Locky – Einer Ihrer größten Feide

Ein Virus, der seinem Namen gerecht wird. Locky hat im Februar zeitweise 5000 PC/Stunde in Deutschland verschlüsselt. Locky ist seit dem 21.6.2016 mit einer noch bösartigeren Variante im Netz. Er kann ohne ihr Zutun aktiv werden, auch Netzlaufwerke und virtuelle PCs/Server werden verschlüsselt. Locky kann verzögert wirken, also zu einem bestimmten Datum ihr gesamtes Netz zerstören.

Sicherheitsexperten bewerten Netzwerke, die Medieneingänge nicht mindestens abscannen oder besser ein zweites Netz für Internet und Kommunikation (E-Mail) betreiben als fahrlässig betrieben. Im schlimmsten Fall könnte das bedeuten, ein Kunde oder Lieferant der durch den vielleicht tagelangen Ausfall Ihres Unternehmens beeinträchtig wird kann Sie auf Schadensersatz verklagen. Dabei könnte ggf. die Haftungsbeschränkung einer Gesellschaft fallen uns Sie wären in der privatschuldnerischen Haftung. Auch die Finanzbehörden könnten so argumentieren.

Wie kann man sich schützen?

Locky nutzt geschickt Schwachstellen aus und wird laufend verbessert. Virenscanner sind kein sicherer Schutz mehr vor dieser Schadsoftware. Ein 100%iger Schutz ist niemals gegeben. In erster Linie hilft eine langfristige und vom Netzwerk getrennte Datensicherung.

GENU IT Systemhaus
Ihr Partner für mehr Sicherheit in Unternehmensnetzen empfiehlt Ihnen zum verbesserten Schutz vor Locky und anderer Schadsoftware die folgenden Maßnahmen

1.regelmäßige Datensicherungen über einen längeren Zeitraum
(Managed Online Backup - MOB)

2.regelmäßige und zeitnahe Aktualisierung Ihrer Systeme
(Remote Managed Servcies - RMS)

3.Schutzsoftware (Antivirus)
(Virenschutzsoftware oder RMS mit AV)

4.sichere Clouddienste nutzen
(AMES Mailscan, Cloud Windows AD Kopie, Cloud Firewall + Backup, Webprotection)

5.Makros deaktivieren
(deaktivieren Sie selbst die Office-Funktion –siehe unten oder lassen Sie es prüfen)

6.Mitarbeiter sensibilisieren
(E-Mails von unbekannten Absendern oder mit ungewöhnlichen Anlagen
oder Schreibfehlern und fremdsprachigen Anlagen generell nicht öffnen)

Etwas Ausführlicher zu den Top-Punkten:

-regelmäßige Backups über einen längeren Zeitraum

Mit Online-Backup bieten wir Ihnen die Möglichkeit, Ihre Datensicherung verschlüsselt im Unternehmen und gleichzeitig im Rechenzentrum abzulegen.

Über den Zeitraum von einem Monat und bei weiterer Archivierung darüber hinaus können Sie so Ihre Daten wieder zurück holen, falls Sie von einem Verschlüsselungstrojaner angegriffen wurden.

-regelmäßige und zeitnahe Aktualisierung Ihrer Systeme

Viele Schadprogramme nutzen sog. Exploits, bekannt gewordenen Schwachstellen in Systemen und Programmen. Inzwischen sprechen wir vom Zero Day Exploit. Am Tag an dem die Schwachstelle irgendwo erkannt wurde geht sie bereits um die Welt.

GENU IT Systemhaus bietet Ihnen einen zusätzlichen Schutz vor dieser Bedrohung durch die Remote Managed Services (RMS). RMS aktualisiert Ihre Rechner automatisch und überwacht permanent Ihre Systeme (24 Stunden / 7 Tage in der Woche) RMS erspart Ihnen die kostenintensive regelmäßige Wartung durch Ihren IT-Administrator. Wartung ist nur noch bei Bedarf nötig. RMS sendet eine Alarmmeldung, sofern ein Eingriff erforderlich wird und liefert die nötigen Informationen dazu. So wird auch die zeitaufwendige Fehlersuche oft verkürzt. Zudem sorgt RMS für weniger Ausfallzeiten, da klassische IT-Probleme wie Festplattenfehler, Controlerfehler, voll gelaufene Datenspeicher, unerlaubte Login-Versuche usw. sofort von RMS dokumentiert und gemeldet werden.

RMS aktualisiert nicht nur Betriebssysteme, sondern sorgt auch dafür, das viele Standard-Anwendungen immer auf dem sichersten Stand sind. Nur so können Sie einem Zero-Day Exploit erfolgreich begegnen.

-zuverlässige Schutzsoftware gegen Schadprogramme

Im Normalfall ein Virenscaner, der regelmäßig aktualisiert und ausgeführt wird. Freeware ohne Echtzeitscan im Unternehmen zu nutzen ist als fahrlässige Handlung zu sehen. Zusätzlich zu einem lokalen Schutz im Netzwerk ist weitere Sicherheitssoftware zu empfehlen. Zum Beispiel ein Spam- und Virenfilter bei Ihrem Internetprovider oder auf Ihrem Exchange- oder E-Mailserver. Zusätzliche Lösungen wie z.Bsp. ein Cloud-Virenfilter sind ggf. ratsam (z.Bsp. bei Auftragsdatenverarbeitung oder in Sicherheitszonen).

-Auslagerung von Diensten

Exchange-Server können heute leicht im Rechenzentrum betrieben werden. Dort befaßen sich täglich erfahrene Experten mit der Wartung. Zu dem werden Ihre Kosten und der Verbrauch von Umweltresourcen reduziert. AD Server (Active Directory Server) dienen der Rechtekontrolle und anderer führender Funktionen und können mittels Konnektor einfach ins Rechenzentrum repliziert werden. So können Sie auch ein einem Serverausfall schnell und flexibel reagieren.

-Makrofunktionen von Microsofts Office-Produkten sollten in den Einstellungen zumindest so konfiguriert werden, daß Makros nur auf Nachfrage ausgeführt werden. Keinesfalls automatisch. Dieses Einfallstor wird gerne von Viren benutzt.

Infos dazu finden sie bei google unter „Office Makros deaktivieren“ oder
unter diesem Link

Zuletzt spielt der Mensch eine bedeutende Rolle. Sensibilisieren Sie Ihre Mitarbeiter. Bei dem geringsten Verdacht sollten Sie auf die Öffnung von E-Mails oder E-Mailanhängen verzichten. Für den Besuch von Internetseiten sollten spezielle Webfilter eingerichtet sein. Im Zweifel kontaktieren Sie besser einen Administrator, bevor Sie das Unternehmensnetzwerk lahm legen. Locky und Kollegen können Sie ebenso im Internet wie per E-Mail finden. Statistisch ist jede 5. Internetseite im Netz ein Risikofaktor.

Verbieten Sie die Verwendung von unauthorisierten Datenträgern wie USB-Sticks, CDs, Festplatten, SD-Karten usw. Verbieten Sie die Verbindung und das Aufladen von Smartphones via Kabelverbindung zum PC. Gewähren Sie Besuchern und Mitarbeitern keinen Zugang zu Ihrem Netzwerk. Wenn nötig, verwenden Sie einen Gastzugang in einem getrennten Netz.