Newsletter

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Informationen für betriebliche Datenschutzbeauftragte
und IT-Verantwortliche in kirchlichen Dienststellen

Nr. 03/2017

Abgesicherte Version von WordPress installieren!

WordPress ist das beliebteste Programm zur Gestaltung von Websites. Es wird auch im kirchlichen Bereich häufig eingesetzt. In jüngster Zeit ist diese Software vermehrt erheblichen Angriffen ausgesetzt worden. So wurde eine Sicherheitslücke ausgenutzt, um Beiträge und Kommentare zu verunstalten. Nunmehr versuchen Angreifer durch das Verschieben von PHP-Code auf Webseiten eine Hintertür einzurichten, durch die sie sich Zugang zur kompromittierten Website verschaffen. Es existiert bereits eine abgesicherte Version von WordPress mit der Nummer 4.7.2, die dies verhindert. **Sie sollte daher dringend installiert werden!**

→ heise Security Meldung vom 14.02.2017: „Jetzt patchen! Angriffe auf WordPress-Seiten nehmen zu und werden gefährlicher“

Zwei-Faktor-Authentifizierung für WhatsApp nutzen!

Seit wenigen Tagen stellt WhatsApp eine Zwei-Faktor-Authentifizierung zur Verfügung. Hierdurch wird das Kapern von Accounts verhindert. Es ist nunmehr nicht mehr möglich, die SIM-Karte in ein anderes Gerät zu stecken, um auf diese Weise, wie bisher, den Zugriff auf das WhatsApp-Konto zu erlangen. Bei der Nutzung von WhatsApp wird der Zugang zum Konto standardmäßig nicht durch ein Passwort geschützt, sondern nur über den Besitz des Gerätes und der Telefonnummer, mit der es angemeldet wurde. Erst jetzt wird eine PIN hinzugefügt, die als zweiter Faktor zur Sicherheit beiträgt. Gleichzeitig kann eine Mail-Adresse hinterlegt werden, über die sich die Zwei-Faktor-Authentifizierung wieder abschalten lässt. Einzelheiten hierzu sind dem Artikel auf heise Security zu entnehmen.

→ Meldung von heise Security vom 10.02.2017: „WhatsApp schaltet Zwei-Faktor-Authentifizierung für alle frei“

Der Einsatz diese Software auf Geräten mit iOS- oder Android-Software ist im beruflichen Bereich nach wie vor kritisch. Es bleibt nach wie vor bei der Übertragung von Adressdaten an Facebook! Sollten aber Dienststellen wegen der hohen Verbreitung dieses Programms nicht auf den Einsatz von WhatsApp verzichten können, sollten alle erdenklichen Sicherheitsmaßnahmen ergriffen werden. Hierzu gehört auch die Zwei-Faktor-Authentifizierung!

BSI: Sicheres Android unter Samsung Knox

Das Betriebssystem „Android“ für Smartphones und Tablets bietet von Hause aus keine ausreichende Sicherheitsstruktur. Daher bleibt es den Geräteherstellern überlassen, durch eigene Erweiterungen hier gangbare Lösungen zu finden. Der in diesem Bereich erfolgreichste Anbieter, die Firma Samsung stellt hierfür eine eigene Sicherheitsplattform unter der Bezeichnung „Knox“ zur Verfügung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat nunmehr Sicherheitsempfehlungen zur Konfiguration von Samsung-Geräten mit Knox herausgegeben. Der Leitfaden zeigt auf, wie sich solche Geräte sichern lassen.

→ BSI: „Sicherheitsempfehlungen zur Konfiguration von Samsung Knox“

→ Hierzu auch Meldung von heise Security vom 09.02.2017

Die Schrift umfasst 44 Seiten und geht auf folgende Themen ein:

1. Beschreibung
2. Gefährdungen für mobile Android-Geräte
3. Härtungsmaßnahmen für Samsung Knox
4. Härtungsguide
5. Konfiguration von My Knox

Es wird den verantwortlichen Administratoren empfohlen, die Sicherheit durch Konfiguration von Samsung-Handys mit Knox an Hand dieser Sicherheitsempfehlungen zu überprüfen, beziehungsweise erstmalig vorzunehmen.

Hinweis:

Sie erhalten dieses E-Mail mit dem Newsletter im Anhang, da Sie ihn auf unserer Website abonniert haben. Sollte dies versehentlich erfolgt sein oder kein Bedarf mehr besteht, so teilen Sie und dies bitte in einem Antwortmail unter dem Stichwort „Abbestellung" mit.

Herausgeber:

Der Diözesandatenschutzbeauftragte der norddeutschen Bistümer, info@datenschutz-katholisch-nord.de