Der IT-Sicherheitsbeauftragte (CISO)

Dr. Christian Rank

UNIVERSITÄT PASSAU

Universität Passau · Rechenzentrum · D-94030 Passau

An die Angehörigen
der Universität Passau

Telefon	0851 509-1838 0851 509-1801 (Sekretariat)
Telefax	0851 509-1802
e-mail	christian.rank@uni-passau.de
Zeichen	20151211_teslacrypt
Datum	11.12.2015

Warnung vor der TeslaCrypt-Schadsoftware und Prinzipien zum Umgang mit E-Mails

Sehr geehrte Damen, sehr geehrte Herren,

zur Zeit grassiert (wieder) eine neue Welle von Schadsoftware, die per E-Mail verteilt wird.

Die aktuelle Schadsoftware nennt sich "TeslaCrypt" und gehört zu den sog. Erpressungstrojanern. Wenn diese Schadsoftware auf einem PC aktiviert ist, verschlüsselt sie alle Dateien auf den lokalen und den Netzlaufwerken. Eine Entschlüsselung ist nur nach Zahlung eines Lösegeldes möglich.

Aus diesem Anlass möchte ich auf folgende grundlegende **Prinzipien im Umgang mit E-Mails** hinweisen:

1. Der **Absender** einer E-Mail kann **beliebig gefälscht** werden. Lassen Sie sich nicht dazu verleiten, eine E-Mail für authentisch zu halten, nur weil Sie den (vermeintlichen) Absender kennen. Wenn Sie sich nicht sicher sind, fragen Sie beim Absender nach. **Bitte öffnen Sie im Zweifelsfall weder Anhänge noch klicken Sie auf Links!**
2. **Anhänge** (sog. Attachments) können **Schadcode** enthalten. Sie sollten Änhänge nur dann öffnen, wenn alle der folgenden Bedingungen erfüllt sind:
    - Die E-Mail stammt wirklich von einem Ihnen **bekannten Absender** und Sie **erwarten** von diesem Absender einen entsprechenden Anhang,
    - Die Mail und der Anhang entspricht in Form und Struktur den bisherigen **Kommunikationsgewohnheiten** mit Ihrem E-Mail-Partner (verdächtig ist z. B. wenn Sie eine E-Mail auf Englisch erhalten, wenn Sie bisher auf Deutsch kommuniziert haben),

- Der Anhang (oder der Inhalt eines Dateiarchivs im Anhang) enthält **keine** Dateien mit **kritischen Dateitypen** (u. a. BAT, COM, JS, EXE, PIF, SCR, VBS).

3. **Links** in E-Mails können auf Webseiten führen, die **Schadcode** enthalten. Darüber hinaus kann das Ziel eines Links verdeckt sein, so dass Sie dem Link nicht ansehen können, zu welcher Webseite er schließlich führt. Sie sollten **keinesfalls** auf Links klicken, die Sie **unerwartet** erhalten!
4. Im übrigen verweise ich auf die Empfehlungen des BSI zum "gesunden Menschenverstand".[1]

Weitere Hinweise zur TeslaCrypt-Schadsoftware finden Sie beispielsweise auf den Webseiten der schweizerischen Melde- und Analysestelle Informationssicherung.[2]

Wenn Sie einen Befall Ihres Systems mit TeslaCrypt oder auch anderer Schadsoftware vermuten, wenden Sie sich bitte unverzüglich an den Support des ZIM.[3]

gez. Dr. Christian Rank, CISO Uni Passau

1 https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Menschenverstand/menschenverstand_node.html
2 https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/teslacrypt.html
3 http://www.zim.uni-passau.de/kontakt/