Krypto Trojaner Locky – was können wir tun?

Es gibt zur Zeit keinen wirksamen Schutz gegen „Locky“.
Die Computernutzer haben selbst Vorsorge zu treffen damit eine Infektion nicht zu einem (Daten-)Desaster wird.
Die meisten der hier aufgeführten Empfehlungen sollten für JEDEN selbstverständlich sein – hier kann JEDER noch einmal abklopfen wie viel davon umgesetzt ist ODER wer hier aktuellen Nachholbedarf hat.
Wer von einer Verschlüsselungs-Schadsoftware heimgesucht wird und keine Datensicherung hat ZAHLT

- oder hat Zeit abzuwarten bis es evtl. eine kostenfreie Bereinigung gibt
- oder die Daten hatten sowieso keinen tatsächlichen Wert in welcher Beziehung auch immer.

Unsere Tipps zur Vorgehensweise (ohne Anspruch der einzig gangbare Weg zu sein):

- ➔ **Regelmäßige Backups Ihrer wichtigen Daten anlegen.**
- ➔ **Das System** (insbesondere Betriebssystem, Office, Internetbrowser und PlugIns) **auf dem aktuellen und somit denkbar sichersten Stand halten.**
- ➔ **Sicherstellen das Ihr System von einer Internetsecurity geschützt wird die immer mit aktuellen Signaturen versorgt wird.**
- ➔ **Konfigurieren Sie Microsoft Office so, dass Makro-Code entweder überhaupt nicht oder nur nach einer Rückfrage ausgeführt wird.**
- ➔ **Makro-Code nur bei Dokumenten aus vertrauenswürdigen Quellen zulassen und auch dann nur wenn es unbedingt notwendig ist.**
- ➔ **Dateianhänge von Emails, deren Vertrauenswürdigkeit auch nur im entferntesten zu bezweifeln wäre nicht öffnen.**
- ➔ **Keine ausführbaren Dateien starten an deren Vertrauenswürdigkeit Sie zweifeln.**

Das Sicherungsmedium darf nicht dauerhaft an dem PC, Notebook, etc. angeschlossen sein da Kryptotrojaner alle erreichbaren Datenspeicher verschlüsseln.
Der Kryptotrojaner löscht routinemäßig alle von Windows angelegten Schattenkopien (aus denen im Normalfall eine Wiederherstellung von defekten Dateien bestenfalls möglich wäre).

Wen es doch erwischen sollte, den Datenträger mit den verschlüsselten Daten aufheben und weglegen – nicht für die Neuinstallation benutzen. Günstigstenfalls gibt es nach einiger Zeit ein Bereinigungstool. Dann könnten Daten wiederhergestellt werden ohne den Erpressungsbetrag zu bezahlen.

Nun prüfen Sie IHREN STATUS QUO und handeln SIE!

Handels- und Dienstleistungszentrum Quernes
56237 Nauort, Rheinstraße 12 * Geschäftsführer: Dietmar Quernes
Tel. +49 (0)2601-912143 * Fax +49(0)2601-912144 * email: info@hdlzq.de
Sparkasse Koblenz:BLZ 57050120 Kto 0000228627 IBAN: DE75570501200000228627 BIC: MALADE51KOB
USt-ID: DE155675276 *Gerichtsstand: Montabaur