Kleine Anfrage zur schriftlichen Beantwortung
mit Antwort der Landesregierung
- Drucksache 17/8259 -

„Regierung will den Hack back“ - Ein geeignetes Instrument zur Stärkung der IT-Sicherheit?

Anfrage des Abgeordneten Maximilian Schmidt (SPD) an die Landesregierung,
eingegangen am 06.06.2017, an die Staatskanzlei übersandt am 12.06.2017

Antwort des Ministeriums für Inneres und Sport namens der Landesregierung vom 05.07.2017,
gezeichnet

Boris Pistorius

Vorbemerkung des Abgeordneten

Medienberichten zufolge prüft die Bundesregierung zurzeit, ob und wie offensive Reaktionen auf Hackerangriffe - „Hack back“ - erfolgen können und welche Voraussetzungen hierfür zu schaffen wären. So berichtete u. a. Tagesschau online am 19.04.2017: „Die Bundesregierung will eine Grundlage schaffen, um bei Angriffen im Internet aktiv zurückschlagen zu können. (...) 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 lahmzulegen oder gar zu zerstören, derer sich die Angreifer bedienen. In Regierungskreisen wird in diesem Zusammenhang von einem ‚digitalen finalen Rettungsschuss‘ gesprochen. (...)“

Geprüft werde dabei der Einsatz der Bundeswehr, die im Verteidigungsfall aktiv werden solle. Außerhalb des Verteidigungsfalls - und dies wäre laut Experten bei derartigen Attacken der Regelfall - sollen die Polizeibehörden zuständig sein. Daraus ergibt sich eine Vielzahl von technischen und materiellen, vor allem aber rechtlichen und vor allem kompetenziellen Fragestellungen. Zudem wären besondere Güterabwägungen zu treffen, so u. a. die Frage, welche Gefahren bei einem „digitalen Gegenschlag“ für unbeteiligte Dritte aufkommen könnten.

Vorbemerkung der Landesregierung

Um die Schutzziele der Informationssicherheit - Vertraulichkeit, Integrität und Verfügbarkeit aller Informationen - erfolgreich gewährleisten zu können, ist eine ganzheitliche Sichtweise aller Bedrohungen und Gefahren der Informationssicherheit erforderlich. Als Resultat dieser ganzheitlichen Betrachtung kommt ein Portfolio von Maßnahmen zur Erhöhung der Informationssicherheit zum Einsatz. Wesentlich ist dabei, die Handlungsfähigkeit der eigenen Organisation im Falle eines eingetreten Sicherheitsvorfalls aufrecht zu erhalten. Technische Maßnahmen müssen - im Sinne der ganzheitlichen Sichtweise - durch organisatorische Regeln sowie durch eine intensive Sensibilisierung für die Gefahren aus dem Cyberraum ergänzt werden. In der IT-Strategie „Digitale Verwaltung 2025“ der Landesregierung ist ein solches Zusammenspiel von Maßnahmen dargelegt. Ein „Hack Back“ könnte darüber hinausgehend eine weitere mögliche Maßnahme darstellen.

Unabdingbar ist im technischen Bereich ein ausgereifter Perimeter-Schutz. Angesichts der zunehmenden Häufigkeit und Qualität der Cyber-Attacken werden die technischen Maßnahmen zum Schutz des Datennetzes und der IT-Systeme fortlaufend anzupassen sein. Durch Einsatz einer dafür geeigneten Sensorik können Angriffe von außen oder auch von innen auf die IT-Infrastruktur ebenso erkannt werden wie der unkontrollierte Abfluss von Informationen.

Um den immer ausgereifteren Hackerangriffen auch zukünftig erfolgreich begegnen zu können, plant die Landesregierung den Entwurf eines Niedersächsischen IT-Sicherheits-Gesetzes in den Landtag einzubringen. Damit wird beabsichtigt, die IT-Sicherheit des Landesdatennetzes zu verbessern, in dem auch beispielsweise moderne Intrusion Detection Systeme (IDS) oder Security Information und Event Management (SIEM)-Systeme betrieben werden können. Der Gesetzesentwurf befindet sich aktuell in der Verbandsanhörung.

