WIR GESTALTEN DAS INTERNET.

eco

Verband der deutschen Internetwirtschaft e.V.

STELLUNGNAHME

Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme des Bundesministeriums des Innern

Berlin, 05.04.2013

eco – Verband der deutschen Internetwirtschaft e.V. versteht sich als Interessenvertreter und Förderer aller Unternehmen, die mit oder im Internet wirtschaftliche Wertschöpfung betreiben. Der Verband vertritt derzeit rund 600 Mitglieder. Hierzu zählen unter anderem ISP (Internet Service Provider), ASP (Application Service Provider), Carrier, Hard- und Softwarelieferanten, Content- und Service-Anbieter sowie Kommunikationsunternehmen. Der eco Verband ist damit der größte nationale Internet Service Provider Verband Europas.

Das Bundesministerium des Innern hat am 6. März 2013 einen Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vorgelegt und die Verbände um Stellungnahme bis zum 5. April 2013 gebeten. eco nimmt gerne die Gelegenheit wahr, sich zum geplanten Gesetz und dessen Auswirkungen auf die Internetwirtschaft zu äußern.

Grundsätzliche Anmerkungen

Ziel des Gesetzes soll sein, die Zusammenarbeit zwischen Staat und den Betreibern kritischer Infrastruktur zu verbessern und ein Mindestniveau an IT-Sicherheit bei den Betreibern zu gewährleiten. Dazu sollen den Betreibern kritischer Infrastrukturen neue Pflichten auferlegt werden, die der Verbesserung des Schutzes der von ihnen eingesetzten Informationstechnik sowie einer Verbesserung ihrer Kommunikation mit dem Staat bei IT-Vorfällen dienen sollen, u.a. sollen sie ihre Kunden und das Bundesamt für Sicherheit in der Informationstechnik (BSI) über erhebliche IT-Sicherheitsvorfälle informieren. Im Zuge dieses Gesetzes sollen dem BSI und dem BKA weitere Aufgaben und Kompetenzen zugewiesen und neue Personalstellen gebilligt werden.

Das neue Gesetz wird Änderungen im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz), Bundeskriminalamtgesetz, Telemediengesetz (TMG) sowie Telekommunikationsgesetz (TKM) nach sich ziehen.

Im Hinblick auf die stetig wachsenden und neuen Herausforderungen bei der Gewährleistung von Cybersicherheit und die hohe Abhängigkeit der deutschen Wirtschaft von einer funktionierenden IT-Infrastruktur begrüßt eco grundsätzlich Bestrebungen der Bundesregierung, die Wirtschaft bei der Erhöhung der ITK-Sicherheit zu unterstützen. Insbesondere im Bereich der kritischen Infrastrukturen den Schutz der Integrität und Authentizität datenverarbeitender Systeme zu verbessern und ggf. einer gestiegenen Bedrohungslage anzupassen.

Allein die Betrachtung des Themas ITK-Sicherheit durch die Bundesregierung als branchenübergreifendes Querschnittsthema, wie es der UP-KRITIS unter Mitwirkung des eco seit Jahren behandelt, wird der Bedrohungslage gerecht. Grundlage für die Kooperation zwischen den relevanten Akteuren von Staat und Wirtschaft im Rahmen eines Umsetzungsplans ist der vertrauensvolle und zügige Informationsaustausch. Dabei erscheint das Potential einer Zusammenarbeit im Bereich KRITIS längst nicht ausgeschöpft.

Von der Bundesregierung und der Europäischen Kommission geförderte Initiativen zur der Verbesserung der ITK-Sicherheit gingen in den vergangenen Jahren gerade auf Impulse aus der Wirtschaft unter Beteiligung des eco und seiner Mitgliedsunternehmen zurück. Das Anti-Botnet-Beratungszentrum, die Initiative-S und das europaweite Advanced Cyber Defense Centre sind nur einige Beispiele funktionierender Einrichtungen, deren Maßnahmenpakete das Potential besitzen ineinander zu greifen und staatliche wie private Akteure in die Lage versetzen, flexibel auf neue Bedrohungslagen zu reagieren und die ITK-Sicherheit zu erhöhen.

