Informationsstand: Mai 2016

GLARONIA INFORMATIK AG

Information zu Verschlüsselungs-Viren wie Cryptlocker & Locky etc.

Das Vorgehen der kriminellen Schadsoftware-Hersteller wird immer dreister und raffinierter. Die heutigen Trojaner sind auf einem sehr hohen Niveau entwickelt und werden von professionell agierenden Organisationen auf perfide Art und Weise an zufällige Empfänger verschickt. Wohlgemerkt in lupenreinem Deutsch.

Hier ein Beispiel (real vorgekommen)
Sie erhalten auf eine aktuelle Stellenausschreibung Ihrer Firma ein persönliches Bewerbungs-Mail. Im Anhang dieses E-Mails befindet sich eine ZIP-Datei, welche die Bewerbungsunterlagen enthalten soll. Wird diese ZIP-Datei durch Anklicken ausgepackt, wird ein Trojaner aktiv und verschlüsselt alle Dateien auf Ihrem PC, dem Server und weiteren Dateiaufbewahrungsorten wie externe Disk und NAS, also überall dort, wo Sie aufgrund Ihrer Berechtigungen Zugriff haben.

Aktuell und mit dem gleichen Resultat werden solche ZIP-Dateien auch über einen Downloadlink bei einer Plattform wie Dropbox oder MagentaCLOUD angeboten.

Was kann passieren:
Wenn sich die Schadsoftware auf Ihrem System eingenistet hat, passiert zunächst einmal gar nichts. Die Trojaner sind nämlich so entworfen, dass sie im Hintergrund bleiben, und zwar möglichst lange. Nur so können sie möglichst viele Daten befallen.

Die Schadsoftware verschlüsselt ihre Daten, vornehmlich Office-Dokumente und Bilder, und zwar so, dass sie nicht mehr geöffnet werden können. Sie werden mit einem zufälligen, unknackbaren Schlüssel belegt. Die Dateien weisen danach oftmals die Dateiendung „.locky“ auf. Neben den verschlüsselten Dateien liegen Anleitungen mit dem Namen „HOW_TO_RECOVER“ oder ähnlich.

Sollte sich Ihr Computer also auffällig verhalten, wie Dateien lassen sich nicht mehr öffnen oder ähnliches, so fahren Sie das Gerät unverzüglich herunter und melden sich bitte bei uns. Wichtig ist es, in einem Verdachtsfall umgehend zu reagieren und lieber einmal zu viel als einmal zu wenig anzurufen.

Was kann ich bei einem E-Mail überprüfen, bevor ich ein Anhang oder Link öffne:

1. Kommt das E-Mail von einem bekannten Absender?
2. Erwarte ich ein E-Mail von diesem Absender? Ist das Anliegen plausibel?
3. Vorsicht bei Links! Auch wenn der Link „sicher“ aussieht, kann schon über das blosse Aufrufen von Webseiten Schadcode eingeschleust werden!
4. Keine ausführbaren Dateien wie .exe öffnen, äusserste Vorsicht bei .zip-Dateien!
5. Im Zweifelsfall beim Absender zurückfragen oder die Nachricht löschen

Zur Erhöhung des Schutzes empfehlen wir Ihnen unsere Services:

- Managed Client Security
- IT-Premium Service
- Backup to Glaronia

GLARONIA INFORMATIK AG
8750 GLARUS · ISELIGUET 3 · TELEFON 055 645 46 47 · 8808 PFÄFFIKON SZ · SCHINDELLEGISTRASSE 73 · TELEFON 055 420 20 15 ·
EMAIL@GLARONIA.CH · WWW.GLARONIA.CH