Die rasante Entwicklung von Technologien, vor allem der Angriffsmöglichkeiten aus dem Internet, erfordert jedoch immer schnellere Reaktionen, nicht nur technischer Art. Gefordert sind ebenso Regelwerke, die als organisatorischer Schutz greifen können. Beispielsweise stellen die internationale Norm ISO/IEC 27001 oder das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene Grundschutzmodell anerkannte Vorgehensweisen für die Etablierung eines Informationssicherheitsmanagementsystem (ISMS) dar. Dieser Begriff bezeichnet die Aufstellung von Verfahren und Regeln, welche dazu dienen, die Informationssicherheit dauerhaft zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Auch in der niedersächsischen Landesverwaltung wurde durch die Landesregierung mit der Leitlinie zur Gewährleistung der Informationssicherheit bereits 2011 die Grundlage für ein ISMS gelegt, zuletzt durch ihre Fortschreibung im Dezember 2016.

Ungeachtet der immer zahlreicher werdenden Attacken aus dem Cyberraum stellt unbedachtes Handeln von Anwenderinnen und Anwendern einen großen Risikofaktor für die Informationssicherheit dar. Die Beschäftigten fortlaufend hierfür zu qualifizieren und zu sensibilisieren, ist daher nicht nur Aufgabe der Sicherheitsspezialisten, sondern eine, die auch als zentrale Führungsaufgabe aller Managementebenen erkannt und wahrgenommen werden muss. Mit Blick auf die niedersächsische Landesverwaltung hat der Niedersächsische IT-Planungsrat in seiner 21. Sitzung vom 04.03.2015 die Ressorts aufgefordert, in den Behörden ihres Geschäftsbereichs Sensibilisierungsmaßnahmen zur Verbesserung der Informationssicherheit in der Landesverwaltung auf regelmäßiger Basis durchzuführen. Vorlagen dazu wurden im Niedersächsischen Ministerium für Inneres und Sport erarbeitet und allen Ressorts zur Verfügung gestellt.

Ein Computer Emergency Response Team (CERT) fungiert als eine zentrale Drehscheibe für die Aufnahme, Bewertung und Weitergabe von IT-Sicherheitswarnmeldungen, die entweder aus eigener Erkenntnis oder aufgrund von Erkenntnissen kollaborierender Einrichtungen gewonnen werden. Durch diesen Informationsvorsprung erhalten die Organisationen in der Regel einen Zeitvorteil, um die Sensoren der Sicherheitssysteme auf neue Bedrohungen auszurichten oder IT-Systeme oder -Anwendungen bei Bedrohung vom Netz zu nehmen. Für die Niedersächsische Landesverwaltung betreibt das Niedersächsische Ministerium für Inneres und Sport ein solches CERT.

Als Werkzeuge für Cyberangriffe werden u. a. IT-Infrastrukturen von Dritten durch Täter gekapert, um beispielsweise großflächig verteilte „Distributed Denial of Service“ (DDoS) Attacken durchzuführen. Bei einem sogenannte Hack Back würde regelmäßig auch die Infrastruktur dieser Dritten nachhaltig gestört werden, sodass die jeweilig ursprüngliche Aufgabe dieser Systeme (wie Industriesteuerung, Webshop, Geräte des Internets der Dinge etc.) nicht mehr ausgeführt werden kann und somit ein weiterer Schaden einträte. Dies macht deutlich, dass ein „Hack back“, wenn überhaupt, nur in speziellen, genau zu prüfenden Einzelfallkonstellationen ein geeignetes Mittel darstellen könnte, um gegebenenfalls einen entsprechenden Angriff zu beenden. Dabei ist stets zu berücksichtigen, dass in vielen Fällen nicht nur die Infrastruktur der Täter angegriffen würde, sondern ebenso diejenige von unbeteiligten Dritten und mögliche Auswirkungen der getroffenen Maßnahmen im Voraus nicht abschließend einzuschätzen sind.

