

## **Bekanntwerden der IP-Adresse trotz VPN-Tunnel**

Mit den folgenden beiden Vorbedingungen kann trotz Anonymisierungs-VPN die IP-Adresse eines Anwenders ermittelt werden:

1. In den Netzwerkeinstellungen ist IPv6 eingeschaltet, damit IPv6-Verkehr über IPv4 getunnelt werden kann. Bei Windows Vista und Windows 7 ist das die Voreinstellung, auch wenn keine IPv6-Adresse des Providers vergeben ist.
2. Der Computer ist über eine öffentliche IP-Adresse im Internet, es befindet sich nicht hinter einem Router, der eine interne Adresse über NAT in eine öffentliche umwandelt.

Treffen beide Bedingungen gleichzeitig zu, kann die öffentliche IP-Nummer in IPv6-Anfragen eingebettet und damit übermittelt werden, beispielsweise durch das Anstoßen von IPv6-P2P-Verbindungen durch einen Angreifer. Die Gefahr wird beseitigt, wenn man in den Netzwerkeinstellungen IPv6 deaktiviert.

## **Kompromittierter TrueCrypt-Bootloader**

Mit EvilMaid von <http://invisiblethingslab.com> kann der Bootlader einer vollverschlüsselten TrueCrypt-Installation geknackt werden. Dazu wird der PC von einem USB-Stick gebootet, der die Laderoutine durch eine infizierte ersetzt. Gibt der Anwender beim nächsten Systemstart sein TrueCrypt-Paßwort ein, kann es bei einem erneuten Start mit EvilMaid aus dem kompromittierten Bootloader ausgelesen werden. Der Angreifer muß für das Ermitteln des Paßworts zweimal den PC von USB starten. Das kann man bei einem unbewachten Notebook in einem Hotelzimmer sehr einfach dadurch verhindern, daß das BIOS, in dem das alternative Booten von anderen Datenträgern als der Festplatte abgeschaltet ist, durch ein Paßwort geschützt wird.

Hat man das Empfinden, daß jemand Unberechtigtes am PC war, sollte der Computer außerdem gestartet, die TrueCrypt-Verschlüsselung zurückgenommen und dann neu installiert werden. Dabei wird wieder ein neues Bootladeprogramm geschrieben und das infizierte entfernt.