

IT-Sicherheitsgesetz - Debatte um Meldepflicht für IT-Sicherheitslücken

Von Peter Welchering

Bundesinnenminister Horst Seehofer hat beim Digital-Gipfel angekündigt, die Meldepflicht von Sicherheitslücken in IT-Systemen nun verstärkt einzufordern. Die versorgungstragende Infrastruktur Deutschlands soll dadurch gesichert werden. Doch über die Umsetzung wird in den Ministerien gestritten.

[Hören Sie unsere Beiträge in der Dlf Audiothek](#)



IT-Systeme und digitale Infrastrukturen Deutschlands sollen sicherer werden
(imago / Sergej Iaremenko)

Mehr zum Thema

[IT-Sicherheit](#) Wissenschaftler fordern eine offene Hardware-Entwicklung

[IT-Sicherheit](#) Das Internet der Dinge vor Cyber-Attacken schützen

[IT-Sicherheit](#) Quantencomputer bedrohen die Datenverschlüsselung

[Trojaner Petya](#) Verheerende Lücken bei der IT-Sicherheit

[IT-Sicherheit](#) „Wir Europäer könnten Standards setzen“

Horst Seehofer hat seine Spitzenbeamten im Bundesinnenministerium kalt erwischt. Seine Ansage in Sachen Meldepflicht für IT-Sicherheitslücken auf dem Digital-Gipfel der Bundesregierung vor einer Woche war deutlich.

„Sie kriegen jetzt jede Woche die Frage: Wo ist die Meldepflicht? Wenn man so eine Pflicht in ein Gesetz schreibt, dann muss es auch die Wirkung entfalten, die man sich davon verspricht. Aber ich frage jetzt jede Woche: Wo ist die Meldepflicht?“

Innenministerium genervt

Die Beamten des Bundesministeriums des Inneren zeigten sich ziemlich genervt über diese Ansage ihres Dienstherrn. Sie arbeiten schon seit einiger Zeit an einer Fortschreibung des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme. Im nächsten Frühjahr sollen die Gesetzesentwürfe im Deutschen Bundestag beraten werden. Und jetzt sollen da auch noch Prüfscenarien für eine Meldepflicht erarbeitet werden. Die regierungsnaher Stiftung Neue Verantwortung in Berlin hat da auch schon einen Vorschlag im petto, wie so eine Meldepflicht ausgestaltet sein könnte. Sven Herpig hat diesen Vorschlag maßgeblich erarbeitet und erläutert die Grundidee, wie künftig mit IT-Sicherheitslücken umgegangen werden soll, so:

„Der Vorschlag selber ist mehrfach gegliedert. Wir haben ein paar Prinzipien aufgeschrieben, unter anderem, dass alle bekannten Schwachstellen, die die Behörden kaufen, mieten oder anderweitig finden, einfließen müssen. Das heißt: Es gibt keine Behörde, wie der Bundesnachrichtendienst, die sich da rausziehen kann.“

Es geht um die Sicherheit der Bundesrepublik

Eine Forderung, die den Verfassungsschützern und dem Bundesnachrichtendienst natürlich überhaupt nicht genehm ist.

„Alle Behörden müssen ihre Schwachstellen da rein kippen. Und dann wird eben ein Gremium eingerichtet, wenn es nach uns geht unter der Ägide des Bundeskanzleramts. Denn es geht hier um nicht weniger als die Sicherheit der Bundesrepublik Deutschland. Da kann man das auch ruhig mal ganz oben aufhängen. Dann liegt die Verantwortung für so ein Prozess eben auch ganz oben.“

Ein neues Gremium direkt im Bundeskanzleramt soll sich also um das Schwachstellenmanagement kümmern.

„Im Gremium sind Vertreterinnen und Vertreter der Behörden, die sich mit diesen Themen beschäftigen. Das sind nicht nur die Sicherheitsbehörden, sondern natürlich auch das Auswärtige Amt, das Bundesministerium für Justiz und Verbraucherschutz oder ganz klar auch spezialisierte Behörden, zum Beispiel, wenn es um eine Schwachstelle in einem Herzschrittmacher geht, die mittlerweile auch sehr vernetzt sind. Dann natürlich auch das Bundesamt für Arzneimittel und Medizinprodukte, die dann entscheiden müssen, was passiert mit dieser Schwachstelle.“

„Geben wir sie an den Hersteller, damit er sie beheben kann? Oder wird sie kurzfristig zurückgehalten, damit die Sicherheitsbehörden sie ausnutzen können, um zu spionieren, um militärische Operationen durchzuführen oder um Strafverfolgung zu tätigen?“

Bis zu einem Jahr sollen die Nachrichtendienste nach dem Vorschlag der Stiftung Neue Verantwortung mit solchen IT-Sicherheitslücken arbeiten können, bevor sie geschlossen werden müssen. Sie müssen ...

" ... ab einem bestimmten Zeitpunkt an dem Hersteller gemeldet werden, damit diese geschlossen werden können.“

Ein Jahr - das erscheint Kritikern wie Professor Hartmut Pohl von der Gesellschaft für Informatik zu lang. Auch die parlamentarische Kontrolle des Gremiums für IT-Sicherheitslücken muss Pohl zufolge schärfer gefasst werden. Sven Herpig hält dagegen:

„Eine parlamentarische Kontrolle, am Abschluss jedes Jahres wird an ein Gremium, beispielsweise dem Parlamentarischen Kontrollausschuss, ein Report übermittelt, damit dieser nachvollziehen kann, ob dieser Prozess effizient und sinnvoll ist und für mehr Sicherheit oder mehr Unsicherheit in Deutschland sorgt.“

Missfallen beim BND und Verfassungsschutz

„Das dritte Kontrollinstrument ist ein Transparenzbericht, der sogar der Öffentlichkeit zugänglich gemacht wird. Der beinhaltet ein wenig weniger Details, Vorgaben als der Bericht ans Parlament. Damit auch unabhängige Expertinnen und Experten einen Einblick nehmen können, wie dieser Prozess abläuft.“

Die Diskussion darüber wie eine solche Meldepflicht für IT-Sicherheitslücken ausgestaltet werden könnte, ist also eröffnet. Im Bundesnachrichtendienst und beim Bundesamt für Verfassungsschutz wird das mit Missfallen gesehen. Denn einfach abstellen lässt sich eine solche Diskussion nicht mehr.