Gemeinsame Stellungnahme zu

ENISA

Europäische Agentur für Netz- und Informationssicherheit

Vorschlag der EU-Kommission

Die Europäische Kommission plant die Schaffung einer „Europäischen Agentur für Netz- und Informationssicherheit – ENISA (European Network Information Security Agency)“. Zum 1. Juli dieses Jahres wird die EU eine Arbeitsgruppe einsetzen, in der weitere Detailfragen zur Ausgestaltung der Agentur bis Ende 2003 geklärt werden sollen.

Die Ministerien BMI und BMWA geben BITKOM und TeleTrusT die Möglichkeit, zu dem Vorhaben der Europäischen Kommission Stellung zu nehmen sowie Themenfelder zu benennen, die in dieser Agentur behandelt werden sollten.

Eine Grundvoraussetzung für vertrauenswürdige Anwendungen in offenen Netzen ist die Vertrauenswürdigkeit der Netze selbst sowie der in ihr zur Unterstützung der Anwendungen angebotenen Dienstleistungen. Von besonderer Bedeutung dabei ist, dass die Netze und die in ihnen angebotenen Dienste nicht an Staatsgrenzen enden, während die Maßnahmen zur Sicherstellung der Grundlagen ihrer Vertrauenswürdigkeit durch teils differierende nationale Interessen geprägt sind.

Es ist wichtig, dass die nationalen Maßnahmenkomplexe, die aus verschiedenen Sichten und unterschiedlicher Realisierungstiefe bei der Umsetzung der EU-Richtlinien entstanden sind und zu nicht interoperablen Lösungen geführt haben, mit Hilfe der Agentur harmonisiert werden.

Grundsätzlich begrüßen BITKOM und TeleTrusT den Vorschlag der EU Kommission zur Einrichtung einer Agentur für Netz- und Informationssicherheit in Europa. Sie geben aber zu bedenken, dass es sich bei der Agentur nicht um eine zusätzliche Regulierungsinstanz der ohnehin bereits stark regulierten TK Industrie handeln darf. Vielmehr stellen BITKOM und TeleTrusT die Notwendigkeit einer Agentur mit empfehlendem Charakter heraus, die sich um die Förderung des Bewusstseins für IT und TK Sicherheit in allen Gesellschaftsschichten kümmert.

Gerade dieser Bereich ist originär international und grenzüberschreitend zu behandeln. Die informationsgesellschaftlichen Ziele der Europäischen Union, formuliert in den Initiativen eEurope 2005 (Förderung sicherer Dienste, Anwendungen und Inhalte auf der Grundlage einer weithin zugänglichen Breitband-Infrastruktur), und das auf dem EU Gipfel in Lissabon verabschiedete Ziel „Europa 2010“ (die wettbewerbsfähigste Wissensgesellschaft weltweit

TeleTrusT Deutschland e.V.
Chamissostraße 11
99096 Erfurt
Telefon +49 361 3460531
Telefax +49 361 3453957
E-Mail info@teletrust.de
Internet www.teletrust.de

Geschäftsführer:
Prof. Dr. Helmut Reimer

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin Mitte
Telefon +49 30 27576-0 ,
Telefax +49 30 27576-400
E-Mail bitkom@bitkom.org,
Internet www.bitkom.org

Präsident: Dr. Volker Jung

Hauptgeschäftsführer:
Dr. Bernhard Rohleder (Vors.)
Dr. Peter Broß

Ansprechpartner:
Dr. Sandra Schulz
Hauptgeschäftsstelle
Telefon +49 30 27576-242, Telefax -247

zu schaffen) können nur auf der Grundlage robuster Infrastrukturen erreicht werden. Das Hauptziel der Agentur „… in Europa eine gemeinsame Sicht der Fragen der Informationssicherheit zu erreichen, die notwendig ist, um die Verfügbarkeit und Sicherheit von Netzen und Informationssystemen in der Union zu gewährleisten.“ wird daher von der ITK-Industrie voll unterstützt. Mit einer solchen Agentur besteht die Möglichkeit, dass im europäischen Binnenmarkt ein harmonisiertes Sicherheitsniveau für Telekommunikation und Informationstechnik und damit eine vertrauenswürdige Basis für Anwendungen in offenen Netzen erreicht wird.

