BEST Practice

Ihr Service für Information und Technologie

SCHUTZ
VOR RANSOMWARE „LOCKY“ UND ANDEREN TROJANERN

Um sicherzustellen, dass bei Ihnen die Risiken in Bezug auf den aktuell grassierenden Kryptotrojaner „Locky“ weitestgehend minimiert sind, empfehlen wir, dass Sie eine kurze Bewertung Ihrer Ist-Situation anhand unserer Checkliste vornehmen.
Sind folgende Maßnahmen bei Ihnen umgesetzt und Bestandteil Ihres Sicherheitskonzeptes?

1 Alle IT-Systeme, die mit dem Netzwerk verbunden sind oder externe Daten verarbeiten, werden ohne Ausnahme regelmäßig mit Patches für das Betriebssystem und Updates für die installierte Anwendungssoftware versorgt.

2 Die Updates der Systeme erfolgen zeitnah binnen weniger Stunden nach Verfügbarkeit und werden, wo immer möglich, automatisiert durchgeführt.

3 Alle Systeme sind mit einem aktuellen und wirksam konfigurierten Virenscanner ausgestattet.

4 Die Virenfilter sind so konfiguriert, dass alle Daten beim Öffnen oder Schreiben sowohl im Arbeitsspeicher als auch auf den permanenten Speicherbereichen in Echtzeit überprüft werden.

5 Alle Bestandsdaten, z. B. auf den Fileservern, werden in regelmäßigen Abständen neu überprüft, um die Zeitlücke zwischen dem ersten Auftreten eines Virus bis zum Bereitstellen von wirksamen Signaturen durch die Antivirus-Hersteller zu überbrücken.

6 Von externen Quellen werden nur dort aktive Inhalte angenommen, wo es betriebliche Erfordernisse notwendig machen. Das betrifft insbesondere Formate, die Makrosprachen enthalten wie die Dateiformate der gängigen Microsoft Office Produkte.

7 Für den Fall einer konkreten Bedrohung sind wir in der Lage, an zentraler Stelle, wie z. B. der Firewall, bestimmte Dateiformate gezielt zu blockieren.

8 Im Falle eines Befalls unserer Systeme, der zu einer Schädigung der Daten geführt hat, sind wir darauf vorbereitet, betroffene Rechner schnell zu identifizieren und vom Netz zu trennen.

9 Bei uns stehen aktuelle Sicherungen bereit, um den Originalzustand der Daten in kurzer Zeit wiederherstellen zu können.

10 Dank Einsatz von Snapshots können wir den Datenbestand auf unseren Fileservern nach Beseitigung der betroffenen Rechner binnen weniger Minuten wiederherstellen.

11 Alle IT-Anwender werden bei uns in regelmäßigen Abständen darüber informiert, mit welchem Verhalten sie aktiv zur Erhöhung der Betriebssicherheit beitragen.

12 Allen IT-Anwendern sind die besonderen Gefährdungssituationen in Bezug auf Locky bereits bekannt. Sie wurden darüber informiert und sensibilisiert, unerwartete E-Mail-Korrespondenz von unbekannten Absendern und insbesondere die Datei-Anhänge dieser E-Mails nicht zu öffnen.

13 Für Zweifelsfälle gibt es bei uns einen benannten internen Ansprechpartner, z. B. den internen IT Service Desk, den man als IT-Anwender kontaktieren und um Rat fragen kann.

Sollten diese Maßnahmen bereits zu Ihrem betrieblichen Alltag gehören, ist ein Befall zwar nicht zu 100 % auszuschließen, aber Sie bzw. Ihr Unternehmen sind gut vorbereitet. Wenn dies nicht der Fall sein sollte, empfehlen wir ein Gespräch mit einem unserer Sicherheitsexperten. **Sicher ist sicher!**

Grünwalder Weg 28 b 82041 Oberhaching Telefon: +49 89 6389848-0 Telefax: +49 89 6389848-9 info@is4it.de www.is4it.de