ITK-Sicherheit ist für die Internetwirtschaft bereits seit Jahren eine Selbstverständlichkeit. Gesetzliche Maßnahmen zur Implementierung eines Mindestsicherheitsstandards, wie sie der Entwurf vorsehen, erscheinen hier heute überholt, allenfalls sachfremd. Dies betrifft auch das Ziel des vorgelegten

Referentenentwurfs, das Sicherheitsniveau von ITK-Infrastrukturen vorzugeben, in dem auf den jeweiligen Stand der Technik verwiesen wird.
Die Zusammenarbeit mit BSI und Strafverfolgungsbehörden ist für die in den relevanten Bereichen tätigen Akteuren der Internetwirtschaft ebenso selbstverständlich wie die regelmäßige Teilnahme an nationalen und europäischen Notfall-Übungsszenarien.

Das System für den durch die durch den Referentenentwurf intendierte Regulierung des Informationsflusses im Falle von sicherheitsrelevanten Vorfällen bei Betreiber kritischer Infrastrukturen besteht bereits, so dass zunächst zweifelhaft erscheint, ob eine gesetzliche Regelung in diesem Bereich überhaupt angezeigt ist.

Maßgeblicher Bezugspunkt und Grundlage jeglicher Überlegungen zur Verbesserung der IT-Sicherheit kann nur das bestehende, im Zuge der Selbstregulierung der Internetwirtschaft und damit auch auf Public-Private-Partnerships aufgebaute System sein.

Hinzu kommt, dass der Begriff der „Betreiber von kritischen Infrastrukturen“ gerade in der Internetwirtschaft nicht festgelegt ist. Damit ist der Umfang des Gesetzesentwurfes und dessen Bedeutung für viele Interneternehmen nicht geregelt bzw. unklar. Vor diesem Hintergrund können auch keine seriösen Aussagen zu jährlichen Fallzahlen und einer Kostenschätzung übermittelt werden, wie vom BMI gebeten. Auf jeden Fall werden Kosten für die Internetbranche entstehen (Personal, Hardware, Software, Management), um die Anforderungen des Gesetzes zu erfüllen.

In Expertenausschüssen und Arbeitsgruppen wie EP3R oder denen des IT-Gipfels (etwa Unterarbeitsgruppe 3 der Arbeitsgruppe 4 „Providerverantwortung stärken“ des BMI) oder der Task Force „IT-Sicherheit in der Wirtschaft“ des BMWi arbeiten die Akteure und Verbände nachhaltig an Lösungen zur ITK-Sicherheit mit nationalem, aber auch mit europäischem Bezug. In zahlreichen freiwilligen Initiativen der Wirtschaft und Verbände wie z.B. Deutschland sicher im Netz wird seit Jahren gemeinsam mit der Bundesregierung an der Erhöhung des Sicherheitsniveaus gearbeitet.

Insbesondere vor dem Hintergrund der nunmehr auf der Grundlage der EU-Cybersecurity-Strategy sowie des Entwurfs einer Direkte zur Netzwerk- und Inofrmationssicherheit (NIS-Direktive) initiierten europäischen Regulierungsbestrebungen ist der Entwurf des BMI zum jetzigen Zeitpunkt kritisch zu sehen. Auch unter der Voraussetzung, dass die Bundesregierung bzw. das BMI proaktiv an dem europäischen Prozess teilnimmt und diesen in ihrem Sinne begleitet ist darauf zu achten, dass ein sinnvoller Gleichlauf mit einem nationalen Gesetzgebungsvorhaben entsteht. Der Entwurf eines IT-Sicherheitsgesetzes erscheint zu einem Zeitpunkt, zu dem der Entwurf einer NIS-Direktive gerade erst vorgestellt worden ist, jedenfalls verfrüht.

