Sicherheit von Webseiten der Abteilungen

Merkblatt zur Verbesserung der Sicherheit und zur Verhinderung eines möglichen Zugriffs durch fremde Personen

Folgende Massnahmen dienen dazu, die Sicherheit der eigenen Pfadiwebseite zu verbessern. In diesem Dokument wird auf allgemeine Punkte eingegangen. Je nach eingesetztem Basissystem sind weitere Sicherheitsvorkehrungen erforderlich. Eine regelmässige Kontrolle der eigenen Website ist unbedingt notwendig, um mögliche Manipulationen frühzeitig zu erkennen und rückgängig zu machen.

Basissystem

- Basissystem, wie auch Erweiterungen und Zusatzprogramme, regelmässig updaten und auf dem neusten Stand halten.
- Newsletter der Hersteller abonnieren, um auf Sicherheitslücken und Updates aufmerksam zu werden.
- regelmässig Backup der Website durchführen
- Wiederherstellung auf Basis des Backups testen
- Sicherheitsempfehlungen der Hersteller des Basissystems wenn möglich implementieren
- Berechtigung innerhalb des Filesystems, welcher das Ausführen von Fremdsoftware (Scripts etc.) zulässt, kontrollieren und dieses entsprechend verhindern
- falls Dienste auf dem System freigeben werden müssen (SSH, SFTP etc.) folgendem Leitsatz folgen: Soviel wie nötig – so wenig wie möglich
- sobald Passwörter übertragen werden, ausschliesslich verschlüsselte Protokolle verwenden

Zugriff auf die eigene Website

- Benutzergruppen je nach Funktion mit den dazugehörigen Rechten erstellen. Jemand, der lediglich Inhalte einer Website veröffentlicht oder ändert, braucht keine Systemverwalterrechte.
- Alle Systemverwalter sollten keine einfachen Passwörter verwenden können. Mindestens 10 Zeichen mit Sonderzeichen und Zahlen sollten Pflicht sein.
- Zugriff auf wichtige Systemeinstellungen nur Personen gewähren, welche instruiert sind und abschätzen können, welche Änderung die Einstellungen bewirken.
- Diesen Personen einen persönlichen Login geben, keine allgemeinen verwenden
- Personen den Zugriff entziehen, sobald dieser nicht mehr benötigt wird