Newsletter

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Informationen für betriebliche Datenschutzbeauftragte in den katholischen Krankenhäusern Norddeutschlands

Nr. 02/2016

TeslaCrypt in mp3-Variante

Heise berichtet von Leserhinweisen, die eine neue Dateivariante des Verschlüsselungstrojaners TeslaCrypt aufzeigen. Der Trojaner erzeugt beim Verschlüsseln neuerdings Dateien mit der Endung .mp3. Es scheint sich dabei nach ersten Erkenntnissen um eine modifizierte Version von TeslaCrypt3 zu handeln, das bislang Dateien mit den Endungen .xxx, .ttt oder .micro erzeugte.

→ http://www.heise.de/newsticker/meldung/Verschluesselungs-Trojaner-mp3-Variante-von-TeslaCrypt-3101992.html

Heise berichtet weiter, dass es zurzeit keine Möglichkeit gibt, die hiermit gekaperten Dateien zu entschlüsseln. Der vor kurzem vorgestellte TeslaDecoder funktioniert nur mit Dateien, die mit TeslaCrypt2 erzeugt worden sind. Es bleibt also nur eine entsprechende Vorsorge durch regelmäßige Sicherungen vorzunehmen Ein Beispiel hierfür findet sich im nächsten Bericht.

Gefahr durch Verschlüsselungstrojaner auch für Krankenhäuser

Heise berichtet von dem Fall, in dem die IT des Lukaskrankenhauses in Neuss von einem Verschlüsselungstrojaner infiziert wurde. So ist ein „unbewusst angeklickter“ Anhang einer E-Mail ursächlich für die Infizierung gewesen. Unmittelbar danach hat der Trojaner begonnen alle erreichbaren Dateien zu verschlüsseln.

Das Krankenhaus ist daher derzeit nur noch eingeschränkt funktionsfähig, da viele Systeme heruntergefahren werden mussten. In der Folge mussten auch einige Operationen verschoben werden. Nach Angaben der Westdeutschen Allgemeinen Zeitung sind in Nordrhein-Westfalen zwei weitere Krankenhäuser von einem Verschlüsselungstrojaner betroffen, die den Vorfall jedoch nicht öffentlich gemacht haben.

Der Schaden soll sich im Falle des Neusser Krankenhauses allerdings in Grenzen halten, da anscheinend ein bestehendes IT-Sicherheitskonzept existiert hat. Nach Angaben des Lukaskrankenhauses soll es ein zeitnahes Backup, das kurz vor der Infizierung erstellt wurde, geben. Zudem seien die Patientendaten vor dem Zugriff der Angreifer sicher, da diese ausschließlich verschlüsselt gespeichert wurden.

Die enorme Bedrohung, insbesondere auch für Krankenhäuser, durch (Verschlüsselungs-)Trojaner und der damit einhergehenden Notwendigkeit wirksamer Sicherheitskonzepte wird nicht zuletzt an dem Beispiel des Neusser Krankenhauses deutlich.

→ http://www.heise.de/newsticker/meldung/Ransomware-Virus-legt-Krankenhaus-lahm-3100418.html

Fahrlässiger Umgang bei der Vernichtung von Patientendaten

In Thüringen wurden im Klinikum Bad Salzungen Patientenakten nicht ordnungsgemäß entsorgt. Betroffen soll eine Außenstelle des medizinischen Versorgungszentrums gewesen sein, in der „unter Missachtung der Vorschriften patientenbezogene Papiere nicht ordnungsgemäß entsorgt wurden“. Die Akten seien nicht bis auf die vorgeschriebene Endgröße zerkleinert wurden.

Der fahrlässige Umgang mit den Patientendaten ist beim Karnevalsumzug in Dermbach ans Licht gekommen. Dort hat eine Anwohnerin beim Straßenfegen Schnipsel entdeckt auf denen der Name Ihrer Schwester zu lesen war. Auf den Papierschnipseln waren personenbezogene Daten wie Namen, Adressen und Telefonnummern – auch von Ärzten – deutlich zu erkennen. Die Schnipsel wurden auf dem Umzug als Konfetti verwendet.

→ http://www.heise.de/newsticker/meldung/Karneval-vs-Datenschutz-Patientenakten-aus-der-Konfetti-Kanone-3099751.html

Der Landesdatenschutzbeauftragte Lutz Hasse hat entsprechende Medienberichte bestätigt und die Einleitung eines Verwaltungs- und Bußgeldverfahrens wegen Verstoßes gegen das Datenschutzrecht angekündigt.

→ https://www.tlfdi.de/tlfdi/presse/aktuell/

Problem bei Sicherheitsupdate von Microsoft Word

Das zuletzt veröffentlichte Microsoft-Update vom 09. Februar 2016 enthält einen Fehler, der sich offensichtlich bei MS Word in der Version von Office 2013 auswirkt. In einigen Fällen wird Word dadurch so stark verlangsamt, dass mit dem Programm nicht mehr gearbeitet werden kann. Dieses hat heise online am 12.02.2016 berichtet. Nach Angaben der Redaktion lässt sich dieser Fehler nur dadurch beheben, dass man das entsprechende Tool (KB3114717) wieder deinstalliert.

→ http://www.heise.de/newsticker/meldung/Microsofts-Februar-Update-fuehrt-zu-Problemen-in-Office-2013-3100987.html