Überwachung

Aktive Cyber-Abwehr: Innenminister schaltet bei IT-Sicherheit schrittweise von Verteidigung auf Angriff

Trojaner, Hacking, Denial-of-Service: Was Kriminelle für Angriffe nutzen, soll bald auch der Staat dürfen. Innenminister Seehofer schafft staatliche Befugnisse zur „aktiven Cyber-Abwehr“ – dem digitalen Gegenangriff. Der letzte Baustein soll noch dieses Jahr kommen.

24.04.2019 um 16:02 Uhr - Gastbeitrag, Sven Herpig - keine Ergänzungen

Ist Angriff die bessere Verteidigung?— CC-BY-NC-ND 2.0 Militärakademie West Point

Die Stiftung Neue Verantwortung ist eine gemeinnützige Denkfabrik in Berlin. Dr. Sven Herpig leitet dort den Bereich Internationale Cyber-Sicherheitspolitik. Er ist erreichbar per E-Mail (OpenPGP) und Twitter.

Das Bundesinnenministerium produziert derzeit Gesetze am laufenden Band. Ende März veröffentlichte netzpolitik.org den Gesetzentwurf zur Harmonisierung des Verfassungsschutzrechts, Anfang April folgte der Gesetzentwurf für das IT-Sicherheitsgesetz 2.0.

Beide Entwürfe stammen aus dem Ministerium von Horst Seehofer und sollen die Befugnisse der Sicherheitsbehörden massiv ausweiten. Noch etwas haben sie gemeinsam: Beide Gesetze treiben das Thema „Aktive Cyber-Abwehr“ voran.

Was ist Aktive Cyber-Abwehr?

Seit ungefähr zwei Jahren gibt es in Sicherheitskreisen ein „Stufenmodell“ für Aktive Cyber-Abwehr. Diese vereinfachte Übersicht stellt die digitalen Möglichkeiten dar, auf Cyberangriffe zu reagieren – sortiert nach Intensität.

Bei Stufe 1 handelt es sich um Unterstützung, um Angriffe zu vereiteln. In Stufe 2 sollen konkrete Bedrohungen erkannt werden, beispielsweise mit Honeypots, die Angreifer in eine Falle locken. Fließen Daten ab, können diese in Stufe 3 nachverfolgt werden.

In Stufe 4 wäre es möglich, Geräte von Angreifern zu hacken und Daten auf diesen Geräten zu verändern. Die größtmögliche Eskalation würde in Stufe 5 erfolgen – etwa ein koordinierter Denial-of-Service-Gegenangriff, um IT-Infrastruktur des Angreifers auszuschalten.

Für einige der Maßnahmen auf den unteren Stufen gibt es bereits entsprechende Befugnisse. Mit dem ersten IT-Sicherheitsgesetz, das 2015 verabschiedet wurde, wurden Internet-Zugangsanbieter verpflichtet, ihren Kunden eine Information anzuzeigen, wenn deren

Rechner mit Schadsoftware infiziert sind. Seit der Umsetzung von EU-Vorgaben können Zugangsanbieter Geräten den Internetzugang verwehren, die zum Beispiel mit Schadsoftware infiziert sind.

Zurückcybern auf fünf Stufen

Obwohl in einer öffentlichen Bundestagsanhörung auch über das Stufenmodell gesprochen wurde, ist es bisher nicht öffentlich. Das Bundeskriminalamt hat es entwickelt, aber mit der Geheimhaltungsstufe „Nur für den Dienstgebrauch“ versehen.

Es ist nicht öffentlich bekannt, ob dieses Modell noch die aktuelle Referenz des Innenministeriums ist oder ob es mittlerweile aktualisiert wurde.

Um etwas mehr Licht ins Dunkel zu bekommen und eine nuanciertere Debatte voranzutreiben, hat die Stiftung Neue Verantwortung ein eigenes Modell zur Erklärung Aktiver Cyber-Abwehrmaßnahmen entwickelt.

Laut dieser Definition ist Aktive Cyber-Abwehr „eine aktive Gegenmaßnahme unterhalb der Schwelle des bewaffneten Konflikts, die dazu ausgelegt ist, einen Cyber-Angriff abzuwehren und/oder aufzuklären“. Diese Definition ähnelt nach aktuellem Kenntnisstand offenbar der des Innenministeriums.

Aktive Cyber-Abwehr im IT-Sicherheitsgesetz 2.0

Mit dem neuen IT-Sicherheitsgesetz will das Innenministerium gleich eine Reihe an Befugnissen für aktive Cyber-Abwehr einführen. Das Bundesamt für Sicherheit in der IT soll mit Sinkhole-Servern den Verkehr von Botnetzen umleiten und mit aktiven Honeypots Angriffstechniken besser studieren. Beide Maßnahmen lassen sich auf Stufe 2 des Modells einordnen.

Das gilt auch für ein weiteres Vorhaben im Gesetzentwurf: Das BSI soll Internet-Anbietern anordnen dürfen, ihre Dienste bei Störungen einzuschränken, umzuleiten oder zu unterbinden. Wenn zum Beispiel ein System durch einen Denial-of-Service-Angriff lahmgelegt wird, könnte die Behörde Internet-Anbietern anordnen, diesen schädlichen Datenverkehr umzuleiten oder zu unterbinden.

