VERBAND DER INTERNETWIRTSCHAFT E.V.

Eckpunkte für Maßnahmen zur Verbesserung der Sicherheit in Netzwerken

Berlin, 25. April 2017

IT- und Netzwerksicherheit stehen im Fokus der Politik. Einige spektakuläre Angriffe haben die Debatte aufgeworfen, ob die rechtlichen Rahmenbedingungen für Netzbetreiber und IT-Anbieter ausreichen, um geeignete Maßnahmen gegen entsprechende Angriffe durchzuführen. Im Zuge der Debatte um das NIS-Richtlinien Umsetzungsgesetz kam dabei auch die Frage auf, inwieweit es gesetzlicher Klarstellungen im Telekommunikationsgesetz bedarf, um Betreiber von Telekommunikationsnetzen dazu zu ertüchtigen, zukünftig effektiv für mehr Sicherheit sorgen zu können. Im Rahmen eines Änderungsantrags der Koalitionsfraktionen CDU/CSU und SPD wurden nun auch mehrere Aspekte adressiert. Das Thema IT-Sicherheit wird mit der wachsenden Bedeutung vernetzter Systeme auch weiterhin hohe Priorität in der fachpolitischen Debatte haben. Die Umsetzung der NIS-Richtlinie auf europäischer Ebene ist noch nicht abgeschlossen. Und auch für Deutschland stellt sich dann die Frage nach Anpassungs- und Umsetzungsbedarf.

I. Zum Änderungsantrag der Regierungskoalition (BT-Drs. 18/11808)

Für mehrere derzeit diskutierte und technisch mögliche Maßnahmen zur Abwehr und Eingrenzung von Angriffen und zur Verbesserung der IT-Sicherheit möchte eco – Verband der Internetwirtschaft e.V. sich nachfolgend in die Beratungen in den Fachkreisen von Politik und Verwaltung einbringen und die derzeit diskutierten Vorschläge im Kontext des Änderungsantrages der Beschlussempfehlung des Innenausschusses des Deutschen Bundestages (BT-Drs. Nr. 18/11808) näher beleuchten.

Die im Rahmen des Änderungsantrags vorgeschlagenen und diskutierten Maßnahmen sorgen für eine gesetzgeberische Klarstellung und ermöglichen den Unternehmen verschiedene Handlungsoptionen, um auf potentielle Angriffsszenarien die die IT-Sicherheit gefährden im Einzelfall angemessen und flexibel reagieren zu können. Hierbei ist wichtig, dass Maßnahmen im Rahmen der vorgesehenen engen Grenzen des Telekommunikationsgesetzes und unter Berücksichtigung weiterer gesetzlicher Bestimmungen ergriffen werden können, die Entscheidung, ob und welche Maßnahmen Beseitigung ergriffen werden, letztlich aber bei den Unternehmen verbleibt. Entscheidend ist, dass der gesetzliche Rahmen ein schnelles, effektives und flexibles Handeln ermöglicht. Eine Verpflichtung zur Durchführung bestimmter Maßnahmen wäre demgegenüber nicht zielführend.

- **Analyse des Datenverkehrs (DPI)**

Um Datenverkehre genauer überprüfen zu können, benötigen Telekommunikationsunternehmen eine Rechtsgrundlage. Denn aufgrund des in Deutschland geltenden Fernmeldegeheimnisses ist dies bisher nicht möglich, auch wenn die Maßnahme als effektiv eingeschätzt wird.

