Sicherheitsempfehlungen zu E-Mail-Anhängen

- BSI-Paper

Jeder kennt die Situation: Eine E-Mail mit einer angehängten Datei landet im Posteingang.

In einer optimalen Welt kein Problem, anklicken, anschauen, vielleicht ausdrucken, oder wegsortieren. Dummerweise befinden wir uns leider nicht in einer solchen Welt, denn speziell in letzter Zeit werden vermehrt wieder E-Mail's mit Anängen verschickt, deren Inhalt, falls angeklickt, doch ziemliches Chaos anrichten kann. Stichworte wie locky oder **Petya** sind nur die bekannteren jüngsten Exemplare eines Malwaretyps, die als Ransomware bekannt geworden sind.

Sie alle haben gemein, daß sie als Trojaner im Anhang einer regulären E-Mail auf den Rechner des Anwenders gelangen. Automatisch werden diese Plagen normalerweise nicht aktiv. Es liegt am Anwender die sogenannte Payload den aktiven Teil des bösartigen Anhanges zu starten. Das geschieht häufig schon durch simples anklicken. Der Trojaner landet im Word und startet von dort aus dann ein Hintergrundprogramm mittels eines Word-Makros, welches dann seine Schadroutine ablaufen läßt.

Die üblichen Schadroutinen sind eher darauf ausgelegt, Dateien zu löschen oder Botnetzwerk-Komponenten zu installieren, die wiederum als Sprungbrett für weitere Attacken im Internet dienen.

Ransomware ist keine neue Erfindung. Diese tauchten in den letzten Jahren immer wieder einmal auf. Inzwischen haben sie sich aber recht weit entwickelt.

Sie verschlüsseln bei Aktivierung die Daten des Nutzers und verlangen nach Abschluss ein Lösegeld, um auf diese wieder zugreifen zu können. Im Falle von **Locky** geht das sogar über die persönlichen Daten des Nutzers hinaus. Locky verschlüsselt eigentlich alles auf das er Schreibzugriff hat, d.h. lokale Festplatten, angehängte USB-Platten oder USB-Sticks und natürlich auch gerade verbundene Netzlaufwerke. Letzteres sind dann meist auch gemeinsame Netzlaufwerke die von Arbeitsgruppen oder sogar vom ganzen Institut genutzt werden.

Die Auswirkungen sind meist umgehend bemerkbar. Der Zugriff auf wichtige Dokumente und Dateien schlägt fehl. Nichts geht mehr. Was nun, ist die Frage?

Als erstes, keine Panik! Sämtliche Maßnahmen die sicherstellen sollten, das sowas nicht passiert, waren vergebens. Die gute Nachricht? Es kann jetzt kaum noch schlimmer werden ;)

Folgendes ist zu klären:

- Wer betreut den betroffenden Rechner? → Betreuer/Admin umgehend informieren
- Gibt es Backups der lokalen Festplatten? → Betreuer/Admin sollte das im Zweifel wissen

- Sind Netzwerklaufwerke betroffen? → Rechenzentrum muss informiert werden (per E-Mail: support@rz.tu-clausthal.de oder per Telefon: 72-2626)
- Ausfallzeit für die Restauration der Daten einplanen
- Lokale Daten die nicht im Backup waren sind futsch und weg, genauso Daten von lokalen USB-Platten oder USB-Sticks die zum Zeitpunkt der Schadsoftwareaktivierung mit dem Rechner verbunden waren. Abschied nehmen 🙁
- Wenn die Arbeitsumgebung wieder hergestellt wurde, durchatmen.
- In Zukunft besser aufpassen! 😎

Letzteres ist leicht gesagt. Heutzutage sind E-Mails mit angehängter Schadsoftware raffiniert verpackt und häufig auf den ersten Blick nicht einfach zu entlarven. Es gibt natürlich trotzdem ein paar Hinweise auf die der Anwender achten kann um potentielle Schadmail zu erkennen:

- Ist es eine TU-interne E-Mail die signiert oder sogar verschlüsselt ist, ist es mehr als unwahrscheinlich das sie Schadsoftware enthält
- Den Header (Kopf/Absender) genau anschauen, dabei beachten der Absender kann **immer** gefälscht sein.
- Bei einer externen E-Mail grundsätzlich misstrauisch sein.
- Ist ein Link enthalten und wenn ja wohin führt dieser? (Mit der Maus drüber gehen aber **nicht** anklicken)
- Passt der Zielpfad des Links zum angeblichen Absender? (Falls nicht, **niemals anklicken!**)
- Ist ein Dokument angehängt? Falls ja, was für ein Dokument? PDF → Vorsicht, DOCX → sehr viel Vorsicht, EXE → Finger weg!
- Im Zweifelsfall den Absender telefonisch kontaktieren, falls möglich, alternativ den Admin fragen.
- Ein Restrisiko bleibt immer, 100%tige Sicherheit ist Illusion

Präventionsmaßnahmen

Um wichtige Daten nach einem Befall durch einen Krypto-Trojaner wiederherstellen zu können benötigt man Backups (= Sicherungen) der Daten. Die Verschlüsselung der meisten Krypto-Trojanern lässt sich nicht wieder entschlüsseln, so dass die Daten nur dann wieder in einen lesbaren Zustand versetzt werden können, wenn man Backups der Daten besitzt.

Aus diesem Grunde empfiehlt das Rechenzentrum wichtige Daten auf den Netzlaufwerken des Rechenzentrums (z.B. \\nas.tu-clausthal.de\windows-home$) zu speichern. Von den Daten der Netzlaufwerke werden in regelmäßigen Abständen Sicherungen in Form von Snapshots angefertigt, so dass im Ernstfall ggf. eine Sicherung, die vor dem Befall durch den Krypto-Trojaner angefertigt wurde, wiederhergestellt werden kann.

Des Weiteren wird empfohlen sogenannte Offline-Backups anzufertigen. Daten, die existenziell wichtig sind, sollten ggf. zusätzlich z.B. auf einer USB-Festplatte oder einem USB-Stick gesichert werden. Das USB-Speichermedium sollte nicht dauerhaft am Rechner angeschlossen bleiben.

[studierende], [mitarbeitende]

Direkt-Link:
https://doku.tu-clausthal.de/doku.php?id=it-sicherheit:sicherheitsempfehlungen&rev=1586163374

Letzte Aktualisierung: **10:56 06. April 2020**