Newsletter

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Informationen für betriebliche Datenschutzbeauftragte
und IT-Verantwortliche in kirchlichen Dienststellen

Nr. 02/2017

Microsoft speichert Office 365 Daten in Deutschland

Microsoft hat am 24. Januar „Office 365 Deutschland“ gestartet mit dem Versprechen, besonders strenge Datenschutz- und Compliance-Richtlinien einzuhalten. Dabei werden die Daten in einer deutschen Cloud gespeichert, bei der sich die Rechenzentren in Frankfurt a.M. sowie in der Nähe von Magdeburg befinden. Insoweit ist deutsches Datenschutzrecht (künftig Europäisches Datenschutzrecht) obligatorisch anzuwenden. Sichergestellt werden soll das dadurch, dass die Verwaltung der Rechner durch einen Treuhänder, die Deutsche Telekom erfolgt. Das Angebot richtet sich daher vor allem an Unternehmenskunden, den Öffentlichen Dienst und Bildungseinrichtungen.

→ Microsoft: Office 365 Deutschland

Eine genaue Aufstellung der Angebote und Preise hierfür sind ebenfalls von Microsoft veröffentlicht worden:

→ Microsoft: Pläne und Preise

Microsoft muss keinen Zugriff auf Nutzerdaten im Ausland erlauben

Passend zu der vorangegangenen Meldung ist die Entscheidung, die ein US-Berufungsgericht über eine erneute Anhörung im Fall Microsoft ./. United States getroffen hat. Es hatte im Juli 2016 festgestellt, dass amerikanische Behörden Microsoft nicht zwingen können, Nutzerdaten aus europäischen Rechenzentren herauszugeben. Zur Begründung wurde angegeben, es handele sich um eine exterritoriale Angelegenheit, die von den örtlich zuständigen Behörden entschieden werden müsste. Die Staatsanwaltschaft hatte aufgrund von Bedenken zur Aufrechterhaltung der Sicherheit des Landes, eine erneute Anhörung beantragt. Hierfür war jedoch keine Mehrheit der Richter zu finden, so dass die ursprüngliche Entscheidung bestehen bleibt.

→ Meldung von heise online vom 25.01.2017
→ Meldung von Zeit Online vom 25.01.2017

Warnungen des BSI

Das Bundesamt für Sicherheit in der Informationstechnik hat folgende Warnmeldungen veröffentlicht, die das Apple-System betreffen:

1. 24.01.2017: macOS Sierra. Mehrere Schwachstellen ermöglichen die Ausführung beliebigen Programmcodes mit Kernelprivilegien. Risikostufe 4 (hoch). Hierzu sollte umgehend das Security Update macOS Sierra 10.12.3 installiert werden. → CB-K17/0124
2. 24.01.2017: iTunes. Mehrere Schwachstellen ermöglichen das Ausführen beliebigen Programmcodes. Risikostufe 4 (hoch). Betroffene Systeme: Microsoft Windows 7, 8.1, 10. Nutzer sollten daher schnellstmöglich iTunes 12.5.5 installieren. → CB-K17/129
3. 24.01.2017: iCloud for Windows 6.1. Mehrere Schwachstellen ermöglichen die Ausführung beliebigen Programmcodes. Risikostufe 4 (hoch). Betroffene Systeme: Microsoft Windows 7, 8.1, 10. Nutzer sollten dringend das Security Update 6.1.1 installieren. → CB-K17/0130

4. 24.01.2017: Apple iOS 10.2. Mehrere Schwachstellen ermöglichen die Ausführung beliebigen Programmcodes mit Kernelprivilegien. Risikostufe 5 (sehr hoch). Betroffene Systeme: iPads & iPhones mit aktuellem Betriebssystem. Nutzer sollten daher umgehend auf die Version 10.2.1 updaten.
   → CB-K417/131
5. 24.01.2017: Apple Safari 10.0.3. Ausführen beliebigen Programmcodes mit Remotezugriff möglich. Risikostufe 4 (hoch). Betroffene Systeme: Apple macOS X 10.10.5, 10.11.6, macOS Sierra 10.12.3. Zur Behebung der Schwachstelle stellt Apple soll die Version 10.0.3 von Safari installiert werden.
   → CB-K17/0132