Geht es nach dem Willen des Innenministeriums, kann das BSI Diensteanbieter auch verpflichten, infizierte IT-Systeme zu bereinigen. Dabei würde dann beispielsweise Schadsoftware von einem Gerät entfernt. Je nachdem, wie das technisch umgesetzt wird, entspricht das Stufe 1 (Unterstützung) oder Stufe 4 (Löschen/Verändern von Daten).

Der Gesetzentwurf sieht auch neue Regelungen vor, wenn in den Netzen von Telekommunikationsanbietern Daten rechtswidrig weitergegeben oder veröffentlicht werden. Wenn Netzbetreiber davon Kenntnis erlangen, müssen sie unverzüglich das BKA informieren, den Zugang zu den Daten sperren und diese gegebenenfalls löschen, was Stufe 3 oder 4 entsprechen kann. Diese Maßnahmen können auch von zuständigen Stellen wie dem BKA angeordnet werden.

Aktive Cyber-Abwehr im Verfassungsschutzgesetz

Schwerer wiegen die auch neuen Befugnisse für In- und Auslandsgeheimdienst im neuen Verfassungsschutzgesetz. Damit soll das Bundesamt für Verfassungsschutz die Befugnis bekommen, in IT-Systeme einzugreifen, um dort Daten zu erheben – den Staatstrojaner. Das beinhaltet das Eindringen in Systeme, um Urheber digitaler Angriffe zuzuordnen: Stufe 3.

Das soll analog auch für den BND gelten. Der Auslandsgeheimdienst soll diese Befugnisse aber nicht nur für das Ausland bekommen, sondern auch für das Inland.

Mehr Befugnisse ohne mehr Schutz und Kontrolle

Man kann darüber diskutieren, welche dieser Maßnahmen für mehr IT-Sicherheit sorgen und welche nicht. Vor allem der Entwurf zum IT-Sicherheitsgesetz enthält auch sinnvolle und begrüßenswerte Neuerungen. Das Gesetz bringt zusätzliche Pflichten für Betreiber von Kritischen Infrastrukturen wie Energieversorger, aber auch für Hersteller von Kernkomponenten der IT-Systeme solcher Betreiber.

Wichtiger wäre jedoch, erst einmal herauszufinden, ob die Abwehrmaßnahmen überhaupt benötigt werden. Es ist unklar, ob es hierfür jemals eine Bedarfsanalyse gegeben hat. Es ist davon auszugehen, dass das IT-Sicherheitsgesetz 2.0 formuliert wurde, ohne die Wirksamkeit des bisher geltenden IT-Sicherheitsgesetzes zu prüfen.

Das ist besonders deshalb brisant, da eine solche Evaluierung explizit im entsprechenden Gesetzestext verankert ist. Diesen Mangel an Evaluierung und empirischer Evidenz kennen wir leider bereits von der Cyber-Sicherheitsstrategie 2016.

Aber auch der Koalitionsvertrag wird hier anscheinend wieder einmal ignoriert. Union und SPD hatten beschlossen, dass bei der Ausweitung der Befugnisse von Sicherheitsbehörden eine „gleichzeitige und entsprechende Ausweitung der parlamentarischen Kontrolle“ stattfinden muss.

Auch zusätzliche Schutzmaßnahmen beim Eingriff in IT-Systeme, wie die Stiftung Neue Verantwortung und andere sie letztes Jahr vorgeschlagen haben, finden sich in den Gesetzen nicht wieder.

Die letzte Stufe ist noch nicht erreicht

Es gibt Anzeichen, dass die Bundesregierung diese Kompetenz- und Befugniserweiterungen gar nicht als Aktive Cyber-Abwehr verstanden wissen möchte. Die in den Gesetzentwürfen vorgeschlagenen

Maßnahmen bewegen sich im Stufenmodell für Aktive Cyber-Abwehr zwischen 1 und 4, aber noch nicht auf Stufe 5.

Diese Befugnisse für stark invasive Maßnahmen wie das Übernehmen von Angreifer-Systemen oder ein DDoS-Gegenangriff werden sich in einem weiteren Gesetzespaket finden, an dem das Innenministerium derzeit arbeitet. Ein Sprecher des Innenministeriums bestätigte gegenüber netzpolitik.org: „Es wird einen Referentenentwurf geben."

…. ……. …. ……. …. ……. …. …. ……. …. ……. …. …. …

Über den Autor/ die Autorin

Gastbeitrag

Gastbeiträge sind Beiträge von Personen, die nicht zur netzpolitik.org-Redaktion gehören. Manchmal treten wir an Autor:innen und Verlage heran, um sie nach Gastbeiträgen zu fragen, manchmal treten die Autor:innen an uns heran. Gastbeiträge geben nicht unbedingt die Meinung der Redaktion wieder.

…. ……. …. ……. …. ……. …. …. ……. …. ……. …. …. …

Veröffentlicht

24.04.2019 um 16:02

Kategorie

Überwachung

Schlagworte

Aktive Cyber-Abwehr, BfV, BMI, BND, BSI, cyber-abwehr, IT-Sicherheitsgesetz 2.0, ITSG2, Verfassungsschutzgesetz

0 Ergänzungen