Veröffentlicht auf *LANline* (http://www.lanline.de)

Hacken mit Bildern

Cirosec IT-Defense 2016 in Mainz
Hacken mit Bildern
geschrieben von LANline/wg am 28.01.2016

Zum 14. Mal konnte Veranstalter Cirosec über 200 Teilnehmer auf seiner Sicherheitskonferenz IT-Defense begrüßen, dieses Jahr in Mainz. Das Vortragsspektrum reicht vom Thema Hacken mit Bildern über Angriffe auf vernetzte Fahrzeuge bis hin zu einem Abschlussvortrag von Prof. Gunter Dueck über „Schwarmdummheit“.

Saumil Shah eröffnete den ersten Veranstaltungstag mit seinem Vortrag über Browser-Exploits via kompromittierter Bilddateien mit Stegosploit. „Ein guter Exploit ist einer, der mit Stil ausgebracht wird“, so Shah. Stegosploit versteckt Exploit-Code in den Pixeln. Das Verfahren, so Shah, nutze Polyglotte, also das Vermischen von Mustern, die gegenseitig ihre Syntax brechen (wie man dies zum Beispiel von manchen Bildern von M.C. Escher her kennt).

Für ein Browser-Exploit, erläuterte Shah, bringe das Stegosploit-Toolkit Steganografie-Tools, Polyglott-Tools und Exploits mit. Der binäre Code des Exploits werde dazu in einem niedrigen Bit-Layer der Acht-Bit-Grauskala bestimmter Pixel (jedes dritte, jedes vierte...) versteckt. Er demonstrierte das Verfahren mit einem vorbereiteten Exploit-Code: Bei Code-Einbringung in Bit-Layer 7 wäre die Manipulation noch sichtbar, auf Bit-Layer 2 aber ist sie für das menschliche Auge nicht mehr erkenntlich.

Ein Problem, so Shah, stellen dabei JPGs dar, da deren Code beim Speichern aufgrund der Kompromierung verändert wird. Durch einen iterativen Ansatz konnte Shah allerdings diese Hürde überwinden: Nach zirka neun Iterationen erhalte man trotz der JPG-Komprimierung einen verlustfreien Code.

Jeder Browser, der HTML5 unterstützt, sei heute dank der Canvas-Integration in HTML 5 in der Lage, ein derart manipuliertes Bild zu decodieren. Für einen Angriff sei dann ein Polyglott mit Auto-Run-Javascript-Code erforderlich, gegen eine Entdeckung helfe eine Verschlüsselung des Decoder-Scripts. Der Angriff, den er live demonstrierte, funktioniere auch für PNGs, zumal diese verlustfrei gespeichert werden.

Bildbasierte Angriffe, so Shah, seien derzeit dabei, „in freier Wildbahn“ Verbreitung zu finden. Ein schneller Workaround zur Abwehr sei es, alle Bilder neu zu codieren. Das grundlegende Problem seien die Browser, da sie keine Parser enthalten, die eine strikte Einhaltung der Vorgaben durchsetzen. Nötig seien wirklich strenge Parsing-Regeln für Browser.

Weitere Meldungen von der IT-Defense folgen in Kürze. Informationen zur IT-Defense finden sich unter www.it-defense.de.