

# Locky

Im Moment verbreitet sich der Erpressungstrojaner **Locky** in Deutschland sehr schnell, besonders betroffen sind auch die Niederlande und die USA.

**Die zu erwartenden Schäden bei einer Infektion sind extrem hoch.**

Die Schadsoftware wird über E-Mail verteilt und kommt überwiegend als Office-Dokument, meist als **Rechnung** getarnt. Es gibt leider auch andere Verbreitungswege.

**Wie soll ich mich verhalten?**

Um Schäden vorzubeugen beachten Sie bitte die folgenden Verhaltensregeln:

- **Öffnen Sie keine angehängten Dokumente in E-Mails.**  
Wenn Sie Dokumente von außerhalb erwarten, sprechen Sie mit den Absendern ein Alternativ-Format ab.  
Wenn das nicht möglich ist, lassen Sie das Dokument vor dem Öffnen von einem Administrator untersuchen.
- **Verzichten Sie in der aktuellen Gefahrenlage auch auf das interne Versenden von Office-Dokumenten.**
- **Wenn Sie beim Öffnen von fremden Office-Dokumenten eine Sicherheitswarnung *Dieses Dokument enthält Makros* erhalten, lassen Sie die Makrofunktion bitte deaktiviert.**

**Und wenn doch schon etwas passiert ist?**

Sollten Sie das Gefühl haben, dass etwas nicht stimmt, sollten Sie den Verdacht auf eine Infektion haben, geraten Sie nicht in Panik.

- **Benachrichtigen Sie sofort einen Administrator. Sie/Er weiß, was zu tun ist und hilft Ihnen.**
- **Wenn Sie niemanden erreichen können, schalten Sie Ihren Arbeitsplatz bitte sofort aus. Nicht Herunterfahren, Not-Aus. Im Zweifelsfall den Stecker im laufenden Betrieb aus der Steckdose ziehen.**

Informationen zur Bedrohung finden Sie z.B. unter <http://www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html>

# Dokumente in Emails

Hier sind noch einmal allgemeine Vorsichtsmaßnahmen zusammengefasst.

- E-Mails von Unbekannten sind mit besonderer Vorsicht zu behandeln. Anhänge an diese E-Mails bitte sollten nur nach eingehender Prüfung geöffnet werden.
- Bei E-Mails von bekannten Absendern sollten Sie vorher prüfen, ob Sie eine solche E-Mail erwarten. Der E-Mail-Absender könnte auch gefälscht sein, was für Sie ohne spezielle Kenntnisse nicht leicht zu erkennen ist.
- Generell sollten Sie Dokumente und Anhänge nicht direkt aus dem E-Mail-Programm (Outlook) öffnen, sondern die Anhänge zuerst im Dateisystem abspeichern. Vergewissern Sie sich dann noch einmal, dass Sie dieses Dokument benötigen.
- Gute gelebte Praxis ist es auch, zum Austausch mit externen Partnern andere Dateiformate zu verwenden. Das können PDF-Dokumente sein, Office-Dokumente OHNE Makro-Einbettung oder auch RTF als Textaustauschformat.