Vor diesem Hintergrund erlauben wir uns folgende Anmerkungen zu dem vorgelegten Gesetzentwurf:

Artikel 1: Änderung des BSI-Gesetzes

§ 10 Ermächtigung zum Erlass von Rechtsverordnungen

Die Kriterien, nach denen Einrichtungen, Anlagen oder Teile davon als kritische Infrastrukturen im Sinne des BSI-Gesetzes einzuordnen sind, sollen gemäß dem Referentenentwurf nach Anhörung der betroffenen Betreiber und der betroffenen Wirtschaftsverbände über eine Verordnung des BMI bestimmt werden. Für die Betroffenen haben die gesetzlichen Regelungen weitreichende wirtschaftliche Folgen mit nicht unerheblichen Eingriffen in ihre Freiheitsrechte. Die Bestimmung der Definitionskriterien durch das BMI als Verordnungsgeber gibt Betroffenen, auch soweit sie als solche vorher angehört wurden, nicht mit hinreichender Sicherheit Aufschluß darüber, ob sie Adressat der gesetzlichen Regelung sind oder nicht.

Die Definitionskriterien für kritische Infrastrukturen sollten daher Gegenstand einer parlamentarisch zu verabschiedenden Gesetzes sein.

§ 8a Absatz (1)

Die in dem Entwurf vorgesehene Umsetzungsfrist von zwei Jahren ist vor dem Hintergrund der vorzunehmenden umfangreichen operativen Implementierungen sowie entsprechender Audits nach Absatz (4) erheblich zu kurz. Bereits die Erarbeitung und Anpassung der Standardisierungsprozesse innerhalb der Branchen kann, insbesondere auch international, einen längeren Zeitraum in Anspruch nehmen. Zudem sind binnen gleicher Frist noch ggf. Anerkennungen durch das BSI nach Absatz (3) sowie die Sicherheitsaudits nach Absatz (4) durchzuführen. Ein Implementierungszeitraum von nicht weniger als vier Jahren erscheint daher angemessen. Die Umsetzungsfrist sollte dabei erst dann laufen, wenn die Branchenverbände ihre branchenspezifischen Sicherheitsstandards (Absatz (3)) verabschiedet haben bzw. wenn der Stand der Technik - siehe Absatz (2) - für die Branche einheitlich definiert worden ist.

§ 8a Absatz (2)

Die Bundesregierung kann sich nicht auf eine allgemein gehaltene Erläuterung zur Bestimmung des Standes der Technik zurückziehen. Da alle Maßnahmen der Betreiber von kritischen Infrastrukturen an diesem Stand gemessen werden, ist eine Verknüpfung mit den branchenspezifischen Sicherheitsstandards (Absatz (3)) unabdingbar.

§ 8a Absatz (3)

eco begrüßt die Möglichkeit, Sicherheitsstandards branchenspezifisch zu entwickeln und einzuführen. Auf der Grundlage dessen, was sich in der Internetwirtschaft bereits als „Best Practice“ sowie auch normativ etabliert hat, vor allem aber im Rahmen des im Zuge der Selbstregulierung beständig stattfindenden Austauschs wird die praxisnahe und individuell-risikobezogene Entwicklung von Lösungsansätzen begünstigt. Soweit diese jedoch unter dem Vorbehalt der Anerkennung durch das BSI stehen, ist zur Vermeidung nationaler Alleingänge zu beachten, dass dadurch nicht die Prozesse der internationalen Standardisierung konterkariert werden dürfen. Gerade auch Branchen, die sich auf nur wenige nationale Anbieter stützen, werden europäischen bzw. internationalen Standards den Vorzug geben.
Vor diesem Hintergrund sollte dem BSI bei der Entwicklung branchenspezifischer Lösungen ausschließlich beratende Funktion zukommen.

Eine weitere Ausweitung der Aufgaben und Befugnisse des BSI lehnt eco grundsätzlich ab. Dies würde den im BSI-Gesetz festgelegten Tätigkeitsrahmen (Sicherheit der Informationstechnik des Bundes) überschreiten. Hierfür wird keine Notwendigkeit gesehen.

