Abwehr von Cyberangriffen

Regierung will den "Hack Back"

Stand: 19.04.2017 17:00 Uhr

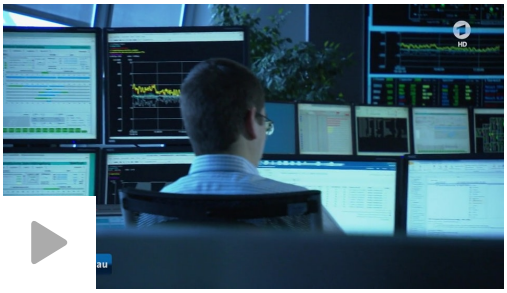
Wenn ein Hackerangriff etwa das deutsche Stromnetz lahmlegt, muss die Bundesregierung schnell handeln. Nach Recherchen von NDR, WDR und SZ plant sie, bei diesem Szenario digital zurückzuschlagen. Der "Hack Back" wirft viele Fragen auf - nicht nur rechtliche.

Von Georg Mascolo und Jan Strozyk, NDR

Die Bundesregierung will eine Grundlage schaffen, um bei Angriffen im Internet aktiv zurückschlagen zu können. Nach Informationen von NDR, WDR und "Süddeutscher Zeitung" erteilte der Bundessicherheitsrat unter dem Vorsitz von Bundeskanzlerin Angela Merkel im März den Auftrag, zwei Analysen anzufertigen: jeweils eine um die technischen Voraussetzungen für Gegenangriffe dieser Art zu prüfen, und eine, um die Frage zu klären, welche juristischen Grundlagen hierfür notwendig sind.

Noch im Sommer soll der geheim tagende Bundessicherheitsrat über die Ergebnisse der Analysen und daraus folgende Maßnahmen beraten. Offensive Reaktionen auf Hackerangriffe, Experten sprechen von "Hack Back", sind seit langem in der Diskussion. Ihr Ziel ist es, im Falle eines Angriffs die Infrastruktur lahm zu legen oder gar zu zerstören, derer sich die Angreifer bedienen. In Regierungskreisen wird in diesem Zusammenhang von einem "digitalen finalen Rettungsschuss" gesprochen.

Als Beispielszenarien werden Angriffe auf das Stromnetz der Bundesrepublik angeführt oder auch ein erneuter Einbruch in das Bundestagsnetz. Im Falle einer solchen Situation, und falls sich der Angriff aus dem Ausland nicht anders stoppen lässt, sollen Hacker im Auftrag der Bundesregierung die Server der Angreifer mit Hilfe von Schadsoftware vom Netz nehmen und auch eventuell gestohlene Daten löschen dürfen. Wer genau diese "Hack Back"-Angriffe durchführen soll, darüber herrscht noch Unklarheit.



Video: Recherche zu Cybersicherheit
tagesschau 17:00 Uhr, 19.04.2017, Svea Eckert/Jan Strozyk, NDR

Mehr zum Thema

Experten entdecken Sicherheitslücken im Bundestagsnetz, 12.04.2017
Bundeswehr: Kaum Krieger für die virtuelle Front, 05.04.2017
Nach Angriff auf Telekom: Mutmaßlicher Hacker gefasst, 23.02.2017

Rechtliche Fragen noch offen

Bislang sind staatliche Angriffe auf Computersysteme im Ausland rechtlich nicht geklärt. Die Bundeswehr stellte Anfang April dieses Jahres das "Kommando Cyber- und Informationsraum" vor. Allerdings dürfen die dort stationierten Soldaten nur im Verteidigungsfalle oder im Zuge eines durch den Bundestag mandatierten Einsatzes, wie etwa in Afghanistan, eingreifen.

Andere Gegenangriffe auf IT-Systeme im Ausland müssten derzeit wohl vom Bundestag beschlossen werden, wie andere Bundeswehreinsätze auch. Denkbar wäre auch, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) bei den Gegenangriffen eine Rolle spielt. Dort ist das Cyber-Abwehrzentrum des Bundes angesiedelt. Da es um Angriffe aus dem Ausland geht, käme auch der Bundesnachrichtendienst infrage, auch das Bundeskriminalamt und der Verfassungsschutz werden als zuständige Behörden gehandelt.

Experte plädiert für geteilte Zuständigkeit

Um die Kompetenz- und Regelungslücken zu schließen, sollen nun entsprechende gesetzliche Vorschläge erarbeitet werden. Der IT-Sicherheitsexperte Martin Schallbruch von der European School of Management and Technology plädiert im NDR-Gespräch für eine geteilte Zuständigkeit. Viele der Angriffe werden voraussichtlich "außerhalb eines klaren Verteidigungsfalles stattfinden", sagte Schallbruch. Daher seien diese Attacken Sache der Innenbehörden.

Auf der anderen Seite habe die Bundeswehr natürlich einen Verteidigungsauftrag und baue bereits entsprechende Fähigkeiten auf. "Rechtlich sollten die Polizeibehörden diese Befugnis haben, aber die technische Ausführung könnte durch die Bundeswehr erfolgen", so Schallbruch weiter. Gegenangriffe wie ein "Hack Back" sind nicht nur wegen Fragen der Zuständigkeit unter Experten umstritten. In vielen Fällen leiten Angreifer ihren Datenverkehr bewusst über mehrere Server um, Spuren zu verwischen. Das erschwert die Zuordnung der Hacks und auch die Suche nach dem eigentlichen Ausgangspunkt.

Zudem besteht das Risiko, dass versierte Angreifer sich bewusst auf Servern einnisten, die besonders sensible Daten verarbeiten - beispielsweise in Krankenhäusern. Bei einem Gegenschlag könnte dann nicht nur der Hacker getroffen werden, sondern auch kritische Infrastruktur ausfallen. Der Whistleblower Edward Snowden machte etwa 2014 öffentlich, dass der US-Geheimdienst National Security Agency (NSA) vor einigen Jahren bei einem offensiven Hacker-Gegenangriff versehentlich ganz Syrien vom Internet abschnitt.

Über dieses Thema berichtete die tagesschau am 19. April 2017 um 17:00 Uhr.

Sicherheitslücken im Bundestagsnetz, 11.04.2017
Bundeswehr: Kaum Krieger für die virtuelle Front, 04.04.2017
Recherche zu Cybersicherheit, S. Eckert/J. Strozyk, NDR | video
Weltatlas | Deutschland