ACHTUNG: NEUER KRYPTO-TROJANER IM UMLAUF!

Veröffentlicht am 22. Februar 2016 von Catharina

In diesen Tagen sind Kriminelle mit einem neuen Krypto-Trojaner (Verschlüsselungstrojaner) im Netz unterwegs. Der Trojaner ist eine neue Ransomware namens Locky und agiert weltweit, indem die Daten auf infizierten Computern verschlüsselt und erst nach Zahlung eines „Lösegelds“ wieder freigegeben werden.

ACHTUNG VOR DEM KRYPTO-TROJANER!

Vorgehensweise
Der neue Verschlüsselungstrojaner verbreitet sich derzeit hauptsächlich via E-Mail. In den meisten Fällen handelt es sich dabei um eine frei erfundene Rechnung, die den neugierigen Empfänger zum Öffnen des Anhanges verleiten soll. Der vermeintliche Inhalt wird dann als Buchstabensalat angezeigt, mit der Aufforderung: „Bitte Makros aktivieren, wenn die Datencodierung falsch ist.“ Dieses Makro lädt dann den eigentlichen Trojaner „ladybi.exe“ herunter, der dann die Dokumente in „hash.locky-Dateien“ verschlüsselt. So schafft es der Trojaner alle Dateien auf Ihrem Computer zu

verschlüsseln und anschließend Lösegeld zur wieder Freischaltung zu fordern.

Die Besonderheit hierbei ist, dass der Trojaner Locky nicht nur auf Ihren Computer eindringt, sondern sich auch über das vorhandene Netzwerk weiter verbreitet und alle daran angebundenen Computern infiziert, der Trojaner kopiert sich selbstständig weiter.

Neues von den Experten
Das Sicherheitsunternehmen Kaspersky berichtete am Freitag, dass sich Locky nicht mehr nur über infizierte E-Mails verbreitet, sondern auch über Webseiten. "Zudem haben wir auch einige legitime Websites entdeckt, auf denen die Locky-Schadsoftware platziert wird. Besucht ein Nutzer - mit entsprechenden Software-Schwachstellen auf seinem Rechner - eine solche Seite, versucht sich Locky automatisch auf diesem Rechner zu installieren".

Vorkehrungen bei Trojanern
Bitte achten Sie in diesen Tagen und im Allgemeinen darauf, dass Sie und auch Ihre Mitarbeiter nicht unbedarft auf Anhänge in E-Mails unbekannter Absender klicken. Auf Ihren Virenscanner allein dürfen Sie sich nicht verlassen, weil Schadsoftware so neu sein kann, dass sie das Schutzprogramm einfach noch nicht erkennt.

Trotzdem sollten Sie natürlich immer darauf achten, dass die Virendefinitionen Ihres Virenscanners auf dem neuesten Stand sind. Wenn Sie Fragen zu dem Thema haben, schreiben Sie uns oder rufen Sie uns an.