EUROLUFTBILD.DE / AKG-IMAGES

US-Konsulat in Frankfurt am Main: Mehr Steuergelder für Cyberabwehr und Angriffsmethoden

„Die USA sind die Guten“

Sicherheit Deutsche Geheimdienstler reagieren gelassen auf die jüngsten CIA-Leaks – und blicken neidvoll auf das Cyberwaffen-Arsenal der Amerikaner.

Im Frankfurter US-Generalkonsulat arbeiten rund 900 Menschen für die Regierung der Vereinigten Staaten – und nicht alle haben mit Visafragen und Passangelegenheiten zu tun. Der ausgedehnte Gebäudekomplex im Stadtteil Eckenheim, ein ehemaliges Militärkrankenhaus, umfasst auch eine „Sensitive Compartmented Information Facility“, einen besonders gesicherten Bereich, zu dem nur Mitarbeiter der US-Geheimdienste Zugang haben.

Auch der Auslandsgeheimdienst CIA ist in dem Riesenkomplex mit seinen Agenten vertreten; unter anderem organisierte der Dienst von hier aus einst ein Netz von Geheimgefängnissen in Osteuropa und Marokko, in denen US-Häftlinge von besonderer Bedeutung („High-Value Detainees“) außer Landes gefoltert wurden.

Nun hat die Enthüllungsplattform WikiLeaks unter dem Namen „Vault 7“ knapp 9000 Dateien aus der CIA-Abteilung „Center for Cyber Intelligence“ veröffentlicht, in denen Frankfurt erneut prominent vorkommt: Demnach starten die Agenten der Agency von Frankfurt aus auch Attacken an der neuesten Front: dem Cyberkrieg.

Die neuen Enthüllungen zeigen, dass Deutschland weiter eine zentrale Basis für heikle verdeckte US-Operationen in Europa ist. Weder die Proteste über die Drohnensteuerung via Ramstein noch die Snowden-Veröffentlichungen haben daran etwas geändert. Ließ das Bundesamt für Verfassungsschutz (BfV) damals noch Helikopter über die US-Einrichtungen fliegen, herrscht bei deutschen Sicherheitsbehörden nun demonstrative Gelassenheit.

Auch die Empörung der Bundesregierung halte sich diesmal offenbar in noch engeren Grenzen, sagt ein hoher Sicherheitsbeamter. „Es gibt die Bösen, die bei uns spionieren, und es gibt die Guten“, erklärt er lakonisch. „Die USA sind die Guten. Ihr Aufklärungsinteresse deckt sich derzeit mit unserem zu 90 Prozent.“

Größere Neugier zeigen Gesprächspartner aus deutschen Diensten, wenn es um den nun veröffentlichten Werkzeugkasten der CIA-Cyberkrieger geht. Wie auch die NSA hat er für jedes Betriebssystem und jedes Endgerät eigene Einbruchslösungen parat. Über seine Wege in die mobilen Betriebssysteme von Apple (iOS) und Google (Android) kann er offenbar auch Nachrichten vermeintlich sicherer Messenger-Dienste wie Telegram mitlesen.

Viele der Fähigkeiten aus der CIA-Giftküche sind in Varianten sogar schon öffentlich vorgestellt worden. Dass „smarte“ Fernseher sich, ähnlich wie viele andere vernetzte Geräte, in Wanzen verwandeln lassen, ist seit Jahren Thema auf Hackerkonferenzen. Und 2015 führten IT-Experten vor, wie sie einen Jeep Cherokee von ihrem Rechner aus unter ihre Kontrolle brachten.

Die CIA hätte ihre Hausaufgaben nicht gemacht, würde sie über diese Fähigkeiten nicht längst verfügen. Gleiches gilt wohl für die anderen Staaten mit offensiv agierenden Cybertruppen wie Russland und China. Vertreter einer großen israelischen Rüstungsfirma, die eng mit den Geheimdiensten des Landes verbunden ist, erklärten gegenüber dem SPIEGEL schon vor Monaten, sie könnten die Verschlüsselung von Messenger-Nachrichten zwar nicht knacken – aber umgehen.

Die Verbreitung dieses Wissens ist indes alles andere als beruhigend, denn es macht das Internet für alle Nutzer unsicherer. Es ist paradox: Während immer mehr Steuergelder für die Cyberabwehr ausgegeben werden, fließen gleichzeitig immense Mittel in neue Angriffsmethoden, auch hierzulande.

In München wird dafür noch in diesem Jahr sogar eine neue Behörde aufgebaut: Die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“ soll vor allem verschlüsselte Onlinekommunikation knacken.

Auch die deutschen Geheimdienste kennen sich inzwischen mit „Exploits“ aus – jenen Schwachstellen in Programmen, die Eindringlingen den Zugang erleichtern. So will sich der Bundesnachrichtendienst (BND) im Rahmen seiner „Strategischen Initiative Technik“, eines 300-Millionen-Euro-Programms, bis 2020 auf den neuesten Stand bringen. Dabei plant er laut internen Unterlagen auch, derlei „Exploits“ von Dritten einzukaufen.

Da die rechtliche Grundlage hierfür aber noch weitgehend unklar ist, müssen die entsprechenden Gesetze für den BND oder das BfV möglicherweise erweitert werden.

„Das ist ein sehr sensibler Bereich, an den sich so richtig niemand traut“, sagt einer, der an den ersten Diskussionen mit Behörden und Ministerien beteiligt war. „Aber der Bedarf bei den Diensten, zum Beispiel endlich das Problem der verschlüsselten Chats zu lösen, ist riesig.“

In deutschen Behörden wurden die neuesten Enthüllungen deshalb intensiv studiert – immerhin lesen sie sich teils wie eine Gebrauchsanweisung für die Hightechspionage. „Als Erstes“, sagt ein Sicherheitsbeamter, „habe ich mir am Montag alle Dokumente gesichert.“

Martin Knobbe, Marcel Rosenbach