Bei der etwaigen Einführung von Datenverkehrsanalysen ist allerdings Vorsicht geboten. Das hohe Maß an Datenschutz und an Vertraulichkeit der Kommunikation darf nicht ausgehöhlt werden, das Vertrauen der Nutzer in die Telekommunikationsdienste nicht geschwächt werden. Eine solche Verkehrsanalyse kann daher aus Sicht des eco nur erfolgen, wenn mehrere Bedingungen zusammenfallen. Zum einen sollte eine solche weitreichende Maßnahme nur punktuell und bei Vorliegen von erheblichen Schad- oder Störfällen durchgeführt werden, und sollte auch nur dann ergriffen werden, wenn keine andere Abhilfe möglich ist. Im Fall, dass eine solche Maßnahme ergriffen wird, sollte das Einverständnis des Nutzers eingeholt werden, mindestens aber ist er darauf hinzuweisen, dass eine solche Maßnahme durchgeführt wird. Die Maßnahme ist mit den zuständigen Datenschutzbeauftragten abzustimmen. An die Analyse solcher Verkehre ist eine enge Zweckbindung anzulegen. Auch sollte bei der Durchführung solcher Maßnahmen kritisch geprüft werden, wie genau die Analyse von Paketen erfolgt, um tatsächlich sicherheitsrelevante Erkenntnisse zu gewinnen.

Mit der vorliegenden Änderung des Telekommunikationsgesetzes unter Nummer 1 des Änderungsantrages wird diese Maßnahme eingeführt. Dem Datenschutz wird durch Nummer 1 c) ausführlich Rechnung getragen. Inwieweit die unter Nummer 1 b) festgesetzte Definition, dass Kommunikationsinhalte nicht Bestandteil der Steuerdaten seien letzten Endes Bestand haben kann, bleibt abzuwarten. Zumindest für einige wichtige Protokolle, wie beispielsweise HTTP, sind diese Unterscheidungen nicht zutreffend.

- **Umleitung von Anfragen (Sinkholing / Blackholing)**

Die Umleitung von Datenströmen bei Angriffen auf bestimmte Netze oder Infrastrukturen gilt bereits gegenwärtig als probates Abwehrmittel, insbesondere von DDoS-Attacken, aber auch zur Unterbindung des Datenabflusses aus bestimmten Netzen oder zur Isolierung von Command & Control Servern in Botnetzen. Die Maßnahme gilt als zentrale Abwehr- und Schutzmaßnahme für Ziele und wird bereits erfolgreich angewandt. Da Blackholing als Abwehrmittel vor allem eine Schutzmaßnahme für ein Angriffsziel darstellt und sich explizit auf das Umleiten von „Schadverkehr“ fokussiert, ist es nicht mit den Beeinträchtigungen für infizierte Nutzer verbunden, die bspw. die Begrenzung des Datenverkehrs mit sich bringt. Oftmals sind die entsprechenden Nutzer zu Beginn der Umleitung noch nicht bekannt und werden – falls überhaupt erforderlich – erst im Laufe des

Verfahrens ermittelt. Auch das angegriffene Ziel profitiert davon, da der „Schadverkehr“ es gar nicht mehr erreicht, sondern bereits im Vorfeld umgeleitet bzw. abgefangen wird.

Mit dem Änderungsantrag wurde in Nummer 3 der § 109a des Telekommunikationsgesetzes angepasst und dahingehend klargestellt, dass das „Umleiten“ von Verkehren im Falle einer Störung möglich ist. Die Antragsbegründung greift diese Maßnahme zwar nicht ganz umfassend auf, zeigt jedoch klar, dass Sinkholing / Blackholing als intendierte Maßnahme angedacht ist. Der Gesetzestext selbst deckt diese auch entsprechend ab, so dass diese Klarstellung begrüßenswert ist.

- **Beschränkung von Datenverkehren von Nutzern (Walled Garden)**

Eine weitere Option ist es, den Verkehr von infizierten Geräten beim Nutzer einzuschränken, so dass dieser bspw. nur noch auf Angebote zugreifen kann, die seine Sicherheitslücke beheben bzw. die Schadsoftware auf dem entsprechenden Endgerät entfernt. Die Maßnahme hat gegenüber dem jetzt teilweise bereits praktizierten kompletten Stilllegen des Anschlusses den Vorteil, dass über den Anschluss es noch möglich ist, Abhilfe für das Problem zu schaffen, was insbesondere für Privatkunden hilfreich sein dürfte.

