Newsletter

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Informationen für betriebliche Datenschutzbeauftragte
und IT-Verantwortliche in kirchlichen Dienststellen

Nr. 02/2016

Ransomware TeslaCrypt 2.0 durch TeslaDecode zu entschlüsseln

Dieser Newsletter befasst sich mit den immer beliebter werdenden Erpressungen durch Internetkriminelle.

Dabei spielt der Einsatz eines Trojaners unter der Bezeichnung TeslaCrypt eine entscheidende Rolle. Er verschlüsselt die Daten auf dem Server der angegriffenen Dienststelle durch einen symmetrischen AES-Schlüssel. Auf diese Weise verhindert er vollständig die weitere Nutzung der Einrichtungsdaten. Dieser Trojaner war bisher nicht zu knacken. Zwar konnte er durch Virenschutzprogramme erkannt werden, aber auch diese waren nicht in der Lage, die verschlüsselten Dateien wiederherzustellen. Den beeinträchtigten Einrichtungen blieb also nichts anderes übrig, als die Lösegeldforderung zu bezahlen, damit die Hacker die Zwangsverschlüsselung aufhoben und ihnen wieder Zugriff auf das System ermöglichten.

Nunmehr ist ein Weg gefunden worden, die verschlüsselten Daten auch ohne Lösegeldzahlung wiederherzustellen, mit Hilfe des Tools „TeslaDecode“. Das Verfahren, das dabei anzuwenden ist, wird von heise Security beschrieben:

→ TeslaCrypt 2.0 entschlüsselt

→ Verschlüsselungs-Trojaner TeslaCrypt geknackt; Kriminelle rüsten nach

Allerdings gibt es hierzu auch eine schlechte Nachricht: Inzwischen soll schon ein neuer Trojaner unter der Bezeichnung TeslaCrypt 3 existieren, gegen den das vorbezeichnete Verfahren nicht wirksam ist:

Für TeslaCrypt 2 können nur Dateien mit den Endungen .aaa, .abc, .ccc, .ecc, .exx, .vvv, .xyz, und .zzz wiederhergestellt werden.

Bei TeslaCrypt 3 werden Dateien mit den Endungen .xxx, .ttt, .micro verwendet, die sich derzeit nicht retten lassen.

Empfehlung des BSI: Opfer von Ransomware sollen nicht zahlen, sondern Anzeige erstatten

Auf dem Safer Internet Day, der am 9. Februar stattgefunden hat, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Betroffenen von Verschlüsselungs-Trojanern geraten, die Lösegeldforderung nicht zu bezahlen, sondern den Bildschirm mit der Erpressungsnachricht zu fotografieren und Strafanzeige zu erstatten. Es sei nicht sicher, dass die Daten nach Zahlung des Lösegeldes wieder freigegeben werden.

→ Safer Internet Day: BSI informiert über Risiken durch Ransomware

Backups sind nach Auffassung des BSI die einzige wirksame Möglichkeit, die Daten wiederherzustellen. Darüber hinaus müssen alle Nutzer des Systems darüber aufgeklärt werden, dass diese Trojaner meist über Dateianhänge in E-Mails übertragen werden und daher besondere Vorsicht beim Öffnen von Anhängen oder Links geboten ist.

Akuter Fall: Online-Apotheken werden von Erpressern ins Visier genommen

Eine weitere Möglichkeit, sich durch Online-Erpressung Geld zu verschaffen, ist die Drohung mit einem DDoS-Angriff, bei dem die Hosts durch eine übergroße Zahl von Datenpaketen traktiert werden. Die angegriffenen Server stellen infolge der Überlastung daraufhin den Dienst ein. Eine Erpresserbande mit dem Namen „Gladius“ hat

mit dieser Methode Online-Apotheken angegriffen und deren Server für jeweils eine Stunde lahmgelegt. Anschließend wurde die Zahlung von 1.500 € verlangt, damit der DDoS-Angriff nicht noch weiter ausgedehnt werde und dann einen Totalausfall des Shops zur Folge hätte.

→ Hacker legen Apotheken-Shops lahm (Deutsche Apotheker Zeitung, 08.02.2016)
→ Online-Erpresser nehmen Versandapotheken ins Visier (heise Security, 10.02.2016)