§ 8a Absatz (4)

Zur Überprüfung der Umsetzung der Maßnahmen nach Absatz 1 sind Sicherheitsaudits vorgesehen. Der vorgesehene Umfang eines solchen Audits ist jedoch unklar, sowohl hinsichtlich der Prüftiefe als auch des Prüfgegenstandes. Eine ausdrückliche Beschränkung des Audits auf für den Betrieb kritischer Infrastrukturen wesentliche Elemente erscheint jedenfalls sinnvoll. Zur Reduzierung des Ausfallrisikos der zu überprüfenden Infrastrukturen bei technischen Audits erscheint es geboten, die Qualifikation der Auditoren an besondere Voraussetzungen zu knüpfen. Vor diesem Hintergrund sollte als Alternative zum Audit auch die Anerkennung einer Zertifizierung nach internationalen Sicherheitsstandards in Betracht gezogen werden.
Im Rahmen der Zertifizierung etwa nach ISO 27001 sind Sicherheitsmanagement sowie die entsprechenden Sicherheitsmaßnahmen nachzuweisen. ISO 27001 beinhaltet auch ein umfangreiches Auditprogramm. Hinsichtlich eines Re-Audits nach Absatz (4) ist zu empfehlen, die Frist der dreijährigen Zertifikatslaufzeit nach ISO 27001 anzupassen.
Hinzu kommt, dass schon heutzutage im Rahmen der regulären Wirtschaftsprüfung bzw. des Jahresabschlusses durch einen Wirtschaftsprüfer die IT eines Unternehmen geprüft und abgenommen wird. Im Rahmen dieser Audits werden auch IT-Sicherheitsaudits vorgenommen, da die Geschäfte von den betroffenen Unternehmen maßgeblich von der Funktionsfähigkeit der IT abhängig sind. Es ist daher nicht nachvollziehbar, warum zusätzliche Sicherheitsaudits durchgeführt werden müssen. Des Weiteren ist eine automatische Meldung der aufgedeckten Sicherheitsmängel an das BSI für die Unternehmen nicht tragbar. Diese Informationen unterliegen dem Geschäftsgeheimnis und sollten nicht einer Behörde automatisch weitergeleitet werden. Besonders vor dem Hintergrund, dass keinerlei Definition zu Art und Umfang des Sicherheitsmangel vom BMI vorgeben ist.

§ 8b Meldepflicht für IT-Sicherheitsvorfälle

Wie schnell auf einen IT-Sicherheitsvorfall reagiert und dessen Schadpotential begrenzt werden kann, hängt maßgeblich von der Effektivität des Informationsflusses zwischen den Beteiligten im Risikoumfeld ab. Doppelzuständigkeiten bei der Meldung von erheblichen IT-Sicherheitsvorfällen i.S.d. § 8b sind daher in jedem Falle zu vermeiden. eco begrüßt die Rolle des BSI als zentrale Stelle zur Auswertung erheblicher Sicherheitsvorfälle im Bereich kritischer Infrastrukturen sowie vor diesem Hintergrund auch grundsätzlich die sektorspezifische Abgrenzung der Zuständigkeiten durch Absatz (5) in Bezug auf bereits durch Bundesgesetz etablierte Kommunikationsstrukturen. Ein effektiver Informationsaustausch findet allerdings bereits heute unter Beteiligung des BSI im Netzwerk staatlicher und privater CERTs sowie bei Einrichtungen wie der Allianz für Cybersicherheit und zukünftig auch dem Advanced Cyber Defense Centre statt. Auch und vor allem erhebliche Sicherheitsvorfälle sind Gegenstand der hier ausgetauschten Informationen. Eine Privilegierung der an diesen Kommunikationsstrukturen teilnehmenden Anbieter ergibt sich indes nicht. Eine entsprechende Erweiterung des Absatz (5) würde dieses Manko beheben und betroffene Unternehmen bei der Vielzahl der bereits bestehenden Meldepflichten entlasten.

Schließlich ist auch kein Grund ersichtlich, warum statt der bisherigen im TKG definierten Meldewege für solche Vorfälle, „die zur Störung der Verfügbarkeit“ führen, neue Warn- und Alarmierungskontakte nach Absatz (3) genutzt werden sollen. Bereits die Definition eines erheblichen IT-Sicherheitsvorfalls als “Vorfall, der zur Störung der Verfügbarkeit“ führt, ist nicht greifbar. Die Ausweitung der im Rahmen des § 109a Abs. 4 TKG-E zu meldenden Vorgänge erfasst ohne Weiteres bereits kurzzeitige und in diesem Sinne geringfügige Verfügbarkeitseinschränkungen und erscheint daher nicht sachgerecht. Zudem sollte, wenn schon eine gesetzliche Regelung der Meldepflichten erheblicher Sicherheitsvorfälle angestrebt wird, deren Definition auch hinreichend eindeutig ausfallen. Praktikabel erscheint es dabei, im BSI-Gesetz und TKG einheitliche Maßstäbe für die zu meldenden Ereignisse zu definieren. Eine Information des BSI sollte demnach grundsätzlich über die BNetzA erfolgen.

