Entwurf für ein neues Bundespolizeigesetz

Reaktionen auf die Hackback-Pläne des Innenministeriums (Update)

„Eine Gefahr für die öffentliche Sicherheit“, „Militarisierung des Cyberraums“, „erhebliche verfassungsrechtliche Bedenken“, „Gegenreaktionen sind zu erwarten“: So lauten die ersten Reaktionen auf frühere Pläne des Innenministeriums, der Bundespolizei das Zurückhacken zu erlauben. Die Pläne sind mittlerweile offenbar vom Tisch.

29.01.2020 um 12:49 Uhr - Anna Biselli - in Technologie - 2 Ergänzungen

Wie ein Bumerang könnten die digitalen Gegenangriffe wieder zurückkommen.
— CC-BY 2.0 chaf.haddad

Update 16:12 Uhr: Ein Sprecher des Bundesinnenministeriums teilte uns inzwischen mit, dass der hier diskutierte Paragraf nicht mehr im Gesetzentwurf sei: „In dem aktuell im Ressortverfahren befindlichen Gesetzesvorschlag ist eine solche Regelung nicht enthalten.“ Unsere Fassung ist offenbar eine frühere. Wann genau oder aus welchen Gründen der Paragraph entfernt wurde, dazu will das Ministerium nicht Stellung nehmen. Damit könnte das gleiche passiert sein, wie bei der automatisierten Gesichtserkennung: Sie ruht. Dass die lange bestehenden Pläne damit vom Tisch sind, ist vermutlich nicht zu erwarten. Wir haben die Zeitform zur Klarstellung im Teaser angepasst.

Laut einem Gesetzesvorschlag aus Horst Seehofers Innenministerium, den wir heute veröffentlicht haben, soll die Bundespolizei bei Angriffen auf IT-Systeme bald zurückhacken dürfen. Solche sogenannten Hackbacks sind stark umstritten. Wir tragen hier einige Reaktionen zusammen und aktualisieren den Artikel, sobald neue eintreffen.

Konstantin von Notz, stellvertretender Fraktionsvorsitzender der Grünen im Bundestag:

> Mehr und mehr bewahrheitet sich, was in den vergangenen Tagen bereits kaum zu übersehen war: Nach den öffentlichen Verlautbarungen Horst Seehofers, seines Sprechers und Vertretern der CDU/CSU-Fraktion im Deutschen Bundestag war offensichtlich, dass man nicht etwa aus grundsätzlichen Überlegungen auf die tief in die Grundrechte der Menschen eingreifende Technik verzichtet, sondern es sich vielmehr um ein sehr durchsichtiges Ablenkungsmanöver des Ministers handelt.
>
> So steht nicht nur zu befürchten, dass im Zuge des weiteren parlamentarischen Verfahrens erneut einen entsprechenden Passus durch die konservative Fraktion im Deutschen Bundestag in das Bundespolizeigesetz aufgenommen werden soll. Zudem gibt es gute Gründe anzunehmen, dass das Innenministerium mit diesem Manöver von weiteren, verfassungsrechtlich höchst fragwürdigen Vorhaben im Gesetz ablenken will. Hierzu gehört neben der Quellen-TKÜ und der Online-Durchsuchung vor allem die offenbar ebenfalls im Gesetzesentwurf versteckte gesetzliche Legalisierung des „Hackbacks“, also digitaler Gegenschläge.
>
> Auch hier bestehen seit langem ganz erhebliche verfassungsrechtliche Bedenken, die die Bundesregierung bis heute negiert. Was für die Gesichtserkennung gilt, gilt für den Hackback genauso: Auch den Passus zu diesem hochumstrittenen Instrument müssen Bundesregierung und die Fraktionen von CDU/CSU und SPD zwingend aus dem bisherigen Entwurf streichen und insgesamt von der Ermöglichung digitaler Gegenschläge Abstand nehmen.

Martina Renner, stellvertretende Parteivorsitzende der Linken und Mitglied im Innenausschuss des Bundestages:

> Die Pläne von Horst Seehofer zeigen vor allem, dass hier eine zweifelhafte Idee um jeden Preis durchgesetzt werden soll, ohne sich Gedanken über die Umsetzbarkeit und mögliche Folgen zu machen. Wenn am Ende bei einem Hackback die IT-Systeme eines Krankenhauses, die unerkannt infiziert und für einen Hackerangriff missbraucht wurden, durch die Bundespolizei atomisiert

> werden und Patienten sterben, werden die Verantwortlichen Betroffenheit und Unschuld heucheln. Es gibt nur einen verantwortlichen Umgang mit diesen Bedrohungen: Sichere IT-Systeme ohne Backdoors und kein Handel mit Sicherheitslücken!