Ausdrücklich begrüßen BITKOM und TeleTrusT, dass die Europäische Kommission in ihrer Begründung auf „das menschliche Verhalten als einem maßgebenden Faktor“ hinweist. Die Agentur berücksichtigt damit nicht einzig technische Sicherheitsaspekte, sondern erkennt auch den Menschen und die Organisation der Geschäfts- oder Verwaltungsprozesse als relevante Komponenten zur Herstellung einer angemessenen Systemsicherheit.

BITKOM und TeleTrusT fordern die Bundesrepublik Deutschland auf, sich um den Standort der Agentur zu bewerben.

BITKOM und TeleTrusT stehen für weitere Gespräche auf nationaler wie auch europäischer Ebene sowie für unterstützende Leistungen (sowohl hinsichtlich der Aufgabendefinition der Agentur als auch bei der kontinuierlichen Arbeitsprogrammgestaltung) gern zur Verfügung. In weiteren Gesprächen zwischen Industrie und Ministerien sollte die derzeit ungenaue Einbeziehung der Wirtschaft in das Arbeitsprogramm speziell den Arbeitsgruppen (Artikel 10, Arbeitsgruppen) konkretisiert werden.

Im Folgenden wird der Vorschlag der EU-Kommission und der daraus resultierende Verordnungstext für den EWR seitens BITKOM und TeleTrusT kommentiert.

Vorschlag der EU-Kommission

In folgenden Punkten liegt ein Verbesserungspotential hinsichtlich des Verordnungstextes vor:

(1) Seite 4, Abschnitt 3.1 Hintergrund

Es wird in dem Abschnitt dargestellt, dass eine europäische Regulierungsagentur gemäß den Rahmenbedingungen KOM(2002) 718 gegründet werden soll.

Wir befürchten, dass dadurch eine weitere (europäische) Regulierungsbehörde entsteht und der gewünschte harmonisierende Effekt durch die Konkurrenz zu den in den Mitgliedsstaaten etablierten Regulierungsbehörden verloren geht.

Die Erfahrungen in Deutschland zeigen, dass eine ausgeprägte Regulierung nicht automatisch zu einer Belebung des Marktes und zu einer Förderung innovativer Lösungen führt. Einschränkende Wirkungen überwiegen meist. Im Übrigen scheint durch die RegTP (in Deutschland) und vergleichbaren Behörden in anderen europäischen Staaten bereits ein ausreichendes Maß an Regulierung gegeben. Wie in Erwägungsgrund (9) der Verordnung des Europäischen Parlamentes und des Rates zutreffend dargestellt, müssen Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste ohnehin geeignete Maßnahmen ergreifen, um die Sicherheit ihrer Dienste und die Vertraulichkeit der Datenkommunikation zu gewährleisten. Außerdem können Doppelregulierungen und ggf. widersprüchliche Regulierungen entstehen, insbesondere dann, wenn in jedem EU-Mitgliedsstaat eine angereicherte und abgeänderte Regulierung umgesetzt wird. Regulierungen sollten, nur wenn es sinnvoll ist, auf internationaler Ebene erfolgen. Ansonsten sind Regulierungen national durchzuführen.

(2) Seite 5, Abschnitt 3.1 e)

Die Kommission muss die Arbeit der Agentur lenken können.

BITKOM und TeleTrusT empfehlen, die Transparenz bei der Auswahl inhaltlicher Arbeiten und Zuständigkeiten zu erhöhen. Die Lenkung durch die Kommission muss klar umrissen sein.

(3) Seite 6, Abschnitt 3.3.1 Ziele

Die Agentur muss bei der Durchführung von Gemeinschaftsmaßnahmen im Bereich der Netz- und Informationssicherheit Amtshilfe leisten können.

Hier ist zu befürchten, dass die Agentur in eine operative Arbeit verfällt, anstatt die Aufgaben wie im Verordnungstext Abschnitt 1, Artikel 2 zu erfüllen. Des Weiteren ist unklar, auf welcher formaljuristischen Grundlage Amtshilfe zu leisten sein wird. Aus dem Begriff Amtshilfe ergeben sich unterschiedliche Interpretationen, so dass dieser Abschnitt insgesamt nicht eindeutig definiert ist.
Der Beistand der Agentur soll für Interoperabilität der Sicherheitsfunktionen in Netzen und Informationssystemen sorgen. Dafür wären als technologische Basis z. B. ISIS-MTT, RFC 2401 oder das Modell der European Bridge-CA zur Nutzung vorhandener Teilstrukturen für die Umsetzung zu prüfen.

