Vorbeugung gegen Ransomware

Vielleicht habt ihrs aua den Medien vernommen: Eine neue grosse Gefahr bezüglich Computer und Datensicherheit ist im Aufwind, sogenannte Ransomware (z.B. TeslaCrypt, Locky). Einmal infiziert, verschlüsselt solche Ransomware alle Daten auf dem betroffenen Rechner/Server und allenfalls auf anderen Geräten/Rechnern im selben Netzwerk, die dadurch unbrauchbar werden. Oft sind auch alle Backup- (=Sicherungs-) Dateien davon betroffen. Es wird Lösegeld erpresst mit dem Versprechen, dass nach entsprechender Bezahlung die Daten wieder freigegeben werden. Da dies aber überhaupt nicht sicher ist, wird generell davon abgeraten, den Erpressern Geld zu überweisen. D.h. alle Daten bleiben im schlimmsten Fall für immer verloren.

Technische Vorkehrungen zur Abwehr solcher Ransomware-Angriffe habe ich soweit möglich in Zusammenarbeit mit Fachleuten getroffen. Das gefährlichste Einfallstor aber ist und bleibt das Verhalten der Computernutzer. Und da ihr alle auf dem gleichen Server-/Mailserver arbeitet, ist ein äusserst vorsichtiges Verhalten von euch allen gefordert.

Vorsichtsmassnahmen (gemäss Melani – Schweiz. Melde- und Analysestelle Informationssicherung):

- **besonders vorsichtiger Umgang mit E-Mails: Bei unbekannten Absendern oder unerwarteten Nachrichten keine Textanweisungen befolgen, keine Anhänge öffnen (ganz wichtig) und nicht auf Links klicken ohne diese vorher zu überprüfen (mit der Maus darüberfahren / von Hand im Browser eintippen)**
- besondere Vorsicht beim Öffnen gefährlicher Dateitypen (Office-Dateien mit Makros = m am Schluss, exe, com, bat, pif, js, scr, vbs, ps1 u.a.), solche können auch in gepackten Dateien (zip) vorkommen
- keine dubiosen, anstössigen oder widerrechtlichen Internetseiten aufrufen
- aus dem Internet heruntergeladene Dateien vorgängig auf Viren checken*
- Ebenfalls besondere Vorsicht beim Einstecken von fremden Datenträgern (z.B. USB-Sticks), im Zweifelsfall gar nicht verwenden oder zumindest vor deren Verwendung auf Viren checken*
- bei Software-Installationen Dateien vorgängig auf Viren checken*
- sorgfältiger Umgang mit Kennwörtern (auch mit denjenigen der Schüler-Konten), bei Missbrauchsverdacht sofort Kennwörter ändern
- jeglichen Verdachtsfall sofort dem Informatikverantwortlichen melden

* Virencheck: Rechtsklick auf die zu kontrollierenden Dateien und „Scannen mit MS Forefront Endpoint Protection...“ wählen oder Online-Virencheck, z.B. über http://www.virustest.de/deu/online-check.asp.