Artikel 3: Änderung des TMG

Die in dem Entwurf vorgesehene Verpflichtung geschäftsmäßiger Dienstanbieter zum Schutz ihrer Systeme vor unerlaubtem Zugriff erscheint für das grundsätzlich unterstützenswerte Anliegen der Gewährleistung von IT-Sicherheit der für Dritte angebotenen Inhalte nicht zielführend. Bereits systematisch fügt sich die Regelung nicht in den Gesamtkontext des Referentenentwurfs ein, der die IT-Sicherheit kritischer Infrastrukturen im Fokus hat Die mit dem Referentenentwurf vorgeschlagene Änderung des Telemediengesetzes erfasst zudem mit den Diensteanbietern nicht nur die Betreiber kritischer Infrastrukturen, sondern einen unüberschaubaren Adressatenkreis.

Der Adressatenkreis des § 13 Abs. 7 TMG-E ist deckungsgleich mit dem der Impressumspflicht aus § 5 Abs. 1 TMG. Nach der gefestigten Rechtsprechung ist Adressat dieser Norm nahezu jeder Betreiber, der Telemedien auf Grund einer nachhaltigen Tätigkeit (also nicht einmalig) mit oder ohne Gewinnerzielungsabsicht erbringt. Bereits die Werbefinanzierung einer Website (z.B. durch Bannerwerbung) kann hier genügen. Ein beträchtlicher Anteil der hier Betroffenen ist weder technisch noch organisatorisch in der Lage, die geforderten Maßnahmen zur IT-Sicherheit zu ergreifen. Das ist aus Sicht des eco auch gar nicht notwendig, denn nur eine Minderheit der hier angesprochenen Anbieter von Telemedien betreibt zugleich auch die technische Infrastruktur selbst. Diese wird vielmehr von kommerziellen Hostern und Infrastrukturanbietern betrieben, die ihrerseits bereits durch andere Regelungen zur IT-sicherheit verpflichtet werden sollen. Reine Content-Anbieter sind zumeists bereits faktisch nicht in der Lage, in einer Weise auf die IT-Infrastruktur einzuwirken, die es ihnen gestatten würde, die vom Gesetzentwurf geforderten technischen Vorkehrungen zu treffen. Auch die Einschränkung "soweit technisch möglich und zumutbar" hilft hier nicht; sie führt vielmehr zu Rechtsunsicherheit im Einzelfall. Insgesamt sollte daher von einer Einbeziehung der Telemedienanbieter Abstand genommen werden.

Betreiber kritischer Infrastrukturen werden durch andere Regelungen verpflichtet, Betreiber stark frequentierter nicht-kommerzieller Angebote indes nicht erreicht, so dass auch die Wirksamkeit der Regelung fraglich ist. Als effektiv hat sich dagegen die Unterstützung von Angeboten wie der Initiative-S des eco erwiesen, wobei hier auch kleinere Anbieter mit einfachen Mitteln

Sicherheitsmindeststandards umsetzen können. Von den vorgeschlagenen Änderungen des Telemediengesetzes sollte daher abgesehen werden,

Artikel 4: Änderung des TKG

§ 109a Absatz (4) Daten- und Informationssicherheit

Entsprechend den Ausführungen zu den Änderungsentwürfen zu § 8b BSI-Gesetz ist auch hier zunächst darauf hinzuweisen, dass der Auslöser einer Meldepflicht „Beeinträchtigungen, die zur Störung der Verfügbarkeit der über die betroffenen Netze erbrachten Dienste führen können“, zu weitgehend ist. Mangels hinreichender Einschränkung wären hiervon auch Beeinträchtigungen der Verfügbarkeit betroffen, die nur kurzzeitig bestehen und geringfügig ausfallen. Die Auslöseschwelle kann jedoch nicht unterhalb der von der Rechtsprechung für die Beziehung Anbieter-Kunde als vertraglichwesentlich bewerteten Mindestverfügbarkeit liegen, nach der kurzzeitige Verfügbarkeitsbeeinträchtigungen toleriert werden.

eco lehnt eine gesetzliche Verpflichtung der Telekommunikationsanbieter zur Information solcher Nutzer, von deren Datenverarbeitungssystemen Störungen ausgehen, zum Hinweis auf Mittel zur Behebung ab.

