn der Browser mit einem Haupt- / Masterpasswort abgesichert ist, dazu weiter unten mehr.
Sicherheit im Web allgemein
In letzter Zeit häufen sich Berichte von Kunden, die Opfer einer Hackerattacke geworden sind. Ich schreibe diese Zeilen nicht als Fachmann, sondern aus meiner Sicht als Anwender. Ursache war dann immer fahrlässiges Nutzerverhalten, davor schützt auch ein Virenscanner nicht.
Übrigens, der bereits integrierte Virenschutz bei Windows und Apple ist sehr gut, eine zusätzliche App ist nicht nötig.
Es gibt natürlich einige Möglichkeiten, ihr Verhalten im Web sehr sicher zu gestalten. Dazu gehören auf jeden Fall Passwortmanager, die 2-Faktor-Authentifizierung/Authentisierung und Passkeys.
Einige Anbieter setzen auf schon seit einiger Zeit auf die 2-Faktor-Authentisierung (2FA), insbesondere wenn es um Geld geht. Es sollte allerdings vermieden werden, diese Methode, also **beide Faktoren auf einem Gerät**, dem Smartphone oder Tablet zu nutzen.
Passkeys ist ein noch relativ junges Verfahren, welches ein sicheres Login ganz ohne Passwort ermöglicht. Passkeys eines Anbieters lassen sich auch auf mehreren Geräten nutzen. Diese Methode ist der "Goldstandard" und ihr gehört wohl die Zukunft.
Im Sicherheitsranking folgt nach einem dezidierten Passwortmanager, ich empfehle Bitwarden als kostenlose Version, im Browser integrierte Passwortmanager. Ich persönlich nutze hierfür den Firefox, der ist noch ein Stück sicherer, als der im Google Chrome oder der im Microsoft Edge und wird nur knapp übertroffen vom Safari in der Macwelt.
Allerdings nur, wenn im Browser ein Hauptpasswort / Masterpasswort vergeben wird. Das ist dann nach jedem Browserneustart einzugeben.
Über ein Benutzerkonto bei Firefox lassen sich die Passwörter, aber auch die Lesezeichen geräte- und systemübergreifend synchronisieren und nutzen, egal ob Android, MacOs, Windows oder Linux.
Und zu guter Letzt, aber enorm wichtig:
Nutzen Sie nie, wirklich niemals, das Passwort Ihres E-Mail-Accounts bei Logins auf irgendwelchen Websites. Leider häufen sich in letzter Zeit die Leaks auch bei großen seriösen Anbietern, weil die wider aller Sicherheitsaspekte die Passwörter in ihren Datenbanken immer noch im Klartext speichern. Nicht nur Hacker haben dann ein leichtes Spiel, auch Mitarbeiter dieser Dienste könnten die Passwörter einsehen.
In unserem "Pastos" gibt solch eine fahrlässige Speicherung der Passwörter schon seit ca. 15 Jahren nicht mehr. Deshalb können wir bei vergessenen Passwörtern unseren Kunden nicht direkt weiterhelfen, sondern müssen auf die "Passwort vergessen" Funktion verweisen.