Angriffe mit USB-Sticks

Wechseldatenträger sind ein interessantes Ziel für Cyberkriminelle: Sie können damit auch Netze außerhalb des Internets erreichen.

Hackerangriffe sind nicht unbedingt auf das Internet angewiesen, ein infizierter USB-Stick reicht da schon aus, um Zugang zum Gerät zu verschaffen.

Das Beispiel ist inzwischen ein Klassiker: Vor ein paar Jahren sorgte ausgerechnet das französische Militär für Kopfschütteln bei Experten für IT-Sicherheit. In Militärrechnern ohne Verbindung mit dem Internet verbreitete sich eine Schadsoftware so schnell, dass die Streitkräfte ihr internes Netzwerk ausschalten mussten.

Was war passiert? Zwei banale, ohne Aufwand vermeidbare Nachlässigkeiten ermöglichten das Malheur. Erstens wurde eine längst verfügbare Sicherheitsaktualisierung für Windows nicht an die Rechner verteilt und zweitens wurden die USB-Anschlüsse nicht genügend überwacht. So konnten mit der Malware infizierte USB-Sticks die Sicherheitslücke ausnutzen.

Sprung über das „Air Gap“

Dies zeigt deutlich, dass Hackerangriffe nicht unbedingt auf das Internet angewiesen sind, um einen Computer zu erreichen. Nicht nur beim Militär, auch in vielen Unternehmen gibt es IT-Systeme, die mit dem sogenannten „Air Gap“ von der Außenwelt isoliert sind. Sie haben keine Verbindung zum Internet, wodurch sich zahlreiche Unternehmen recht sicher fühlen.

Diese Scheinsicherheit macht es Cyberkriminellen häufig sehr leicht. Schon seit einiger Zeit treibt der Spionage-Ring Sednit, auch bekannt als Sofacy-Gruppe, APT28 oder „Fancy Bear”, sein Unwesen und hat bereits eine Vielzahl an Institutionen angegriffen.

Forscher des IT-Sicherheitsspezialisten ESET haben eine perfide Angriffstechnik von Sednit aufgedeckt: Win32/USBStealer kann auch Computer und Netzwerke wirksam angreifen, die physisch völlig isoliert sind. Die Verbreitung erfolgt über Wechseldatenträger wie zum Beispiel USB-Sticks. Das Ziel der Kriminellen sind in der Regel bestimmte Dateien, die ganz gezielt angegriffen werden.

Nach Einschätzung von ESET bedient sich Sednit bereits seit etwa zehn Jahren dieses Tools. Dabei wird zunächst ein Computer infiziert, der mit dem Internet verbunden ist. Die Malware erkennt, wenn ein USB-Stick eingelegt wird und kopiert sich darauf.

Wird dieser Stick nun in einen anderen Computer ohne Internetverbindung eingelegt, wird dieses Gerät infiziert. Anschließend verbreitet sich der Trojaner weiter, zum Beispiel über ein internes Netzwerk. Die Schadsoftware kann für gezielte Spionageaktionen genutzt werden, die zur Spezialität der Sednit-Gruppe gehören.

Angriffe durch veränderte USB-Firmware

Im Oktober 2014 hatte ESET aufgedeckt, dass die Gruppe sogenannte Watering-Hole-Angriffe mittels eines maßgeschneiderten Exploit Kits ausgeführt hatte. Dabei werden die Besucher einer bestimmten Webseite umgeleitet auf eine Seite mit Schad-Software, die dann im Hintergrund installiert wird.

Die Gefahr eines solchen Angriffs ist ebenso groß wie das Risiko durch sogenannte BadUSB-Malware. Dabei wird die Firmware eines USB-Sticks so verändert, dass der USB-Controller im Computer umprogrammiert wird.
Die Malware befindet sich also nicht relativ leicht identifizierbar auf dem Datenbereich, sondern gut versteckt im Systembereich. Ein großer Teil der verbreiteten USB-Controller-Chips hat keinerlei Schutz gegen eine solche Umprogrammierung.

Durch Hacking-Tricks dieser Art wird deutlich: Die Gefahren kommen oft aus einer Richtung, die in den Sicherheitskonzepten von Unternehmen leicht übersehen wird. Externe Datenträger wie USB-Sticks, Mobilgeräte im Storagemodus oder Speicherkarten können ebenso zum Risiko werden wie eine ungeschützte Internetverbindung.