Forum InformatikerInnen für Frieden
und gesellschaftliche Verantwortung e.V.

Pressemitteilung vom 11.11.2014

BND will Cyber-Angriffskrieg vorbereiten

Studie von NATO-Experten zeigt sicherheitspolitische Gefahren auf

Wie der Spiegel in seiner aktuellen Ausgabe berichtet, beantragt der Bundesnachrichtendienst (BND) Haushaltsmittel, um das Wissen um Schwachstellen in Softwaresystemen aufzukaufen. Mit so genannten Zero-Day-Exploits – der Begriff umschreibt der Öffentlichkeit unbekannte Sicherheitslücken – will der BND weltweit in Computersysteme einbrechen, sie sabotieren und den Datenverkehr abfangen.

Der Einbruch in fremde Computersysteme bedeutet die Planung offensiver Cyberoperationen. Solche Cyberoperationen bergen erhebliche Gefahren. Das NATO Cooperative Cyber Defence Center of Excellence (NATO CCD COE) hat führende Experten im internationalen Recht mit einer detaillierten Bewertung von Cyberattacken beauftragt. Laut dem so genannten „Tallinn-Manual“ sind Cyberangriffe bereits dann als kriegerische Handlung zu bewerten, wenn sie von zivilen Stellen ausgeübt werden, die von staatlicher Seite nicht daran gehindert werden. Hacker sind danach bereits legitime Angriffsziele, wenn sie ein System auf Schwachstellen untersuchen. Cyberangriffe durch staatliche Stellen werden eindeutig als internationaler Konflikt bewertet, die militärisch-geheimdienstliche Gegenreaktionen rechtfertigen. Sofern durch solche Computermanipulationen erhebliche materielle Schäden verursacht werden – z.B. an Infrastruktursystemen wie bei der Computersabotage am Energienetz – sind angegriffene Staaten sogar zu einer konventionellen militärischen Antwort berechtigt, so die NATO-Experten.

„Folgt man dieser Bewertung der NATO, will der BND in die Vorbereitung eines Cyber-Angriffskrieges einsteigen und beschwört mit seinen beabsichtigten Computermanipulationen geheimdienstliche und militärische Gegenreaktionen auf Computersysteme in Deutschland herauf“, erklärt Stefan Hügel, Vorsitzender des FIfF und Sprecher der Kampagne. „Bisher waren die zuständigen Behörden des Bundes offenbar nicht einmal in der Lage, ihre Systeme vor Ausspähung und Sabotage zu schützen. Wenn der BND das Wissen um IT-Sicherheitslücken kaufen will, um sie für Cyberangriffe zu nutzen, statt diese Lücken zu schließen, zeigt sich damit aufs Neue eine alarmierende Unkenntnis über die Gefahren von Cyberattacken und ein Mangel an Verantwortung gegenüber der Sicherheit unseres Landes.“

Sylvia Johnigk, Vorstandsmitglied des FIfF und ebenfalls Sprecherin der Kampagne „Cyberpeace“ des FIfF ergänzt: „Die Staatsgewalt ist dazu verpflichtet, das vom Bundesverfassungsgericht 2007 definierte „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ umzusetzen. Wenn Nachrichtendienste Sicherheitslücken in IT-Systemen vorsätzlich ausnutzen, statt sie zu schließen, ist dies ein Bruch von Grundrechten. Das FIfF fordert die Bundesregierung auf, die Sicherheit Deutschlands nicht zu gefährden und dem unverantwortlichen Spiel mit digitalen Angriffswaffen Einhalt zu gebieten!“

Mehr zur Kampagen siehe **cyberpeace.fiff.de**

Bremen, 7. November 2014

FIfF e.V. • Goetheplatz 4 • 28203 Bremen • T 0421 3365 9255 • F 0421 3365 9256 • fiff@fiff.de • www.fiff.de