syBOS-Serie / Teil 11:

Upgrade auf syBOS Version 3.00 (1709)

Mit der Version 3.00 vom Verwaltungssystem syBOS eröffnen sich viele neue Möglichkeiten, inklusive der Nutzung auf Handys oder Tablets.

Ebenfalls ergeht in dem Beitrag ein eindringlicher Hinweis, Passwörter nicht weiterzugeben; Stichwort „Social Hacking“.

Von Florian Schmidt, IT Oö. LFV

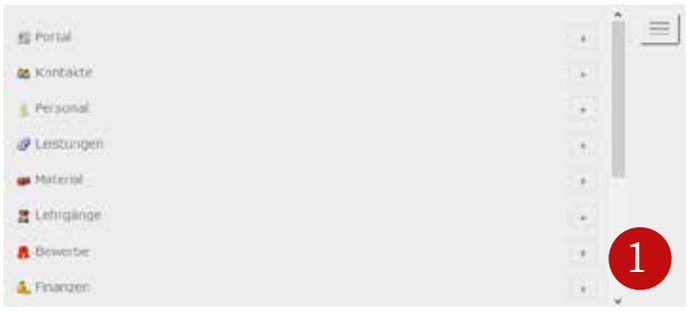
In den letzten Jahren verbreiteten sich Tablets und Smartphones immer weiter. Kaum jemand besitzt nicht zumindest eines dieser Gadgets. Daher war es ein logischer Schritt, syBOS für die Nutzung dieser Geräte zusätzlich zu optimieren. Neben einer neuen Benutzeroberfläche mit der bereits bekannten Menüstruktur und Bedienung wurden auch einige Funktionen im Detail verbessert.

Moderne Benutzeroberfläche im „Responsive Design“

Durch die Einführung des „Responsive Designs“ passen sich die Inhalts- und Navigationselemente an die Bildschirmauflösung des aktuell verwendeten Gerätes an. Dies ermöglicht die einfache Bedienung auf Geräten mit kleinen Bildschirmen wie Tablets und Smartphones.

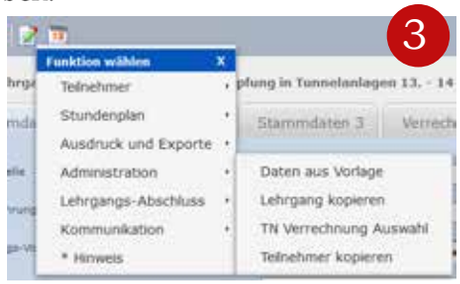
Neuerungen

- Widgets im Portal können einfach per „Drag & Drop“ verschoben werden (ausgenommen News, Verwaltung, Benutzer und Online).
- Das Hauptmenü wird auf kleinen Bildschirmen ausgeblendet und kann durch einen Button rechts oben (Toast Button) ausgeklappt werden - *siehe Abbildung 1.*



- Reicht die Bildschirmbreite nicht zur Darstellung aller Tabs aus, wird rechts ein Pfeil angezeigt. Nach einem Klick hierauf wird ein Drop-Down Menü mit den restlichen Reitern angezeigt - *siehe Abbildung 2.*

- Die Inhalte in den Reitern werden normal in zwei Spalten angezeigt. Bei Bedarf wird die zweite Spalte unter die erste verschoben.
- Funktionen in den Menüs wurden in Untermenüs zusammengefasst - *siehe Abbildung 3.*



Sicherheit

Im syBOS werden viele, teils **sensible und personenbezogene Daten** gespeichert. Um Unbefugten einen unberechtigten Zugriff auf diese zu verwehren, werden persönliche Benutzer mit Passwörtern verwendet. Leider hört man in den Medien oft von „Hackingangriffen“ auf diverse Datenbanken, wo Millionen persönliche Daten „gestohlen“ wurden (gestohlen ist nicht der ganz korrekte begriff, da die Daten ja noch in der Datenbank sind, sie wurden meist nur repliziert). In vielen dieser Fälle wurden nicht die Sicherheitssysteme der Dienste aufgrund von Sicherheitslücken umgangen, sondern entweder zu einfache Passwörter durch **„Brute-Force“** (z.B. „Wörterbuchattacken“) oder **„Social-Hacking“** erbeutet.

