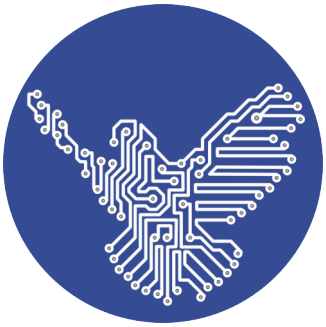
Forum InformatikerInnen für Frieden
und gesellschaftliche Verantwortung e.V.



Presseerklärung des FIfF e.V. vom 26.11.2014

Ganz großes Staatstheater – Die Geister, die ich rief, ich werd sie nicht mehr los

In dieser Woche wird im Deutschen Bundestag ein Staatstheater der besonderen Art aufgeführt, das es an Überheblichkeit und Wichtigtuerei mit Goethes Zauberlehrling aufnehmen kann. Die Beamten des Bundesnachrichtendienstes (BND) werden unseren Vertretern im Deutschen Bundestag vorführen, wer sich ihrer Ansicht nach in diesem Staat nicht zu verantworten, aber stets etwas zu sagen hat.

Am 28. November soll nach dem gegenwärtigen Stand im Deutschen Bundestag über die Haushaltsmittel beraten werden, mit denen der BND das Wissen von Kriminellen über geheim gehaltene Software-Schwachstellen – sog. Zero-Day-Exploits – aufkaufen will. Daraus soll Schadsoftware entwickelt werden, um Computersysteme im Ausland anzugreifen und zu sabotieren. Der BND hat bereits erklärt, „man müsse jetzt auf Augenhöhe mit anderen Diensten operieren". Dass NATO-Rechtsexperten eine staatliche Computersabotage als militärische Aggression mit erheblichen Eskalationsgefahren werten, wird seitens des BND verschwiegen.

Diese Woche soll dem „Fokus" zufolge die Bundesanwaltschaft die Untersuchungen zur Überwachung des Handys der Bundeskanzlerin einstellen – mangels Beweisen. Bemerkenswert ist, dass weder die Deutsche Telekom noch das Telekommunikationsunternehmen NetCologne jene Sicherheitslücken in ihren Computersystemen finden konnten, durch die die NSA Interna aus den Steuerungssystemen beider Unternehmen abgreifen kann. Interessant wird dies durch die aktuellen Veröffentlichungen über den Trojaner Regin, der zu 28 % auf Backbones von Telekommunikationsunternehmen aufgetaucht ist und von der Funktionalität her, Aktivitäten und Daten in der infizierten Infrastruktur aufzeichnen und an den GHCQ bzw. an die NSA übermitteln soll. Die Telekom bestreitet laut „Spiegel-Online", dass sie von Regin betroffen war. Dieses Dementi kommt verdächtig schnell. „Eine solche Analyse braucht deutlich mehr Zeit" kommentiert Kai Nothdurft, IT Sicherheitsexperte im FIfF Vorstand.

Deutsche Behörden und Unternehmen beweisen wieder mal, dass sie nicht mal im Ansatz in der Lage sind, die Kommunikations- und IT-Systeme der wichtigsten Personen des politischen Lebens im Lande zu schützen, geschweige denn die der Bürger und Bürgerinnen. Und weil sie ganz offensichtlich nichts von IT-Systemen verstehen, wollen sie nun Wissen über Sicherheitslücken zukaufen – aber nicht, um unseren Staat und die Bürger zu schützen, sondern um selbst zu Cyberangreifern zu werden.

Das wirkt fast schon verzweifelt mutig, ist aber letztendlich gefährlich dumm. Cyberangriffe ziehen häufig Gegenreaktionen nach sich, also weitere Angriffe auf Computersysteme in Deutschland. „Angriffe von anderen Staaten auf dem Qualitätsniveau von Regin können gegenwärtig weder Staat noch Unternehmen entdecken, geschweige denn unterbinden", gibt Sylvia Johnigk, ebenfalls Sicherheitsexpertin im FIfF Vorstand zu bedenken. Sie spricht aus der Praxis, denn sie berät Unternehmen im Bereich Informationssicherheit.

Wir sorgen uns über außenpolitische Krisenherde wie in der Ukraine und die daraus entstehende Gefahr für die Versorgung mit russischem Erdgas. Mit Cyberwaffen in Händen des BND brauchen wir für solche Szenarien gar keine Konflikte im Ausland. Ein wenig Schadsoftware, ein kleiner Cyberangriff eines anderen Staates und die Gegenreaktion des Angegriffenen kann völlig ausreichen, um zum Beispiel die Energieversorgungssysteme hierzulande zusammenbrechen zu lassen.

Zero-Day-Exploits durch den BND aufzukaufen, daraus Cyber-Angriffswaffen zu entwickeln und für Angriffe einsetzen zu wollen ist kriminell und unverantwortlich. Die vom BND geforderten 300 Mio. € für Cyberangriffssysteme sind eine Gefährdung der Sicherheit Deutschlands. Nötig ist stattdessen, dass zum Beispiel das BSI solches Wissen bekannt macht und dafür sorgt, die Sicherheitslöcher in staatlichen und zivilen IT-Systemen zu stopfen. Das Geld sollte in Personal und Infrastruktur fließen, um einen vertrauenswürdigen und transparenten „Cyber-Zivilschutz" zu gewährleisten.

Pressekontakte: Sylvia Johnigk, 0179 289 7714, Kai Nothdurft, 0172 856 1971, cyberpeace.fiff.de