Der Schwachpunkt einer solchen Einhegung ist, dass damit lediglich eine Schadensquelle beseitigt wird. Im Falle z.B. einer DDoS-Attacke wären hierbei zahlreiche einzelne Anschlüsse zu beschränken, so dass es für die Nutzer wie eine großflächige Beeinträchtigung des Internetverkehrs wirkt. Auch sollte nicht verkannt werden, dass für die Betreiber von Telekommunikationsdiensten diese Maßnahme mit Aufwand für die Indentifizierung von Störungsquellen und ggfs. für die Bereitstellung von Informationen zur Beseitigung von Störungen durch den Nutzer verbunden ist. Hier darf das Haftungsgefüge nicht zu Ungunsten der Betreiber von Telekommunikationsdiensten verschoben werden.

Mit dem Änderungsantrag wurde in Nummer 3 eine Änderung des § 109a des Telekommunikationsgesetzes angeregt, die – im Fall einer Störung die Nutzung von Telekommunikationsdiensten „eingeschränkt“ werden dürften, wodurch auch die hier beschriebenen Walled Gardens abgedeckt wären. Die Begründung führt diese zwar nicht namentlich auf, weist jedoch darauf hin, dass der Diensteanbieter mit Hilfe von Warnseiten die Nutzer seines Dienstes dabei unterstützen kann, die Störung zu beseitigen.

- **Blocken schädlicher Domains (Domain Filter)**

Die Beschränkung des Zugriffs auf schädliche Domains soll verhindern, dass diese Schadsoftware verteilen können. Diese Maßnahme besitzt den Vorteil, dass sie an der Schadquelle ansetzt und eine Infektion weiterer Nutzer verhindert. Gleichwohl besitzt dieses Verfahren mehrere Schwachpunkte. So ist zunächst klarzustellen, dass zwar der Zugriff auf eine solche Domain

verwehrt bliebt, aber umgekehrt diese Domains nach wie vor selbst Schadsoftware verteilen können. Auch würde im Fall einer Domainblockade die dahinterliegende IP-Adresse nach wie vor für Nutzerinnen und Nutzer erreichbar sein. Zuguterletzt bleibt auch offen, ab wann eine Domain als „schädlich“ eingestuft wird und wie das Blocken und ggfs. das Entblocken einer Domain erfolgt. Oftmals ist Webseitenbetreibern gar nicht klar, dass sie Schadsoftware verteilen bspw. durch mit Malware infizierte Werbebanner. Hieran knüpfen dann auch Fragen zur Übernahme von Kosten für die temporäre Beschränkung des Zugriffs auf Websites auch im Fall von Rechtsstreitigkeiten an. Eine Einbeziehung von Netzbetreibern erscheint nicht sinnvoll.

Mit dem Änderungsantrag wird in Nummer 3 die Rechtsgrundlage für das Blocken solcher Domains geschaffen. Inwieweit diese Maßnahme bei Nutzern und Anbietern von Telekommunikationsdiensten Zuspruch erfährt, bleibt abzuwarten.

II. Zur weiteren Debatte

Mit dem NIS-Richtlinien Umsetzungsgesetz ist ein zentraler Meilenstein für die Rechtsordnung der Sicherheit von IT-Systemen und der Netze in Deutschland geschaffen worden. Das Diskussion um weitere Maßnahmen zur Verbesserung der IT-Sicherheit ist jedoch noch nicht komplett abgeschlossen. Auf europäischer Ebene stehen noch Durchführungsrechtsakte an und es werden sowohl auf nationaler als auch internationaler Ebene Diskussionen über weitere mögliche Maßnahmen geführt. eco möchte eine Auswahl dieser derzeit diskutierten Überlegungen ansprechen, die aus seiner Sicht besonderer Kommentierung bedürfen.

- **Regelung der Meldepflicht**

Der Änderungsantrag führt in §109 TKG eine zusätzliche Meldepflicht an das BSI ein. Bisher hat diese für Anbieter von Telekommunikationsdiensten nur gegenüber der BNetzA bestanden. Die Etablierung zusätzlicher Meldepflichten und damit parallele Meldewege und -strukturen belastet Unternehmen zusätzlich und bringt keinen tatsächlichen Mehrwert für die Beseitigung von Sicherheitsvorfällen. Es wäre sinnvoll, wenn die Meldepflichten weiterhin bei der Bundesnetzagentur verblieben, wo bereits etablierte Strukturen und Expertise im Umgang mit Meldungen besteht.