1. Wie bewertet die Landesregierung das Instrument des „Hack back“ als Reaktion auf Hackerattacken mit Blick auf Eignung, Angemessenheit und Wirksamkeit?

Dem Geschäftsbereich der Polizei obliegt insbesondere die Aufgabe der polizeilichen Gefahrenabwehr und der Strafverfolgung. Für den Bereich der Strafverfolgung sind Fallkonstellationen vor dem Hintergrund der Fragestellung denkbar, in denen sich Täter hinter sogenannten Anonymisierungsdiensten verstecken und z. B. eine Firma mittels DDoS-Attacken erpressen. In diesen Fallkonstellationen steht ein eventuell stattgefundener „Hack“ nicht im deliktischen Vordergrund, sondern die

Erpressungstat. Für diese Fälle kann es geeignet sein, die eingesetzte Infrastruktur der Täter polizeilicherseits zu erforschen, um Täter identifizieren zu können. Ein solches Vorgehen bedingt allerdings eine längere Vorbereitungszeit und entsprechende Planungen innerhalb der Polizei. Anhand dieser Fallkonstellation wird deutlich, dass der Begriff „Hack“ nicht für spezifische technische oder fachliche Anforderungen steht, sondern vielmehr bedeutet, dass man vorhandene Sicherheitseinrichtungen auf einem alternativen Weg umgeht.

Daneben kommen zahlreiche weitere Fallbeispiele in Betracht. So beispielsweise eine täterseitig betriebene Internetplattform, die für den Handel illegaler Substanzen genutzt wird. Solche Plattformen sind vielfach durch technische Maßnahmen gegen den physikalischen Zugriff von Strafverfolgungsbehörden geschützt. Aus Sicht der Strafverfolgungsbehörden erscheint es zur Strafverfolgung denkbar, den Server auf eventuell vorhandene Sicherheitslücken zu überprüfen und diese gegebenenfalls zu nutzen, um verdeckt Zugriff auf die Plattform zu erlangen.

Für den Aufgabenbereich der polizeilichen Gefahrenabwehr könnte die Abwehr eines gegenwärtigen und gegebenenfalls andauernden Angriffs z. B. für die bereits vorgenannte DDoS-Attacke in Betracht kommen.

2. Welche rechtlichen Fragen ergeben sich bei der Durchführung eines „Hack back“ insbesondere in Bezug auf die Kompetenzverteilung zwischen Bund und Ländern?

Für eine rechtliche Bewertung sind zunächst die Entwicklungen auf Bundesebene bzw. in den zuständigen Gremien abzuwarten. Auf Basis der bestehenden Erkenntnisse sowie vor dem Hintergrund einer ganzen Vielzahl von offenen und komplexen Fragestellungen ist eine abschließende rechtliche Bewertung zurzeit nicht möglich.

3. Verfügt die Landesregierung über die notwendige technische Infrastruktur sowie personelle Ausstattung zur Anwendung derartiger Verfahren?

Wie bereits in der Beantwortung zu Frage 1 dargestellt, stellt ein sogenannte Hack Back vielschichtige Anforderungen an technische Infrastrukturen etc. Es wären u. a. verschiedene Hardware- und Betriebssystemanforderungen in geeigneter Form so auszugestalten, dass eine entsprechende Maßnahme unter Umständen durchführbar sein könnte. Dem Grunde nach stehen dem Landeskriminalamt Niedersachsen personelle Ressourcen zur Verfügung, um eine solche Maßnahme durchführen zu können.

4. Welche Alternativen kommen zur weiteren Stärkung der IT-Sicherheit in Betracht?

Siehe Vorbemerkung.

5. Wie positioniert sich die Landesregierung auf Bundesebene mit Bezug auf die o. a. Debatte?

Siehe Beantwortung der Frage 2. Darüber hinaus wird auf die Antwort auf die Kleine Anfrage zur mündlichen Beantwortung „Cybergefahrenabwehr“ von Abgeordneten der FDP in der Drucksache 17/8120 Nr. 4 verwiesen.

(Ausgegeben am 06.07.2017)