DENIC eG
Kaiserstraße 75 - 77
60329 Frankfurt am Main

Telefon +49 69 27 235-0
Telefax +49 69 27 235-235
E-Mail info@denic.de

https://www.denic.de

DENIC eG · Kaiserstraße 75 - 77 · 60329 Frankfurt am Main · Deutschland

Bundesministerium des Innern, für Bau und Heimat
Referat CI 1
Alt-Moabit 140
10557 Berlin

per E-Mail an CI1@bmi.bund.de

Ihr Ansprechpartner:

Hr. Peter Koch

Ihr Zeichen / Ihre Nachricht vom	Unser Zeichen	
[Ihr Zeichen]	[Unser Zeichen]	10. December 2020

Kommentar der DENIC eG zum *Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)* vom 1. Dezember 2020

Sehr geehrte Damen und Herren,

DENIC unterstützt das Ziel, die IT-Sicherheit insbesondere Kritischer Infrastrukturen zu stärken und das auch durch die Fortschreibung der IT-Sicherheitsgesetzgebung zu begleiten. Dazu hätte eine Evaluierung des IT-SiG aus dem Jahre 2015 (wie ebd. vorgesehen) insbesondere unter Beteiligung der Normadressaten wertvolle Hinweise liefern können.

Der vorliegende Entwurf verfolgt eine Vielzahl von Ansätzen mit unterschiedlicher technischer Detail- und ebenso unterschiedlicher Eingriffstiefe, vermittelt dabei aber kein klares Gesamtbild der Zielsetzung, insbesondere eines Zugewinns an Sicherheit für die Betreiber Kritischer Infrastrukturen oder deren Kunden.

Diese Kommentierung erhebt wegen der Vorläufigkeit des Referentenentwurfs und der Kurzfristigkeit keinen Anspruch auf Vollständigkeit, darum sei ein einzelner Punkt (Portscans, §7b BSIG-E) beispielhaft adressiert:

Sogenannte Portscans, also das „Abklingeln“ des Internet-Adressraumes in Gänze oder in Teilen zur Auffindung von Systemen oder Diensten auf solchen Systemen, sind Teil des – gelegentlich lästigen – „Grundrauschens“ im Internet. Sie können mit lauteren wie unlauteren Absichten erfolgen und sowohl der Vorbereitung von Angriffen dienen als auch ihrer Vorbeugung sowie der sonstigen Forschung. Insofern ist sicher grundsätzlich zu begrüßen, dass das BSI sich künftig – in begrenztem Rahmen – auch auf diesem Wege einen Überblick verschaffen können soll.

Allerdings wären Überlegungen zur Notwendigkeit einer solchen speziellen Ermächtigung des BSI in der Begründung wünschenswert – stattdessen jedoch muss die Begründung als Raum für die Definition und Erklärung des Begriffs Portscan herhalten, hat also normative Funktion. Dabei wird der – in der Tat auch fachsprachlich nicht eindeutig abgegrenzte Begriff – so weit gedehnt, dass der reine „Scan" sogar das Abprüfen von Standardpasswörten umfassen könnte.

Unverständlich ist, wie die Begründung dann zwei Abschnitte später ausführen kann, dabei handelte es sich gerade nicht um das Eindringen in ein System. Die für die Eingrenzung des Mandats wesentlichen Ausführungen zu Adressen und Adressverwaltung gehen davon aus, dass IP-Adressbereiche „den Staaten […] zugeteilt" seien und sich dadurch das Bild eines „deutschen Adressraumes" ergebe. Das trifft so nicht zu. Die IP-Adressraumverwaltung erfolgt in Europa durch das RIPE NCC in Amsterdam, dabei werden keine nationalen Stellen zwischengeschaltet und auch der Standort eines Systems lässt sich damit weder vorherbestimmen noch nachvollziehen. Schließlich ist die Beschreibung von Portscans nicht technikneutral und damit nicht zukunftsfest, da bereits heute für IPv6 das Verfahren in dieser Form wegen der schieren Anzahl der verfügbaren Adressen (insgesamt, aber auch pro Organisation) nicht praktikabel ist. Zwar haben Angreifer dasselbe „Problem", es ist jedoch absehbar, dass in Bälde ein weiteres oder erweitertes Verfahren wiederum in den Gesetzgebungsprozess eingebracht werden muss.

Damit offenbart sich das grundlegende Dilemma: die Nutzung des Verfahrens mag sinnvoll und – eventuell mit Einschränkungen - wünschenswert sein, die für alle Seiten notwendige technische Detailtiefe lässt sich aber schwerlich in ein Gesetz (und ebensowenig in dessen Begründung) fassen. Das gilt im übrigen nicht nur für Portscans, sondern auch für die im Entwurf vorgesehenen Honeypots, Systeme zur Angriffserkennung oder die Botnetbekämpfung.

Erforderlich ist ein neuer Ansatz, interdisziplinär und multi-stakeholder, der die Akteure und die Betroffenen einbindet, operative Praxis berücksichtigt, auf der gesetzgeberischen Ebene mehr Stabilität schafft und auf der Umsetzungsebene Flexibilität mit Rechtssicherheit vereinbart.

Über die DENIC eG

Die DENIC eG (https://www.denic.de) verwaltet die Top-Level Domain (TLD) .de, den deutschen Namensraum im Internet. Mit einem Bestand von über 16,7 Millionen Domains zählt sie zu den weltweit größten Registrierungsstellen. 1996 als Genossenschaft ohne Gewinnerzielungsabsicht gegründet, führt DENIC heute etwa 300 deutsche und internationale Unternehmen der IT- und Telekommunikationsbranche als Mitglieder, die .de-Registrierungsdienste für Endkunden anbieten. Mehr als 6 Milliarden Mal am Tag werden .de-Adressen über das weltweit verteilte Netz von Nameservern aufgerufen - mit diesem Dienst zählt DENIC zu den kritischen Infrastrukturen. Die DENIC eG hat ihren Sitz

in Frankfurt am Main. Sie beschäftigt etwa 110 Mitarbeiter und erzielt einen Jahresumsatz im zweistelligen Millionenbereich.

Mit freundlichen Grüßen

Dr. Jörg Schweiger

Mitglied des Vorstandes