Sprunghafter Anstieg von Krypto-Trojanern infizierten E-Mails

Anfang diesen Jahres konnte nach Durchführung entsprechender, groß angelegter Analysen festgestellt werden, dass sich die Verbreitung des gefährlichen Krypto-Trojaners Locky massiv gesteigert hat. Davon ausgehend ist mit einer weiteren deutlichen Steigerung der Zahl an infizierten E-Mails in den kommenden Monaten zu rechnen. Im Zeitraum des ersten Quartals 2016 konnte bereits eine Steigerung um das Fünffache beobachtet werden. Das bedeutet in totalen Zahlen, das nahezu jede 5. E-Mail, die in geschäftlich genutzten E-Mail Accounts einging, mit einem Virus infiziert war. Vor dem Hintergrund, dass unternehmerische Dateien be-sonders wertvoll und bei Verlust kaum zu ersetzen sind, wirkt diese Zahl umso bedrohlicher.

Der starke Anstieg verseuchter E-Mails kann vor allem auf sogenannte Krypto-Trojaner, wie auch Locky einer ist, zurückgeführt werden. Noch Anfang des Jahres waren nur etwa drei Prozent aller E-Mails von solchen Viren befallen, zum Quartalsende hingegen ganze 17 Prozent. Begründet werden kann das unter anderem damit, dass der ersten Angriffswelle mit dem Locky-Trojaner zahlreiche weitere Versionen dieses Virus auftraten. Das liegt in der Besonderheit der Krypto-Trojaner begründet, die darin besteht, dass diese Schadprogramme Ihre Programmstruktur häufig und sehr schnell verändern können. Die Folge davon ist, das Virenscanner oft nicht schnell genug auf die veränderten Strukturen reagieren und die vielen, innerhalb kurzer Zeit auftretenden Varianten des Virus erkennen können. So schlüpfen immer mehr infizierte E-Mails trotz Virenscanner ins Postfach. Daher empfiehlt sich momentan eine erhöhte Wachsamkeit aller Nutzer von E-Mail Postfächern in Bezug auf mit Locky oder ähnlicher Ransomware infizierter E-Mails.

Der Schutz gegen diese Art von Software kann erhöht werden, indem man die Ausführung von eingebetteten Makros in Office-Anwendungen deaktiviert. Der Ausführung von Makros sollte generell nur dann zugestimmt werden, wenn die Dokumente, in denen sie eingebettet sind, aus bekannten und vertrauenswürdigen Quellen stammen und die Ausführung zwingend erforderlich ist. Generell gilt weiterhin die bekannte Vorsichtsmaßnahme, dass man ausschließlich E-Mail Anhänge öffnen sollte, deren Quellen als absolut vertrauenswürdig eingestuft werden können. Sollte dennoch eine Infektion vorliegen, empfiehlt es sich regelmäßige Backups für alle sensiblen und wichtigen Daten anzulegen, damit diese nach einem Virus-Befall unkompli-ziert und verlustfrei wiederhergestellt wer-den können. beachtenswert ist dabei, dass Ransomware wie Locky auch externe Datenträger befallen kann, vor allem, wenn diese dauerhaft mit dem infizierten Rechner verbunden sind. Mögliche Anzeichen für

Sprunghafter Anstieg von Krypto-Trojanern infizierten E-Mails

einen Befall können beispielsweise ein träges Ansprech-verhalten des Rechners sowie hohe Fest-plattenaktivitäten ohne entsprechend er-sichtlichen Grund sein. Auch Dateien mit der Endung Jocky auf der Festplatte weisen auf eine Infektion hin.

Bei Verdacht auf einen Befall auf Ihrem Rechner oder wenn Sie intensiveren Schutz für Ihr E-Mail Postfach und Ihren Computer vor Ransomware und anderen Viren wünschen, lassen Sie sich von uns kompetent beraten.

Kontakt:

IT- Systemhaus ROOTTEC
Inh. Michael Knop
Fredersdorfer Chaussee 83-84
15370 Fredersdorf-Vogelsdorf

Telefon +49 33439 177 816
E-Mail: info@roottec.de