Was ist „Social-Hacking“? Hier ein Beispiel: Ein „Techniker“ ruft an und bittet um die Durchsage der Benutzernamen und Passwörter, weil ein technisches Problem vorliegt und er zur Behebung diese Daten „gegenprüfen“ muss – meist mit Zeitdruck!
Wie kann man nun solche Sicherheitslücken stopfen? Bei „Social-Hacking“ hilft nur der gesunde **Hausverstand**. Das Landes-Feuerwehrkommando oder einer seiner Partner fragt nie nach Zugangsdaten für syBOS, Office365 oder anderen Diensten! Sie würden ja auch

Brennpunkt_5_2017.indd 64 21.09.2017 09:29:17

NIE EINEM FREMDEN IHRE BANKOMATKARTE + PIN AUSHÄNDIGEN?!

Gegen **„rohe Gewalt“ (= „Brute-Force“)** helfen nur sehr lange und komplexe Passwörter. Das schränkt die Benutzerfreundlichkeit massiv ein. Daher wurde die Passwortabfrage um einen zweiten Faktor erweitert („2-Faktor Autentifizierung“). Der erste Faktor „Wissen (= Passwort)“ wird um den zweiten Faktor „Besitzen (USB-Key, Smartphone, …)“ erweitert. Dadurch muss der Angreifer nicht nur das Passwort „erraten“, sondern ebenfalls einen geheimen, ständig wechselnden Schlüssel.

Wie sieht das dann in der syBOS-Praxis aus?

Nach der gewohnten Eingabe des Benutzernamens und des Passworts wird der Benutzer nach dem „Einmalpasswort“ gefragt. Dieses kann entweder durch einen Hardware-Token (Spezieller USB-Stick mit einem Knopf zum Erzeugen) oder ein Smartphone mit OTP-App erzeugt werden. Danach kann man wie gewohnt in syBOS arbeiten *(siehe Abbildung 4)*.

4

Hinweis: Hierbei handelt es sich um eine optionale Funktion, welche standardmäßig deaktiviert ist. Auf Wunsch des Benutzers kann diese unter Portal → Einstellungen → „Passwort ändern“ aktiviert werden.

Weitere Neuerungen in Version 3.00 (1709)

- **WebCalendar – Schnittstelle**
  Ausführlicher Artikel mit Beispielen in der nächsten Brennpunkt -Ausgabe 6/2017
- **Export-Einstellungen speichern**
  Bei Exporten wie zum Beispiel dem Adressen-Export in der Personal-Liste oder Einsatz-Export besteht die Möglichkeit, die ausgewählten Spalten zu speichern und später wieder zu laden.
- **Kopieren von Tätigkeiten**
  Eine Tätigkeit kann kopiert werden. Dazu gibt es in der Liste ein Kopieren-Symbol.
- **Einsätze: Zeiten übernehmen**
  Die Funktion „Zeit übernehmen“ bietet nun verschiedene Auswahlmöglichkeiten. Bei „Material“ kann jedes Feld der Stammdaten selektiert werden, ebenso kann jedes Fahrzeug einzeln ausgewählt werden.
- **E-Mail-Konten-Signatur**
  Es kann zu jedem Konto eine eigene Signatur erstellt werden.
- **Auswahl der Dienststelle**
  Die Dienststelle kann bereits auf der Portalseite geändert werden. Somit werden die Inhalte der Widgets aufgrund der Auswahl angepasst, wie beispielsweise Veranstaltungen, Einsätze, usw.

Brennpunkt_5_2017.indd 65 21.09.2017 09:29:17