Plesk-Checkliste

Nur Webanwendungen die folgenden Sicherheitsanforderungen entsprechen können für die weltweite Nutzung freigegeben werden:

- Die Webanwendung ist auf dem neuesten Stand
- Alle Plug-In-Updates müssen regelmäßig installiert werden
- Administrative Verzeichnisse müssen Passwortgeschützt sein
- Administrative Passwörter müssen einen hohen Komplexitätsgrad aufweisen

Um sicherzustellen, dass Ihre Webanwendung den Sicherheitsanforderungen entspricht, folgen Sie bitte folgender Checkliste:

1	**Ändern Sie das Passwort des Benutzers, mit dem Sie auf die Plesk-Verwaltungsoberfläche zugreifen.**
	Nach der Anmeldung in Plesk klicken Sie auf „Account" in der Hauptnavigation und danach auch „Mein Profil". Setzen Sie ein neues Passwort und speichern Sie. Bitte verwenden Sie Passwörter die über 8 Zeichen haben und Groß/Klein-Schreibung, Zahlen und Sonderzeichen enthalten.
2	**Ändern Sie alle Datenbankpasswörter, und passen Sie die Konfiguration der Webanwendung entsprechend an**
	Klicken Sie auf „Websites & Domains". Klicken Sie auf der rechten Seite auf das Symbol „Datenbanken". Wählen Sie Ihre Domäne. Wählen Sie die Reiterkarte „Nutzer". Wählen Sie den Benutzer aus. Setzen Sie ein neues Passwort. Bitte verwenden Sie Passwörter die über 8 Zeichen haben und Groß/Klein-Schreibung Zahlen und Sonderzeichen enthalten. Dieses Passwort müssen Sie nun auch in der jeweiligen Webanwendung eintragen. Wiederholen Sie das für alle Ihre Webanwendungen und Datenbanken.
3	**Ändern Sie die Passwörter von allen administrativen Nutzern die in den Webanwendungen der gehosteten Webdomain hinterlegt sind**
	Passwörter werden oft von Angreifern durch spezielle Techniken erraten. Melden Sie sich bitte in Ihrer Webanwendung als Administrator an. Ändern Sie das Passwort von allen Benutzern, die eine administrative Funktion haben. Bitte verwenden Sie Passwörter die über 8 Zeichen haben und Groß/Klein-Schreibung, Zahlen und Sonderzeichen enthalten.
4	**Prüfen Sie ob die vorhandenen administrativen Nutzer in den Webanwendungen tatsächlich die Ihrigen sind. Gibt es evtl. Nutzer, die Sie gar nicht angelegt haben?**
	Benutzerkonten, die Ihnen unbekannt sind oder ungenutzt bleiben sind ein Sicherheitsrisiko. Bitte achten Sie besonders auf administrative Benutzer, die Sie selbst nicht erstellt haben. Entfernen Sie unbekannte oder überflüssige Benutzer aus der Webanwendung.
5	**Nutzen Sie nach Möglichkeit die aktuellen Webapplikationen aus dem AppVault des Plesk-Servers**
	Das Plesk System verfügt über eine Ansammlung von Webanwendungen, die automatisiert installiert werden können. Diese Anwendungen werden dann vom Plesk System verwaltet und können darüber automatisiert aktualisiert werden. Welche Webanwendungen vom Plesk unterstützt werden, können Sie unter dem Punkt „Applikationen" im Hauptmenü sehen. Finden Sie eine Anwendung nicht, sprechen Sie uns an.
6	**Aktualisieren Sie die Webanwendung auf die aktuellste Version**
	Alte Versionen von Webanwendungen zeichnen sich durch zahlreiche Sicherheitslücken aus. Installieren Sie die neueste Version der Webanwendung bzw. alle vorhandenen Updates für die aktuelle Version. Vergessen Sie nicht auch alle Plug-Ins der Webanwendung zu aktualisieren.
7	**Löschen Sie alte Webanwendungen, die Sie nicht mehr brauchen**
	Haben Sie Webanwendungen die Sie nicht mehr aktiv nutzen? Machen Sie ein Offline-Backup der Webanwendung und löschen Sie diese danach vom Plesk-System.

8	**Überprüfen Sie das Dateisystem nach ungewöhnlichen Dateien. Liegt dort irgendetwas herum, was da nicht hingehört?**
	Angreifer hinterlassen Spuren. Oft sind das Verzeichnisse oder Dateien mit ungewöhnlichen Bezeichnungen und Inhalten. Wenn Sie etwas Verdächtiges finden, melden Sie das bitte umgehend der Campus IT. Überprüfen können Sie Ihre Dateien entweder mit einem FTP-Client oder im Plesk-System machen. Im Plesk finden Sie Ihre Dateien, wenn Sie im Hauptmenü auf „Dateien“ klicken und dann die gewünschte Domäne auswählen.
9	**Überprüfen Sie die Datei- und Verzeichnisberechtigungen**
	Anwendungsdateien sollten nicht für alle zugreifbar oder ausführbar sein. Passen Sie die Dateiberechtigungen nach den Bedürfnissen der jeweiligen Webanwendung an. Meistens reicht es die Berechtigungen auf 755 gesetzt sind. Das können Sie entweder mit einem FTP-Client oder im Plesk-System machen. Im Plesk finden Sie Ihre Dateien, wenn Sie im Hauptmenü auf „Dateien“ klicken und dann die gewünschte Domäne auswählen.
10	**Setzen Sie den Verzeichnisschutz auf die administrativen Bereiche der Webanwendung**
	Der Verzeichnisschutz bietet eine zusätzliche Sicherung von kritischen Bereichen Ihrer Webanwendung. Alle Verzeichnisse in der sich die administrativen Teile der Webanwendung befinden sollten dadurch abgesichert werden. Das können Sie im Plesk-System machen, indem Sie unter „Websites & Domains“ Ihre Domäne auswählen und dann auf „Passwortgeschützte Verzeichnisse“ klicken.
11	**Prüfen Sie Ihre Website, ob alle Funktionen ordnungsgemäß funktionieren. Es wird jetzt PHP in der Version 5.4 genutzt.**
12	**Entfernen Sie den Verzeichnisschutz für die ganze Domäne und senden Sie die Informationen zur Selbstauskunft an den Service-Desk der Campus IT**
	support@campus-it.fh-koeln.de