(4) Seite 7, Abschnitt 3.4.1, Management

Daher wird ein Verwaltungsrat vorgeschlagen, dessen Mitglieder vom Rat und von der Kommission benannt werden. Zwei Vertreter der Industrie werden auf Vorschlag der Kommission in den Verwaltungsrat aufgenommen, allerdings ohne Stimmrecht.

Die Agentur wird von einem Direktor geleitet. Er ist vom Verwaltungsrat auf Vorschlag der Kommission zu benennen.

Daher wird ein Beirat aus Sachverständigen für die Agentur vorgeschlagen, dessen Aufgabe es ist, die Zusammenarbeit … zu fördern.

Der Verwaltungsrat wird deutlich durch die Kommission bestimmt, was angesichts der Finanzierung der Agentur über die Kommission verständlich ist. Entscheidungen fallen im Verwaltungsrat paritätisch zwischen je 6 Vertretern des Rates und der Kommission. Es erscheint wenig sinnvoll, hier 2 Vertreter aus der Wirtschaft und einen Verbraucherschützer (alle ohne Stimmrecht) zusätzlich einzubeziehen. Unterließe man dies, wäre eine Verquickung von Interessen im Verwaltungsrat von vornherein auszuschließen.

TeleTrusT und BITKOM empfehlen, dass die Mehrheit der Sachverständigen für den Beirat aus dem Bereich der Wirtschaft rekrutiert werden sollte. Dabei sollten alle Mitglieder des Fachbeirates gleiche Stimmrechte besitzen.

Die Wirtschaft ist nicht nur Anbieter von Netzapplikationen und –diensten sondern auch Anwender. Damit notwendige Sicherheitsprodukte schnell und zu vernünftigen Preisen zur Verfügung stehen, muss sichergestellt werden, das die Industrie ihre Entwicklungs-kapazitäten auf die Entwicklung innovativer Lösungen konzentrieren kann, anstatt eine Vielzahl unterschiedlicher regulatorischer Forderungen umsetzen zu müssen. Außerdem wird die internationale Standardisierung und Normierung maßgeblich durch die Wirtschaft bestimmt. In diesem Zusammenhang ist es essentiell, eine enge Kooperation mit der Industrie anzustreben und dabei das bereits vorhandene Netzwerk aus Industrieverbänden und Standardisierungsorganisationen effektiv zu nutzen. Der Industrie ist der Mitbestimmungsraum zu gewähren, den sie braucht, um ihr ganzes Potenzial einbringen zu können.

(5) Seite 9ff, Abschnitt 3.8.1, Überprüfung

Zu prüfen ist insbesondere, inwieweit sich die mangelnde Beteiligung an der Durchsetzung von Rechtsvorschriften negativ auf die Wirksamkeit und Effizienz der Arbeit der Agentur ausgewirkt hat.

Sofern die Ausführung darauf abzielt, den Strafverfolgungsbehörden Durchgriff auf die Agentur zu gestatten, warnen wir vor den möglichen Folgen des Vertrauensverlustes in die Institution. Hier muss zwangsweise eine klare Aufgabentrennung vorliegen.

(6) Seite 16, Artikel 2 Aufgaben (c)

Aufbau eines Netzes für nationale und gemeinschaftliche Stellen.

BITKOM und TeleTrusT gehen davon aus, dass es sich hierbei, um ein „soziales Netz“ handelt und unterstützen diese Aufgabe.

Der Aufbau eines physikalischen Netzes kann nicht eine operative Aufgabe der Agentur sein. Sie sollte den Aufbau eines europäischen Netzes initiieren, wohlwollend begleiten und fördern. Wird solch ein Netzwerk von der Europäischen Kommission als relevant angesehen, muss mit dieser Aufgabe eine andere Organisationseinheit betraut werden. Wir empfehlen die Beteiligung der TK Industrie, da hier das notwendige Spezialwissen zur Verfügung steht.

(7) Seite 19, Artikel 5 Verwaltungsrat

Der Verwaltungsrat sorgt dafür, dass das Arbeitsprogramm den legislativen und politischen Prioritäten der Gemeinschaft im Bereich der Netz- und Informationssicherheit entspricht.