Armin Schuster (CDU), Obmann im Innenausschuss des Bundestages, lässt mitteilen, dass er der Anfrage nach einem Statement nicht entsprechen kann.

Matthias Schulze, Experte für die internationalen Aspekte von Cyber-Sicherheit. Er forscht über Cyber-Konfliktdynamiken:

> Es ist bedenklich, dass der Entwurf aktuelle, internationale Cyber-Konfliktdynamiken und den strategischen Kontext komplett ignoriert. Bei Hackbacks gegen Akteure wie Iran, Russland oder Nordkorea, die hinter zahlreichen Angriffe auf deutsche, kritische Infrastrukturen zu vermuten sind, ist von denen eine erneute Gegenreaktion zu erwarten. Weniger digitalisierte Staaten haben bei solchen Hack-Back-Eskalationen weniger zu verlieren, aber mehr zu gewinnen als Länder wie Deutschland.
>
> Es ist unwahrscheinlich, dass das Abschalten eines Angriffsservers die strategische Motivation von Cyber-Mächten, die Deutschland im Visier haben, ändern wird. Wahrscheinlicher ist, dass die einfach über ein anderes, weit offenes Tor wiederkommen werden.

Sven Herpig, Leiter für internationale Cyber-Sicherheitspolitik bei der Stiftung Neue Verantwortung:

> Warum mit der Bundespolizei jetzt noch eine weitere Behörde operativer in der deutschen Cybersicherheitspolitik werden soll ist vollkommen unklar. Vor allem, da die Bundesregierung es offensichtlich immernoch nicht geschafft hat die zentralen Plattform wie das Cyber-Abwehrzentrum
> nachhaltig zu reformieren. Das wird auch daran deutlich, dass die Bundespolizei Budget für den Kauf von Schwachstellen und Angriffswerkzeugen bekommen soll. Etwas das eigentlich durch die Zentrale Stelle für Informationstechnik im Sicherheitsbereich als zentraler Dienstleister gewährleistet werden sollte.
>
> Man versucht hier aus politischen Gründen auf Biegen und Brechen die Aktive Cyberwehr unterzubringen, ohne sich über die bestehende Cybersicherheitsarchitektur Gedanken gemacht zu haben.

Thomas Reinhold ist wissenschaftlicher Mitarbeiter am Lehrstuhl „Wissenschaft und Technik für Frieden und Sicherheit“ (PEASEC) der TU Darmstadt. Er beschäftigt sich seit langem mit den Risiken der Militarisierung sowie Möglichkeiten zur Rüstungskontrolle im Cyberspace:

> Hack-Backs sind als technische Maßnahme zur Abwehr von Cyberbedrohungen kaum sinnvoll, da diese mit redundanten Angriffs-Strukturen leicht umgangen werden können. Dazu kommt ein hohes Risiko- und Eskalationspotential, weil kaum zweifelsfrei geklärt werden kann, ob das Ursprungs-System des Angriffs nicht selbst vom Angreifer fremdgesteuert und missbraucht wurde und ein Gegenschlag damit unter Umständen fremde, zivile Infrastrukturen schädigen würde. Insgesamt tragen Hack-Backs weiter zu einer Militarisierung des Cyberspace bei, indem Cyber-Angriffswerkzeuge und Kompetenzen etabliert und über kurz oder lang auch eingesetzt werden.

Manuel Atug von der AG Kritis:

> Hackbacks gefährden unsere öffentliche Sicherheit, denn Täter nutzen für ihre Angriffe in der Regel IT-Systeme von Dritten, wie z.B. den Active-Directory-Server des Kernkraftwerks Kudankulam im Oktober 2019. Ein Hackback hätte hier nicht die Täter getroffen, sondern die IT-Umgebung des Kernkraftwerks lahm gelegt.
>
> Nach dem Stand der Technik ist es nach wie vor ausgeschlossen, einen Cyberangriff zweifelsfrei zu attributieren. Die Hackback-Pläne des Innenministers schaden durch die notwendige Geheimhaltung der Sicherheitslücken daher direkt der IT-Sicherheit aller Bürger, aber gefährden auch über alle Maßen unsere Kritischen Infrastrukturen.

