Wie Sie bereits der Presse entnommen haben kursiert eine gefährliche Schadsoftware im Internet, die bereits viele Computer in Firmen, Krankenhäusern und Behörden infiziert hat.

Die Software ist der Krypto-Trojaner „Locky", der verschiedene Wege nutzt, um Computer zu befallen.

Er gelangt meistens über E-Mail-Anhänge auf die Computer seiner Opfer, getarnt als vermeintliche Rechnung mit einem Word- oder Excel-Dokument im Anhang. Öffnet man das angehängte Dokument, wird die Schadsoftware aus dem Internet nachgeladen und der darin befindliche Trojaner installiert sich automatisch über die Office-Makros (Makros dienen der Automatisierung wiederkehrender Aufgaben u.a. in Office Anwendungen) auf dem Computer und beginnt mit der Verschlüsselung von Festplatten, Netzlaufwerken oder Cloud-Speichern.

Da die Nutzung der verschlüsselten Daten anschließend nicht mehr möglich ist, kommt dies einem Totalverlust der Daten gleich. Um wieder Zugriff auf seine Daten zu erhalten, verlangen die Täter die Zahlung eines Geldbetrages, der mit der digitalen Währung Bitcoin gezahlt werden soll. Aber die Zahlung des erpressten Lösegeldes ist nicht unbedingt von Erfolg gekrönt und man macht sich zum Ziel weiterer Angriffe.

Schutzmaßnahmen gegen die Infektion:
1. regelmäßige Daten- und System-Backups auf ein externes Speichermedium, welches nicht dauerhaft am System angeschlossen ist, da auch Daten auf externen Laufwerken, Netzlaufwerken und Cloud-Speichern verschlüsselt werden
2. bei Datensicherung in der Cloud: Schutzmaßnahmen beim Anbieter abfragen
3. Durchführung von Rücksicherungen als Test, ob sich Daten wiederherstellen lassen
4. standardmäßiges Ausführung von Makros in Microsoft Office verhindern (deaktivieren)
5. Sensibilisierung und Schulung der Mitarbeiter, damit diese das Problem kennen und verdächtigen Dateianhänge von E-Mails oder Links öffnen
6. Software wie Betriebssystem, Browser und Plugins (Java, Flash, Adobe Reader etc.) auf dem aktuellen Stand halten
7. Einsatz von Sandbox-Lösungen erwägen.