Zum einen ist der Begriff der Datenverarbeitungssysteme erheblich zu weitreichend. Hiervon erfasst würde wohl jedes Endgerät, einschließlich derer, zu denen dem jeweils betroffenen Provider die Expertise fehlt. Die hier angestrebte ausufernde Hinweispflicht entpuppt sich als Beratungsauftrag, den zu erfüllen Provider in diesem universellen Ausmaß unmöglich in der Lage sein werden. Die Beschränkung auf technisch mögliche und zumutbare Fälle ist indes nicht geeignet, das avisierte Handlungsfeld der Provider mit hinreichender Rechtssicherheit einzugrenzen.

Vielmehr plädiert eco dafür, die bisherigen Aktivitäten der Wirtschaft wie das Anti-Botnetz-Beratungszentrum, die Initiative-S, sowie das nunmehr sich im Aufbau befindliche Advanced Cyber Defense Centre weiter zu unterstützen und zu vernetzen. Die Initiativen haben zu einem deutlichen Rückgang der Anzahl infizierter Rechner privater Nutzer geführt. Dies ist dem gelegentlich

vorgebrachten Argument einer mangelnden Beteiligung der Wirtschaft an den Initiativen ebenso entgegenzuhalten wie die Tatsache, dass zur Erreichung des relevanten Teils der Internetnutzer in Deutschland es nicht zielführend ist, auch den kleinsten regionalen Provider zu einer Teilnahme anzuhalten. Initiativen der Selbstregulierung basieren auf den praktischen Erfahrungen der Wirtschaft und sind, anders als gesetzliche Regelungen, in der Lage, Maßnahmen flexibel dort anzubringen, wo sie notwendig erscheinen. Eine gesetzliche Regelung ist gerade im Bereich der im vorliegenden Referentenentwurf im Übrigen sachfremd geregelten Absicherung von für die flächendeckende IT-Sicherheit zunächst unkritischer privater Systeme grundsätzlich abzulehnen.

Erfüllungsaufwand für die Wirtschaft

Durch die angestrebten Regelungen würde nahezu die gesamte Internetwirtschaft mit Mehraufwendungen verbunden. Sowohl die Änderungen im TKG würden aus den vorgenannten Gründen auch bei den Providern zu zusätzlichem Aufwand führen, die an Initiativen wie dem Anti-Botnet-Beratungszentrum teilnehmen, indem deren Handlungsfeld ausufernd ausgeweitet würde. Kleinere Provider, deren Kundenstamm seiner Stärke nach kein relevantes Bedrohungspotential darstellt, würden zusätzlich von den avisierten Verpflichtungen betroffen sein. Wegen der Änderungen im BSI-Gesetz würden für die Betreiber kritischer Infrastrukturen Mehraufwände durch teilweise zusätzliche Meldewege für Vorfälle bestimmter Qualität geschaffen. Schließlich würden durch Auditverpflichtungen im Gesetzentwurf in seiner vorliegenden Form auch jene Unternehmen betroffen sein, die bereits jetzt den angestrebten Sicherheitsstandard durch Zertifizierungen erfüllen.

Insgesamt stellt sich die Frage, ob es nicht in anderen Branchen Nachhol- oder Verbesserungsbedarf gibt, der die IT-Sicherheit ingesamt erhöhen würde. Die ITK-Branche kann nicht stellvertretend für die andere sicherheitsrelevante Bereiche deren "ureigenste Aufgaben" wahrnehmen oder deren "Versäumnisse kompensieren". Die Zuordnung von Zuständigkeiten und Verantwortlichkeiten sollte daher genau geprüft werden.