CIA nutzt gehackte W-Lan-Router zum Abhören – Handbuch aufgetaucht

von Edgar Gärtner

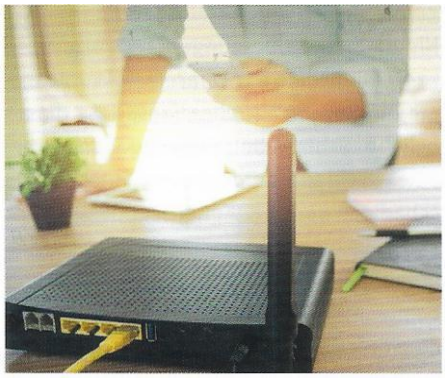
Quelle: KOPP-exclusiv Nr. 27/2017

Früher war das Ausspionieren von Personen ein aufregendes Abenteuer: Wanzen, heimliche Fotos, »*tote Briefkästen*«. Heute gibt es solche Abenteuer nur noch im Kino. Statt versteckt unter Schlapphüten und Trenchcoats um die Ecken zu schleichen, sitzen Spione in Bürosesseln vor PC-Bildschirmen. Wie das geht, schildert ein Handbuch der CIA

Die Enthüllungsplattform *Wikileaks* hat nun einen Beweis geliefert und zwar in Form eines 170 Seiten dicken Benutzer-Handbuchs der CIA.

❖ Dort wird im Detail beschrieben, wie zehn gängige US-Router-und Access-Point-Modelle, die auch in Europa gebräuchlich sind - wie *Linksys, D-Link* oder *Belkin* - auch bei vorhandenem Passwortschutz gehackt und mithilfe eines eingeschleusten Trojaner-Programms mit dem Codenamen *»CherryBlossom*« (*Kirschblüte*) für Lauschangriffe eingesetzt werden können. Diese Software funktioniere auf insgesamt 25 Router-Modellen und mit kleinen Modifikationen auch auf 100 weiteren Fabrikaten, heißt es in dem Handbuch.

- Sobald ein Router mit dem Kirschblüten-Trojaner infiziert ist, verwandelt er sich laut Handbuch in eine »*Fliegenfalle*«, die auf Anweisung eines CIA-Servers namens »*CherryTree*« (*Kirschbaum*) Informationen sammelt und als »*Beacons*« (*Lichtsignale, Leuchtfeuer*) in verschlüsselter Form an den CIA-Server übermittelt. Die Anweisungen, die der Router vom Server erhält, können sich auf bestimmte Computer und Telefone in einem Gebäude beziehen, die mithilfe ihrer IP- und MAC-Adresse (*Internet-Protokoll- und physikalische Adresse*) identifiziert werden.
- Mithilfe der jeweils verwendeten e-Mail-Adressen und Benutzernamen lassen sich aber auch die Internetnutzung und die Kommunikation einzelner Personen kontrollieren. Neben der »Fliegenfalle« und dem »Kirschbaum« gibt es noch ein »CherryWeb«, mit dessen Hilfe überprüft werden kann, ob die »*Fliegenfalle*« noch gebraucht wird und man ihr eventuell neue Anweisungen geben sollte.



Das CIA-Handbuch enthält darüber hinaus detaillierte Pläne der Architektur des ganzen Abhörsystems, die hier aber nicht interessieren. Die Erstfassung des Handbuchs stammt übrigens aus dem Jahre 2007.

Es bleibt unklar, ob es in den vergangenen zehn Jahren ständig genutzt wurde oder ob zwischenzeitlich evtl. weitere Gebrauchsanweisungen für Lauschangriffe eingeführt wurden

→ Denn es gibt vermutlich noch andere Wege der Fernüberwachung von Personen und ihrem Datenverkehr.

Büro mit Kabeln ist sicherer

Das Hacken von W-LAN-Routern ist aber sicher einer der gangbarsten und wird deshalb vermutlich intensiv genutzt. Daher ist generell Vorsicht beim Einsatz dieser Geräte geboten. Ein klassisches Büro- oder Heimnetzwerk (LAN) mit Kabeln ist wohl sicherer und meistens auch schneller als ein bequemes W-LAN, das wegen der allgegenwärtigen Radiowellen möglicherweise auch gesundheitliche Risiken birgt. Es kann durchaus sein, dass Smartphones für Geheimdienste inzwischen eine ergiebigere Informationsquelle darstellen als W-LAN-Router.

Die der Weltöffentlichkeit durch den Informatikspezialisten und ehemaligen CIA-Mitarbeiter *Edward Snowden* zugänglich gemachten Abhörprotokolle der US National Security Agency (NSA) zeigen, dass den großen Geheimdienstorganisationen heute kaum noch etwas entgeht.

→ Nach jedem islamistischen Anschlag stellt sich heraus, dass die Attentäter bereits auf dem Bildschirm der Geheimdienste waren.

Das wirft die Frage auf, ob es die Geheimdienstmitarbeiter lediglich nicht geschafft haben, die ihnen zur Verfügung stehenden Daten rechtzeitig auszuwerten, oder ob sie in bestimmten Fällen aus politischen Erwägungen Attentatsvorbereitungen bewusst zugelassen haben.

Als heikel erwies sich auch die von Snowden enthüllte Tatsache, dass *NSA* und *GCHQ* systematisch Spitzenpolitiker auch befreundeter beziehungsweise verbündeter Staaten ausspionieren. Zum Beispiel überwachte das *GCHQ* im Jahre 2009 beim Londoner G20-Gipfel die Kommunikation aller anwesenden Staatschefs.

G-20 Gipfel wurde ausgespäht

Britische Politiker konnten während des Treffens sämtliche Mobilfunkverbindungen ihrer ausländischen Amtskollegen verfolgen. Das sorgte für diplomatische Verwicklungen, als Snowden im Jahre 2013 die von ihm kopierten Geheimdienstinformationen an die Öffentlichkeit brachte. Daraus geht hervor, dass das *GCHQ* auch die Telefonanlage der Bundesregierung in Berlin anzapft. Im Deutschen Bundestag wurde daraufhin der *NSA-Untersuchungsausschuss* eingerichtet. Doch der BND warnte die Abgeordneten davor, ihre Nase zu tief in das enge Beziehungsgeflecht zwischen *GCHQ* und *NSA* zu stecken, da er von deren Informationen abhängig sei.

Aus den von Snowden veröffentlichen Dateien geht hervor, dass das *GCHQ* über die *Abhörstation Bude in Cornwall* das *Untersee-Glasfaserkabel TAT-14 der Deutschen Telekom* anzapft. Dieses Kabel führt von der ostfriesischen Kleinstadt Norden über Bude in die USA. Die Behörde beschäftigt sich jetzt verstärkt mit sozialen Netzwerken wie *Facebook, Twitter, Linkedln* und *Google+*.

Automatische Programme erlauben es dem *GCHQ*, die ausgewiesene Zugriffsrate auf Webseiten zu manipulieren und die Ergebnisse von Online-Abstimmungen zu beeinflussen. Zu ihren Aufgaben gehört auch die gezielte Rufschädigung beziehungsweise mediale Hinrichtung von unliebsamen Personen und Unternehmen durch Fehlinformationen.