Achtung! Weiterverbreiten:

Im beigefügten PDF-Dokument erklären englische Ingenieure, was sie über das geheime Eigenleben von DSL-Modems und Routern herausgefunden haben.

In den Informationen, die bislang zum Spionageskandal von NSA und GCHQ bekannt wurden, war immer nur die Rede davon, daß die Spitzeldienste Informationen anzapfen und Verschlüsselungen knacken über sogenannte
“Man in the middle
“-Angriffe (
MITM
), die über irgendwelche
Router
geschehen, wobei die enthüllte Präsentation der
NSA
suggerierte, daß diese angezapften Router bei
Google
oder anderen Konzernen bzw Internetanbietern liegen. Dadurch entstand das Bild, das entweder Datenleitungen direkt angezapft werden (z.B. Seekabel, Internetknotenpunkte) oder Daten bei Internetanbietern abgezweigt werden.

Doch neben diesen aufwendigeren Varianten gibt es noch eine viel brisantere und bislang unenthüllte Methode:

In der Firmware (Betriebssystem) beinahe aller Modems und Router steckt ein direkter Zugang für die Geheimdienste, der von der geräteigenen Firewall völlig unbeeinflußt bleibt. Es werden immer zwei Internetverbindungen geöffnet. Erstens die uns bekannte Verbindung zu unserem Internetanbieter und zweitens eine heimliche Verbindung zum
“DoD Network Information Center
“, d.h. zu einem Server des US-Verteidigungsministeriums!

Diese Art von Bespitzelung ist für die Geheimdienste noch viel wichtiger, da sie ihnen direkten Zugriff auf alle Computer und andere Geräte erlaubt, die über das LAN-Kabel oder WLAN an R outer

bzw.
Modem
angeschlossen sind. Es können damit z.B. beliebig Dateien auf Ihrem Computer gelöscht, kopiert, verändert oder aufgespielt werden. Verschlüsselungen werden umgangen, Ihre Festplatte kann gelöscht oder in vielen Fällen der PC ganz zerstört werden. Alles was ein Hacker der direkt an Ihrem Rechner sitzt machen könnte, können auch die Geheimdienste über diese geheime “Standleitung” machen.

All dies geschieht mit Wissen und Unterstützung der Internetanbieter und in vielen Fällen auch der Modemhersteller. Diese Information dürfte noch Wellen schlagen, denn was hier geschieht ist höchst illegal und selbst mit unseren faschistoiden “Anti-Terrorgesetzen” nicht begründbar. Mit dieser Technik wird nicht nur “irgendwo” im quasi öffentlichen Raum des Internets bespitzelt, sondern es wird explizit Spionage- und Manipulationstechnik innerhalb jedermanns Wohnung installiert, ohne daß auch nur irgendein “Terrorverdacht” besteht.

Die Abkürzung MITM müsste also eher als “Man in the modem” übersetzt werden und nicht mit “ Man in the middle“.

Wie man diese Schweinerei nachweisen und wie man sich dagegen schützen kann steht in dem detaillierten Bericht:

Full-Disclosure NSA-GCHQ-Hacks

quelle: politaia.org