SHE Immer eine IT voraus.

Aktuelle Gefährdung durch Krypto-Trojaner (Locky)

Autor: Ralf Naegele

21.03.2016

SHE Informationstechnologie AG
Bereich: Service Delivery Management
Donnersbergweg 3 67059 Ludwigshafen
Fon +49 621.5200-217
Fax +49 621.5200-555
E-Mail: ralf.naegele@she.net

Version 1.0
Status: in Arbeit
Sicherheitsklassifikation: Öffentlich

Aktuelle Gefährdung durch Krypto-Trojaner (Locky)

Bei der aktuellen Verbreitung von Krypto-Trojanern lässt sich durchaus von einer Welle sprechen, die vermehrt Privatpersonen und Firmen bedroht. Die IT-Medien berichten täglich über neue Varianten. Die Hersteller von diesen Krypto-Trojanern haben offensichtlich schnell dazu gelernt, wie Sicherheitsmaßnahmen durch Virenscanner effektiv umgangen werden können, da Antivirenhersteller Probleme haben diese Krypto-Trojaner zeitnah zu analysieren und ihre Virenmuster entsprechend zu aktualisieren. Eine Analyse von Locky zeigt die Einfachheit und Effektivität dieses Trojaner: Mails, welche scheinbar vertrauenswürdig aussehen, enthalten einen Hinweis auf eine Rechnung. Im Anhang befindet sich eine Datei (entweder ein Microsoft Office Word Document mit Macro oder eine einfache Javascriptdatei). Öffnet der Benutzer den Anhang wird der Code ausgeführt und der eigentliche Krypto-Trojaner wird von einem Webserver nachgeladen. An dieser Stelle beginnt dann das Verschlüsseln der Dateien. Die aktuelle Version hört mit dem Verschlüsseln von Dateien lokal aber nicht auf, sondern verschlüsselt auch aktiv Netzlaufwerke. Die Administratoren der Systeme bekommen dann eine Meldung auf Bildschirm mit Anweisungen, wie sie gegen Bezahlung von Bitcoins den Schlüssel zum Entschlüsseln der Dateien bezahlen können. Dies kann im Umfeld eines Unternehmens aber durchaus unternehmenskritisch sein, wie das Beispiel des Lukaskrankenhauses in Neuss zeigte[1]. Hier mussten wegen Krypto-Trojanerbefall die kompletten IT-Systeme heruntergefahren werden. Ein Krankenhaus in Kalifornien hat tatsächlich die Bezahlung vorgenommen, da dies der schnellste Weg war ihre Systeme wieder einsatzfähig zu bekommen[2].

Diese Viruswelle zeigt auch, dass technische Hilfsmittel, die durchaus zur Verfügung stehen, nur ein Teil eines Sicherheitskonzeptes sein können. Mittelpunkt des Angriffes ist die „Schwachstelle“ jeder IT-Systeme und das ist oft der Endbenutzer. Die Meldung vom heise Newsticker „Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde“[3] bedeutet, dass 5000 Endbenutzer in Deutschland aktiv Mailanhänge mit dem Krypto-Trojaner Locky angeklickt haben. Viele Benutzer empfinden IT-Sicherheitsmaßnahmen als lästig, sie stören sie in ihrer Arbeit und behindern mehr, als sie nützen. Oft fehlt es dem Endbenutzer hier am Verständnis, dass IT-Sicherheit nicht einfach

[1] http://www.rp-online.de/nrw/staedte/neuss/neuss-lukas-krankenhaus-kann-nach-hackerangriff-wieder-medikamente-bestellen-aid-1.5773385
[2] http://www.latimes.com/local/lanow/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
[3] http://www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html

nur Mittel zum Zweck ist, sondern dazu da ist, den Endbenutzer selbst zu schützen vor den Gefahren aus dem Internet und damit auch sein Unternehmen zu schützen. Eine regelmäßige Schulung oder zumindest verständliche Informationen für die Mitarbeiter, was passieren kann, warum welche Maßnahmen in einem Unternehmen aktiv sind und welche Folgen unbedachtes Handeln hier haben kann (Stichwort „User Awareness“), muss ein Baustein von jedem IT-Security-Konzeptes sein, wenn es erfolgreich sein will.

Sind die Benutzer hinreichend sensibilisiert, können technische Maßnahmen hier entsprechend unterstützen. Einfach Maßnahmen können eine Härtung der Backend-Mailsysteme in der Form sein, dass z.B. bei Microsoft Exchange-Servern bzw. Outlook als Mailclient generell ausführbare Dateien als Anhänge gesperrt werden. Dazu gehören auch Microsoft Office Dokumente mit Makros oder Javascript-Dateien), optional dass letztere erst nach einer auffälligen Warnung geöffnet werden können. Eine weitere Maßnahme könnte auch in dem Abschalten der HTML-Ansicht des Mailclients bestehen, da diese Ansicht viele Merkmale (z.B. URL-Links die tatsächlich woanders hinzeigen als man vermutet), welche gefährlich sein könnten, vor dem Benutzer verstecken kann. Manche Werbe-Mail dürfte dadurch dem Benutzer nicht mehr ganz so bunt vorkommen, von daher ist diese Maßnahme im Einzelfall abzuwägen.

Technische Maßnahmen / Hersteller

Weitere technische Maßnahmen, welche eher auf Serverebene anzuwenden sind, bieten die Hersteller von IT-Security-Systemen an und helfen einem IT-Security-Konzept, um erfolgreich Krypto-Trojaner abzuwehren:

- Check Point Sandblast: Extrahiert und emuliert eingehende Programme, um auf diese Weise bei verdächtigen Aktivitäten eines Programmes reagieren zu können: http://www.checkpoint.com/products-solutions/zero-day-protection/
- Cisco Advanced Malware Protection (AMP): Cisco Sandboxverfahren als Schutz gegen Malware, integriert in Mail- und Web-Appliances: http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html
- Cisco/IronPort Outbreak Filter: Durch permanentes Monitoring und Analyse von Mailverkehr, werden entsprechende Vorfilter generiert, welche ab einem bestimmten Threat-Level verdächtige Mails zurückhalten, bis die Antivirenhersteller entsprechende Virenmuster bereitgestellt haben: http://www.cisco.com/c/en/us/products/security/email-security-appliance/outbreak_filters_index.html
- Trend Micro Deep Security: Durch die Überwachung der Datei- und Systemintegrität und andere Mechanismen, kann Deep Security frühzeitig einen Trojanerbefall erkennen und abwehren: http://www.trendmicro.de/produkte/deep-security/
- SHE Jericho: Automatisches Erkennen, wenn versucht wird bestimmte Dateien zu verschlüsseln und automatisches Sperren des Benutzers vom Server

Für eine Beratung und Umsetzung der Produkte und Maßnahmen stehen ihnen die SHE-Experten gerne zur Verfügung.