LOCKY – der aktuelle Verschlüsselungs-Trojaner

Die Schadsoftware „LOCKY“ verschlüsselt alle Ihre Dateien und gibt sie erst gegen hohes Lösegeld wieder frei. Doch wie schütze ich mich und mein Unternehmen?

Sie sind das Zielobjekt

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor einer Welle neuartiger Schadsoftware. Betroffen sind nicht nur Privatpersonen, sondern auch Unternehmen und Behörden. An der Spitze steht derzeit der Verschlüsselungs-Trojaner „Locky“, eine sogenannte „Ransomware“.

Ziel der kriminellen Hacker ist die Geiselnahme Ihrer Dateien.

Diese werden verschlüsselt und erst nach Zahlung eines Lösegeldes wieder freigegeben.

Wie erfolgt der Angriff?

Meist werden Ihnen gut aufgemachte, authentisch wirkende Emails mit gefährlichen Anhängen geschickt. Im Unterschied zu früheren Emails mit Schadcode werden keine leicht zu erkennenden zip oder exe-Dateien, sondern Dateien in Office-Formaten wie PowerPoint, Word oder Excel angehängt. Häufig beziehen sich solche Emails auf Rechnungen oder Mahnungen von bekannten Unternehmen, auf einen angeblichen Rechtsverstoß, eine Bewerbung oder einen Gewinn. Auch gefälschte Emails des Bundeskriminalamtes (BKA) kursieren, die den Virus als angebliches BKA-Analyse-Tool mit dem Namen BKA LockyRemovalKit.exe mitführen.

Grundsätzlich gilt: man möchte Sie dazu bringen, den Dateianhang zu öffnen.

Bild: nexusplexus / dreamstime.com

Office-Trojaner „Locky“ verlangt Lösegeld für Ihre Dateien

Daneben gibt es auch Emails, die Sie auf manipulierte Webseiten leiten wollen, indem man Sie dazu verleitet, die enthaltenen Links anzuklicken. Die manipulierte Webseite lädt dann das Schadprogramm auf Ihren PC.

Die Geiselnahme

Beim Anklicken des Email-Anhangs werden alle Dateien verschlüsselt auf die Sie zugreifen können. Das sind sowohl alle Dateien auf Ihrem PC, als auch auf Web- oder Serverlaufwerken auf die Sie Zugriff haben. Darunter sind möglicherweise einige, die für das Unternehmen überlebenswichtig sein können.

Sind die Dateien erst einmal verschlüsselt, gibt es keine Möglichkeit mehr, darauf zuzugreifen.

Die Verschlüsselung ist so gut gemacht, dass es aktuell keine Möglichkeit gibt, diese zu brechen. Vielmehr zeigt ihr Bildschirm eine Mitteilung oder Sie finden bei den verschlüsselten Dateien eine Text-Datei. Darin werden Sie aufgefordert, eine nicht unerhebliche Summe in der anonymen Internetwährung „Bitcoin“ zu zahlen. Nach erfolgter Zahlung wird Ihnen eine Entschlüsselung der Dateien versprochen.

Warum ist Locky so gefährlich?

Locky verbreitet sich sekundenschnell in der Regel als Anhang einer Email. Die Anhänge sind nicht nur hinsichtlich des vermeintlichen Inhalts variantenreich, sondern auch der Dateiformate: neben bekannten, vermeintlich harmlosen doc, docx, xls, xlsx, ppt, pptx, pdf und den bekanntermaßen gefährlichen exe, zip, rar gibt es auch bat, cmd, js, vbs, wsf, com, scr oder pif.

Öffnen Sie Email-Anhänge mit äußerster Vorsicht!

Der Schadcode wird als sogenannter „Payload“ erst nach Infektion des PCs heruntergeladen und umgeht so die meisten Virenschutz-Programme. Der Schadcode kann sich so beliebig verändern und weiter-

entwickeln und wird von Virenscannern trotz regelmäßiger Updates erst nach Tagen entdeckt oder gar nicht lokalisiert.

Schutz vor Locky?

Der einzig wirksame Schutz ist, Locky gar nicht erst in Aktion treten zu lassen.

D.h. grundsätzlich keine Email-Anhänge zweifelhafter Herkunft öffnen oder auf Links zu klicken, die Sie nicht auch durch Eingabe einer kurzen Internet-Adresse im Browser leicht öffnen könnten. Beachten Sie, dass die Adresse im Text nicht identisch sein muss mit der tatsächlich verlinkten Seite.

Misstrauen Sie Links, die nur ähnlich klingen wie bekannte Seiten oder mit vermeintlichen Rechtschreibfehlern.

Lassen Sie sich durch Mail-Inhalte nicht einschüchtern. Fragen Sie im Zweifel telefonisch nach oder lassen Sie es auf eine schriftliche Mahnung ankommen. Leiten Sie keine verdächtige Email im Unternehmen weiter.

Bestätigen Sie keine Makroausführung in Dokumenten, die Ihnen zugesandt wurden. Klicken Sie bei entsprechende Pop-Ups auf „Nein“.

Auch Pop-Ups, die eine Ausführung eines Programms mit Administratorrechten fordern, sollten Sie misstrauisch machen.

Unterstützen Sie Ihre IT-Abteilung bei der Erstellung von Backups, indem Sie Ihre Dateien ausschließlich auf Serverlaufwerken speichern und nicht auf Ihrem lokalen Rechner.

Wenden Sie sich bei Bedenken oder im Schadensfalle sofort an Ihren Vorgesetzten oder Ihren IT-Support!

Jacqueline Bredereck, LL.B.
Informationsjuristin
j.bredereck@daschug.de
http://www.daschug.de

Ralf Becker
Datenschutzberater
ralf.becker@daschug.de
http://www.daschug.de

Tel. 06151-6673440

Bild: Lorenzo Rossi / dreamstime.com

Für Mitarbeiter-Schulungen in “Grundlagen digitaler Selbstverteidigung“ (Präsenz und Online-Trainings) sowie IT-Sicherheits-Checks Ihres Unternehmens kontaktieren Sie uns! info@daschug.de

Weitergehende Tipps, wenn Sie selbst für die Wartung Ihres PCs verantwortlich sind:

1. Updates

Sie sollten sicherstellen, dass das System auf dem aktuellen Stand ist. Dazu gehören nicht nur Updates des Betriebssystems und der Office-Software, sondern auch des Browsers und ggf. von Plug-Ins und von Zusatzprogrammen wie bspw. Java und Flash. Auch die Anti-Virus Software sollte stets aktuell sein.

2. Makro-Schutz in Office

Weiterhin sollten die Makros in Microsoft Office standardmäßig deaktiviert sein, bzw. die Einstellungen sollten so gewählt werden, dass Makros erst nach Bestätigung ausgeführt werden.

3. Backups

Daten sollten – sofern das die Unternehmensrichtlinien erlauben - regelmäßig auf externen Datenträgern gesichert sein, die nicht ständig mit dem PC verbunden sind. Verwahren Sie diese Datenträger grundsätzlich verschlossen am Arbeitsplatz.

4. Zusätzlicher Schutz

Sofern Ihre Unternehmensrichtlinien dies zulassen, können Sie das kostenlos von der Firma „Malwarebytes“ bereitgestellte Programm „Anti-Ransomware“ nutzen, das aber keine Garantie für einen Schutz bietet.

5. Makros & Scripte stoppen

Für unerfahrene Mitarbeiter empfiehlt sich das Deaktivieren von Office-Makros und das Abschalten von Scripten in der Windows-Registry.