Newsletter

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Informationen für betriebliche Datenschutzbeauftragte
und IT-Verantwortliche in kirchlichen Dienststellen

Nr. 09/2017

Dringende Warnhinweise

Die Redaktion von heise online macht auf folgende Gefährdungen aufmerksam:

Gefährdeter Datenschutz: Firefox löscht lokale Datenbanken nicht
Es wird darauf hingewiesen, dass der Mozilla-Browser die durch Websites gespeicherten Daten nicht vollständig beseitigt. Auch nach Aufräumen der Chronik kann eine Webseite mühelos auf die zuvor im Browser gespeicherten Daten zugreifen! Der Grund liegt in einer falschen Implementierung von „IndexedDB". Auch Voreinstellungen wie „Blockieren" oder „Jedes Mal nachfragen" werden ignoriert, so dass sich diese Fehlfunktion nicht umgehen lässt. Als Maßnahme hiergegen ist über das Entwicklerwerkzeug (Reiter „Storage") die IndexedDB zurückzusetzen.

→ *heise online Meldung vom 19.09.2017*

Achtung: Aktuelle Spam-Mails fälschen Absender von Mitarbeitern
Eine neue Schädlingswelle verbreitet Malware via E-Mails. Dabei wird auf starke Personalisierung gesetzt. Sie täuscht real existierende Mail-Verbindungen von Mitarbeitern des gleichen Unternehmens vor. Der Text enthält einen Link, durch den ein Word-Dokument mit angeblich angeforderten Informationen geöffnet wird. Dadurch wird schädlicher Makro-Code übertragen. Das CERT-Bund warnt ebenfalls vor den meist als Rechnungen gestalteten Dokumenten, die den Trojaner Emotet verbreiten sollen.

→ *heise online Meldung vom 18.09.2017*

Backdoor in CCleaner ermöglichte Fernzugriff - Update dringend empfohlen
Die Version 5.33.6162 des Säuberungs- und Optimierungstools CCleaner sollte zügig auf die neue Version 5.34 gebracht werden. Es besteht ansonsten die Gefahr, dass verschlüsselter Schadcode in die Initialisierungsroutine des Programms eingeschleust wird.

→ *heise online Meldung vom 18.09.2017*

Verschlüsselt telefonieren mit Threema

In unserem Newsletter 7/2017 hatten wir über die Beta-Phase zur Erweiterung der Funktionalität der Messenger-App Threema zum verschlüsselten Telefonieren berichtet. Nachdem diese mit Erfolg beendet worden ist, sind Sprachanrufe ab jetzt für alle Nutzer von iOS- und Android-Geräten freigeschaltet (siehe Meldung von heise online vom 15.09.2017). Eine Rufnummer wird dafür nicht gebraucht. Zur Erinnerung: alle Sprachanrufe sind dabei Ende-zu-Ende verschlüsselt und werden über die Threema-ID aufgebaut. Heise weist weiter daraufhin, dass in Folge der verwendeten einheitlichen Bitrate bei der Audio-Codierung der übermittelten Datenpakete keine Rückschlüsse auf den Inhalt möglich sind.

→ *heise online Meldung vom 15.09.2017*
→ *Weitere Informationen hierzu unter https://threema.ch/de/threema-anrufe*

Funktionserweiterung des Messengers Signal

Auch der Messenger Signal der Firma „Open Whisper Systems“ ist unter datenschutzrechtlichen Gesichtspunkten ein vertrauenswürdiges Kommunikationsprogramm. Auch hier wird die Ende-zu-Ende Verschlüsselung zur Übertragung von Nachrichten eingesetzt. Dabei werden Textnachrichten, Telefongespräche über Internetverbindungen, SMS und MMS erfasst. Es werden auch verschlüsselte Gruppenunterhaltungen ermöglicht, falls alle Teilnehmer bei diesem Gespräch Signal einsetzen. Zudem kann das Programm die Datenbank am eigenen Gerät ebenfalls verschlüsseln, so dass die gespeicherten Nachrichten nur nach Eingabe eines Passworts gelesen werden können.

→ *Eine genaue Darstellung findet sich auf Wikipedia*

Nach Meldung von heise security ist nunmehr eine Beta-Version erschienen, die es den Nutzern von iOS- und Android-Geräten ermöglicht Profiltexte und Nutzerfotos zu erstellen. Sie werden ebenfalls mit einem eigenen Schlüsselpaar Ende-zu-Ende verschlüsselt und gespeichert. Nur autorisierte Kontakte haben Zugriff hierauf, nicht jedoch der Anbieter oder Dritte. Im Falle einer Konversation erhalten die Kommunikationspartner dann automatisch den Schlüssel zu den Profildaten. Sie können in diesem Fall nicht nur mit Hilfe des Anfangsbuchstabens ihren Gesprächspartner ermitteln, sondern auch über den Einblick in die Profildaten und das Foto. Dabei ist eine bessere Kontrolle darüber möglich, mit wem sie sich austauschen. Der Empfänger der Profildaten kann jedoch entscheiden, ob auch seine Profildaten übermittelt werden.

Für den Fall, dass die neue Version getestet werden soll, muss den Entwicklern eine Mail übersandt werden, um in das Beta-Programm aufgenommen zu werden.

→ *heise security Meldung vom 08.09.2017*

Der Diözesandatenschutzbeauftragte

des Erzbistums Hamburg, der Bistümer Hildesheim, Osnabrück
und des Bischöflich Münsterschen Offizialats in Vechta i.O.

Schwachhauser Heerstraße 67 – 28211 Bremen – Tel.: +49 (421) 16 30 19 25
Mail: info@datenschutz-katholisch-nord.de – Internet: https://www.datenschutz-kirche.de

Verantwortlich i.S.d. Pressegesetzes: Andreas Mündelein