Ressort: Technik

Bericht: Deutschland plant Cyber-Gegenschläge

Berlin, 19.04.2017, 17:13 Uhr

GDN - Die Bundesregierung will offenbar die Voraussetzungen schaffen, um im Fall eines Cyber-Angriffs zurückschlagen zu können und um darüber hinaus auch in der Lage zu sein, notfalls feindliche Server zu zerstören. Der Bundessicherheitsrat unter Vorsitz von Kanzlerin Angela Merkel beschloss laut eines Berichts von "Süddeutscher Zeitung", NDR und WDR Ende März, eine Analyse der hierfür benötigten technischen Fähigkeiten vornehmen zu lassen.

Zudem sollen der Regierung Vorschläge für notwendige gesetzliche Änderungen vorgelegt werden. Im Sommer sollen die Ergebnisse dem geheim tagenden Bundessicherheitsrat präsentiert werden. Unter Experten sind solche Maßnahmen als "Computer Network Operations" oder "Hack Back" bekannt. Während eines laufenden Angriffs wird der Angreifer identifiziert, Cyber-Kräfte blocken die Attacke ab oder zerstören die Server, über die der Angriff läuft, zum Beispiel durch Schadsoftware. Voraussetzung dafür wäre, dass ein Rechtshilfeersuchen ohne Aussicht auf Erfolg ist und sich der Angriff aus dem Ausland nicht anders stoppen lässt. In Regierungskreisen ist von einem "digitalen finalen Rettungsschuss" die Rede, schreiben die drei Medien. Als Beispiel werde etwa ein Angriff auf ein Stromnetz genannt oder ein weiteres Hacking des Deutschen Bundestages. In diesem Fall etwa könnten auch die Server vom Netz genommen werden, auf denen sich gestohlene Daten aus dem Parlament befinden. Allerdings fehlt es für derlei Vorhaben bisher an einer gesetzlichen Grundlage. Die Bundeswehr, die gerade eine eigene Cyber-Teilstreitkraft installierte, ist nur bei einem kriegerischen Akt aus dem Ausland zuständig oder wenn die eigene Truppe angegriffen würde. Um die Regelungslücke bei Angriffen auf zivile Ziele zu schließen, sollen nun entsprechende gesetzliche Vorschläge erarbeitet werden, schreiben SZ, NDR und WDR. Langfristig gebe es innerhalb der Bundesregierung zudem die Überlegung, die Abwehr von Cyber-Angriffen vollständig dem Bund zu übertragen. Da Gefahrenabwehr aber Sache der Länder ist, wäre hierfür eine Grundgesetzänderung notwendig. Hack Back-Attacken gelten als riskant, oft ist es schwer zu identifizieren, wer tatsächlich hinter einem Angriff steckt. Auch besteht das Risiko, dass die Angreifer - ähnlich menschlichen Schutzschilden im Krieg - für ihre Angriffe Server kapern, auf denen besonders sensible Daten lagern. Als fiktives Beispiel nannte das Bundesamt für Sicherheit in der Informationstechnik (BSI) unlängst den Server einer Frühchen-Station eines Krankenhauses. Unklar ist bisher auch, welche Behörde mit dem Auftrag ausgestattet werden soll. Infrage kommen neben dem BND der Verfassungsschutz, das Bundeskriminalamt oder die Experten des BSI. Dort ist heute bereits das sogenannte Cyber-Abwehrzentrum angesiedelt, das in jedem Fall ausgebaut und eine zentrale Rolle bei der Abwehr von Angriffen spielen soll.

Bericht online:
https://www.germandailynews.com/bericht-88245/bericht-deutschland-plant-cyber-gegenschlaege.html

Redaktion und Veranwortlichkeit:
V.i.S.d.P. und gem. § 6 MDStV:

Editorial program service of General News Agency:
UPA United Press Agency LTD
483 Green Lanes

UK, London N13NV 4BS
contact (at) unitedpressagency.com
Official Federal Reg. No. 7442619