Ann Cathrin Riedel, Vorsitzende des LOAD e.V., eines Vereins für liberale Netzpolitik:

> Petya, NotPetya und Wannacry zeigen, was passiert, wenn staatliche Akteure Sicherheitslücken zurückhalten: Schäden in Milliardenhöhe und die massive Gefährdung von Menschenleben. Diese Schadprogramme konnten einen so enormen Schaden anrichten, da die NSA erfolglos versucht, hat die Sicherheitslücken zurückzuhalten. Wenn schon die NSA nicht in der Lage ist, Sicherheitslücken zurückzuhalten, wie sollte die Bundespolizei dies schaffen?
>
> Haftet die Bundespolizei dann für verursachte Schäden in Milliardenhöhe? Horst Seehofer soll sich auf eine umfassende defensive Cyberabwehrstrategie

> konzentrieren und keine Fantastereien über Hackback anstellen! LOAD verurteilt den Einsatz und die Bereitstellung jeglicher offensiver Wirkmittel im Cyberraum.

Du möchtest mehr kritische Berichterstattung?

Unsere Arbeit bei netzpolitik.org wird fast ausschließlich durch freiwillige Spenden unserer Leserinnen und Leser finanziert. Das ermöglicht uns mit einer Redaktion von derzeit 15 Menschen viele wichtige Themen und Debatten einer digitalen Gesellschaft journalistisch zu bearbeiten. Mit Deiner Unterstützung können wir noch mehr aufklären, viel öfter investigativ recherchieren, mehr Hintergründe liefern - und noch stärker digitale Grundrechte verteidigen!

Unterstütze auch Du unsere Arbeit jetzt mit deiner **Spende.**

Über den Autor/ die Autorin

anna

Auf einem Zettel steht, dass sie eigentlich Informatikerin ist. Anna ist seit 2013 bei netzpolitik.org dabei. Sie interessiert sich vor allem für staatliche Überwachung und Dinge rund ums BAMF. Du erreichst sie unter anna@netzpolitik.org - am besten verschlüsselt [325C 6992 DCD3 1167 D9FA 9A57 1873 5033 A249 AE26]

Veröffentlicht
29.01.2020 um 12:49

Kategorie
Technologie

Schlagworte
ag kritis, Hackback, Horst Seehofer, Konstantin von Notz, Matthias Schulze, Stiftung neue Verantwortung, Sven Herpig

2 Ergänzungen

Tom sagt:
29. Januar 2020 um 13:20 Uhr

Es geht doch nicht um das Hackback. Das lässt sich faktisch, praktisch nicht betreiben und ist als Szenario genauso konstruiert wie die Absichten Kinderschänder oder Terroristen im Netz zu jagen. Um ein „Hackback“ betreiben zu wollen braucht man Kapazitäten, braucht man bereits kompromittierte Systeme und vor allem Exploits, die man sich lange vorher aufgebaut und gehortet hat. Man braucht vor allem Know-How was ich personall und finanziell nicht sehe wenn man nur die Budgets von NSA, GCHQ und den hiesigen Behörden vergleicht.

Die sogenannten Sicherheitsbehörden wollen einfach nur ungestört ohne so als lästig empfundene Dinge wie Grundrechte, Privatsphäre oder Rechtstaatlichkeit operieren. Das alles möglichst bequem vom eigenen Schreibtisch aus ohne aufstehen zu müssen oder sich gegenüber Dritten rechtfertigen zu müssen. Oder noch besser: Externalisiert und an private Anbieter outgesourced . Dann sieht man nicht ganz so blöde aus, wenn z.B. ein LKA anfängt öffentlich nach MAC Adressen zu suchen und behauptet, daß diese einzigartig seien (https://polizei.brandenburg.de/fahndung/f8-e0-79-af-57-eb-cyber-fahndung-nach-ma/1311939)

Zensierter Kommentator sagt:
30. Januar 2020 um 03:14 Uhr

Nur negative Reaktionen werden von euch im Artikel zitiert.. ihr degradiert euch selbst zur links-populistischen Seite...
