INNOVATIVE KOMMUNIKATIONS- UND NETZWERKTECHNIK

Microsoft Partner
Silver Server Platform
Silver Desktop
Silver Midmarket Solution Provider

Sonder-Newsletter

eMail: newsletter@ikn.de

März 2016

Themen in dieser Ausgabe:

- **Krypto-Trojaner „Locky & Co.“**

IKN IT-Service Hannover GmbH

Griesbergstr. 8
31162 Bad Salzdetfurth
Tel.: 05063 / 5775-0
eMail: ikn@ikn.de

Geschäftsführer:
Regina Weber
HRB 203510
Amtsgericht Hannover

Standort Laatzen
Würzburger Str. 15
30880 Laatzen
Tel.: 0511 / 169 33 99-0
eMail: Laatzen@ikn.de

Standort Hameln
Hefehof 8
31785 Hameln
Tel.: 05151 / 58 52 8-00
eMail: Hameln@ikn.de

Wie schütze ich mich vor dem Verschlüsselungs-Trojaner?

Kryptoviren wie Locky sind derzeit eines der zentralen IT-Security-Themen. Weshalb sind sie so gefährlich, wie können sich Unternehmen dagegen schützen und welche Maßnahmen ergreifen Security-Anbieter um ihren Kunden einen optimalen Schutz zu bieten? Wir haben hierzu Daniel Hofmann von Hornetsecurity ein paar Fragen gestellt, um etwas Licht ins Dunkel zu bringen.

Seit kurzem ist der Locky-Virus in aller Munde: Worum handelt es sich eigentlich dabei, und was macht ihn so gefährlich?
Den Locky-Virus, wie er aktuell im Umlauf ist, gibt es in ähnlicher Form bereits seit Anfang Dezember. Dabei handelt es sich um ein Office-Dokument im Anhang von E-Mails, bei dem ein Makro ausgeführt wird, wenn der Empfänger die Datei öffnet. Bei den zunächst im Umlauf befindlichen Makro-Viren handelte es sich um Online-Banking-Trojaner, die Zahlungen auf fremde Konten umleiteten. Bei der aktuellen Virenwelle werden die Inhalte der gesamten Festplatte verschlüsselt, aber auch Netzlaufwerke und sogar Backups.
Die Gefährlichkeit des Virus liegt darin, dass die E-Mail als Träger sehr professionell gemacht ist und es ziemlich schwierig ist, zu erkennen, ob es sich hierbei um eine reguläre E-Mail handelt. Durch den Inhalt der E-Mail wird dem Empfänger zum Beispiel vermittelt, dass er eine Rechnung nicht bezahlt hätte. Öffnet dieser das Dokument, aktiviert sich das Makro sofort und verschlüsselt die Rechnerinhalte. Möchte ein Geschädigter seine Daten wieder entschlüsselt haben, wird er aufgefordert, ein Lösegeld zu bezahlen. Prinzipiell rate ich jedoch davon ab, da nicht sicher ist, ob der Geschädigte den Entschlüsselungscode überhaupt erhält.

Wie konnte es dazu kommen, dass sich dieser Schädling so verbreiten und solche Schäden verursachen konnte?
Das Besondere an dieser Art von Virus ist, dass die Angreifer täglich 2-3 neue Macharten entwickeln. Diese testen die Virenentwickler so lange an den bekannten Virenscannern, bis sie von diesen nicht mehr erkannt werden. Anschließend versenden sie die Viren. Dabei achten die Malware-Spezialisten darauf, den Versand schnell und kompakt durchzuführen, zudem spielt der regionale Aspekt eine große Rolle: Die Virenmails sind auf Zeitzonen und lokale Sprachen abgestimmt, zudem werden die E-Mails inhaltlich vermeintlich von einem Absenderunternehmen gesendet, das der Empfänger kennt. Versendet werden diese Mails meist tagsüber zwischen Montag und Donnerstag.
Wenn man sich die aktuell kursierenden Makro-Viren betrachtet, lässt sich feststellen, dass hier eine Gruppe am Werk ist, die den gesamten Zyklus von der Entwicklung über den Versand bis hin zur Zahlungsabwicklung äußerst professionell geplant hat. Sie bietet Zahlungswilligen sogar einen Live-Chat an!

Worauf sollten Anwender und Unternehmen generell achten, um sich so gut wie möglich vor Malware wie Locky und Konsorten zu schützen?
Da gibt es mehrere Maßnahmen, die regelmäßig vorgenommen werden sollten, um sich vor Angriffen zu schützen. Zunächst einmal sollte jeder Benutzer und jedes Unternehmen stets die aktuellsten Software-Updates durchführen. Zudem ist es sinnvoll, ein regelmäßiges Backup vorzunehmen, entweder auf ein externes Speichermedium oder auf einen Cloud-Speicherdienst, der eine Versionierung anbietet, wodurch Vorgängervarianten einer Datei wiederhergestellt werden können. Die Haupt-Einfallstore für Malware – E-Mail und das Internet – müssen mit einem seriösen und effizienten Spamfilter- und Webfilter-Service geschützt werden. Zu guter Letzt jedoch trägt auch der Anwender selbst eine Verantwortung, indem er jede E-Mail kritisch prüfen sollte, ob etwa der Absender stimmt und was für Dateianhänge sich an der E-Mail befinden. Zur Not sollte eine E-Mail immer gelöscht werden.

Kann Hornetsecurity Locky erkennen und herausfiltern und wenn ja, wie?
Anfang Dezember, als die ersten Makro-Virus-Angriffe im Umlauf kamen, haben wir sofort neue Filter-Methoden entwickelt. Hierzu war ein ganzes Paket an Maßnahmen notwendig: So haben wir sieben bis acht Virenscann-Methoden entwickelt, die speziell auf Office-Dokumente mit darin enthaltenen Makros spezialisiert sind. Die Scanner setzen verschiedene Reputationsmechanismen ein, um festzustellen, ob es sich um ein harmloses oder um ein schädliches Makro handelt. Dies geschieht vollautomatisch und in Sekundenschnelle. Ist ein Schadcode gefunden, passen sich die Filter automatisch an, so dass keine weiteren Makro-Viren durch die Filtersysteme schlüpfen können.

Soweit die Informationen von Hornetsecurity. Wir im Hause IKN setzen auch auf diesen Spamfilter und können sagen—ja, er funktioniert hervorragend.
In der Spam-Verwaltungskonsole konnten wir tatsächlich diese Kryptoviren sehen. Da sie aber nicht zu unserem Mailserver weitergeleitet sondern gleich ausgefiltert wurden fühlen wir uns sicher.

Der Spamfilterservice bietet mit einer garantierten Spamerkennung von 99,9% und einer Virenerkennung von 99,99% die höchsten Erkennungsraten am Markt. Er schützt die Mailserver vor DDoS-Angriffen und Nutzer vor Phishing E-Mails. Die mehrstufigen Filtersysteme von Hornetsecurity blocken den Großteil der Spam-Mails bereits beim Eintreffen ab – dadurch bleibt die Quarantäne übersichtlich und leicht zu verwalten.

Sollten Sie es testen wollen -> kein Problem. Gern richten wir eine Testphase für Sie ein.

Sollten Sie ein Angebot wünschen -> kein Problem. Senden Sie uns eine Mail mit der Anzahl Ihrer E-Mail-Nutzer und Sie erhalten umgehend Ihr persönliches Angebot.