**Verschlüsselungsviren (Ransomware)**

Immer häufiger kommt es in letzter Zeit in der Computerwelt zu einem Bedrohungsszenario durch **Verschlüsselungsviren** (= Ransomware, Erpressungstrojaner, Kryptotrojaner).

Wie viele andere Viren auch, kommen diese Verschlüsselungsviren als **Dateianhang** in einer E-Mail.

Die E-Mails erscheinen oft als harmlos, sobald jedoch der Dateianhang der E-Mail geöffnet wird, fängt der Virus an, alle lokalen Dateien, sowie angebundene Netzlaufwerke auf denen der Benutzer eine Änderungsberechtigung besitzt, zu verschlüsseln.

Dabei sind Dateien auf dem Rechner, die man selbst erstellt hat, bzw. mit denen man arbeitet, wie z.B. Dokumente, Bilder, Präsentationen, Tabellenkalkulationen, Audiodateien, etc. besonders betroffen.

Der **Virus** löscht also nicht das System oder die Dateien, er **verschlüsselt alle gefundenen Dokumente** und macht diese damit unzugänglich für den Benutzer.

Nach dem die Verschlüsselung im Hintergrund abgelaufen ist, erscheint eine Meldung, dass der Rechner von dem Virus befallen wurde und der Benutzer erst nach **Zahlung einer gewissen Summe** den Schlüssel, zum Entschlüsseln der betroffenen Dateien, erhalten wird.

**Prävention:**

* Keine fragwürdigen E-Mail-Anhänge öffnen.
* Sicherungen/Backups aller wichtigen Daten auf externen Laufwerken.

**Reaktion im Schadensfall:**

* Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt im Schadensfall, nicht auf die Forderungen einzugehen.
* Existieren keine Backups ist eine Entschlüsselung jedoch nur mit dem Schlüssel möglich.
* Die Zahlung des geforderten Lösegelds garantiert natürlich nicht die Herausgabe des Schlüssels zur Entschlüsselung der Daten.

**Verwendete Quellen und weitere Informationen:**

* <https://de.wikipedia.org/wiki/Ransomware>, Stand: 6.3. 2016
* <http://www.heise.de/newsticker/meldung/Ransomware-Virus-legt-Krankenhaus-lahm-3100418.html>, Stand: 6.3.2016
* <http://www.spiegel.de/netzwelt/web/ransomware-teslacrypt-stadtverwaltung-dettelbach-zahlt-loesegeld-a-1080528.html>, Stand: 6.3.2016