- **Regelung zur Flexibilität für die Anwendung von Maßnahmen zur Sicherung der Netzwerke**

Die im neuen § 109a und § 100 TKG aufgelisteten Maßnahmen können von Anbietern von Telekommunikationsdiensten im eigenen Ermessen ergriffen werden. Entscheidend ist, dass diese Flexibilität erhalten bleibt. Eine Verpflichtung zur Durchführung bestimmter Maßnahmen wäre

kontraproduktiv. Eine Anordnung einer solchen Maßnahme würde im Zweifel auch am Ziel vorbeiführen. Die Kosten für die Durchführung einer angeordneten Maßnahme können den zu erwartenden Nutzen bei weitem übersteigen, und die Grundlage, auf der Maßnahmen angeordnet würden, wäre mit komplexen Einzelfallprüfungen verbunden, die einer schnellen und adäquaten Maßnahme abträglich wären.

- **Regelung von Telemedienangeboten**

Überlegungen, zur Verbesserung der Sicherheit in Telemedienangeboten sollten sorgfältig geprüft werden. Es bestehen bereits gesetzliche Maßgaben, die ausreichend sind. Der § 13 (7) des Telemediengesetzes verpflichtet Diensteanbieter schon jetzt dazu, Sicherheitsmaßnahmen bereitzuhalten. Und auch auf europäischer Ebene wird das Thema vorangetrieben. Der EUGH hat zuletzt durch seine Rechtsprechung die Möglichkeiten für Diensteanbieter gestärkt und bestätigt. Der Entwurf der ePrivacy-Verordnung der Kommission sieht die Erhebung von Daten ebenfalls als Option an. Eine eigenständige, deutsche Regelung würde an dieser Stelle nicht weiterhelfen. Weitere, darüber hinausgehende Regelungen könnten sich als kontraproduktiv erweisen. Das Haftungsgefüge und die Schutzmechanismen des Telemediengesetzes auch für Nutzerinnen und Nutzer bspw. im Bereich der pseudonymen oder anonymen Kommunikation sollten auf keinen Fall aufgeweicht werden.

- **Regelung allgemeiner Mindeststandards für IT-Produkte**

Eine in der Politik häufig diskutierte Maßnahme sind Mindeststandards für IT-Produkte bzw. Produkte, in denen IT verbaut ist. Die Bandbreite der diskutierten Ansätze beinhaltet dabei Verordnungen oder Gesetze für Anforderungen oder ein weniger strikter Ansatz über ein Gütesiegel.

Beiden Optionen ist eigen, dass sie nicht die Vielfalt und die Breite, in der IT heute Anwendung findet, adäquat wiederspiegeln. Daneben gilt es zu berücksichtigen, dass je nach Anwendungsgebiet auch spezielle Regulierung, Auflagen und spezialgesetzliche Vorgaben bestehen – bspw. im Gesundheitssektor. Einem so feingliedrigen und vielfältigen System könnte eine einheitliche Regelung nicht gerecht werden.

Daneben besteht bei einem Gütesiegel das Problem, dass bereits jetzt mehrere Gütesiegel in einem Markt mit Wettbewerb etabliert sind. Ein „staatliches Gütesiegel“ würde diesen Wettbewerb und damit auch die Innovation im Bereich der IT-Sicherheit hemmen und ausbremsen.

Aus den genannten Gründen sollte ein staatlich getriebenes Gütesiegel nicht weiterverfolgt werden. Eine gesetzliche Regelung für Mindeststandards wird immer hinter den technischen Entwicklungen zurückstehen und bürokratische Auflagen für alle Beteiligten schaffen, die in keinem Verhältnis zum zu erwartenden Nutzen stehen.