BITKOM und TeleTrusT empfehlen, die Agentur von politischen Strömungen zu entkoppeln. Nur so lässt sich ein nachhaltiger Aufbau und eine genügende Reputation für die Agentur erzielen.

Verordnungstext für den EWR

Derzeit ist unklar, welche Aufgaben die Agentur übernehmen soll. Sie sind eindeutig festzulegen.

Insgesamt scheint ein stark regulierender Ansatz vorhanden zu sein. Es ergibt sich der Anschein, dass die Agentur Einfluss auf Standardisierungsaktivitäten nehmen will. Es ist hier u. a. von einem Mangel an Interoperabilität die Rede, welcher den sachgerechten Einsatz von Sicherheitsprodukten und -diensten verhindere. In einem schnelllebigen und sehr innovativen Marktsegment wie der ITK-Technologie ist es bislang sehr kontraproduktiv gewesen, Zertifizierungspläne und Sicherheitsnormen von Regulierungsseite zu erstellen. Wir empfehlen dringend, in dem bereits jetzt schon annähernd überregulierten TK Bereich keine weiteren Regulierungen und Zertifizierungen zu verlangen, da ansonsten die Gefahr besteht, teure Lösungen am Marktbedarf vorbei zu implementieren. Sofern überhaupt weitere Regulierungen notwendig sind, sollten sie unter der Ägide der Industrie auf freiwilliger Basis erarbeitet werden. Des Weiteren existiert seitens der Industrie ein funktionierendes und bewährtes Netzwerk aus Standardisierungsgremien. Bei einer geeigneten, mitverantwortlichen Einbindung der Industrie in die Organisationsstruktur der Agentur würde sich ein regenerativer Rückkopplungsprozess ergeben, der die erforderlichen Standardisierungsanregungen unmittelbar an die relevanten (agenturunabhängigen) Standardisierungsgremien weitergeben würde.

Des Weiteren gewinnt man den Eindruck, dass das Aufgabengebiet der Agentur schleichend erweitert wird und sich jeglicher Kontrolle entzieht. Bei dem begrenzten Zeitraum von nur fünf Jahren sollte eine konkrete Definition der Aufgaben möglich sein, ohne damit einerseits innovative Entwicklungen auszugrenzen und andererseits durch eine permanent wachsende Anzahl von Aufgaben aufgrund von Öffnungsklauseln die vorhandenen Ressourcen zu zerstreuen.

BITKOM und TeleTrusT fordern, die Aufgaben der Agentur klar zu umreißen. Viele der angeführten Teilaufgaben deuten auf die Einrichtung eines europäisches CERT hin, was jedoch nach erläuternden Informationen gerade nicht Aufgabe der Agentur sein soll.

Artikel 2 „Aufgaben“ sollte deshalb wie folgt geändert werden:

Zur Verwirklichung der Ziele in Artikel 1 nimmt die Agentur folgende Aufgaben wahr:

(a) Erfassung und Analyse von Daten, einschließlich Informationen über derzeitige und absehbare Risken, insbesondere derer, die sich auf kritische Kommunikationsnetze und die auf diesem Weg abgerufenen und übertragenen Informationen auswirken;

wie folgt zu ändern:

(a) Erfassung und Analyse von Daten, einschließlich Informationen über jeweils aktuelle Risiken, insbesondere derer, die sich auf Kommunikationsnetze und in ihnen übertragenen Informationen auswirken

(b) Hilfeleistung und Stellungnahmen im Rahmen ihrer Ziele gegenüber der Kommission und anderen zuständigen Stellen;

wie folgt zu ändern:

(b) Hilfeleistung und Stellungnahmen im Rahmen ihrer Ziele gegenüber der Europäischen Kommission und anderen zuständigen Stellen, insbesondere auch nationalen Wirtschaftsvertretungen

(c) Förderung der Zusammenarbeit zwischen verschiedenen Akteuren im Bereich der Netz- und Informationssicherheit, u.a. durch Aufbau eines Netzes für nationale und gemeinschaftliche Stellen;

wie folgt zu ändern:

(c) Unterstützung der Zusammenarbeit zwischen verschiedenen Akteuren (Forschung, Industrie und Behörden) im Bereich der Netz- und Informationssicherheit

(d) Beitrag zur raschen, objektiven und umfassenden Informationsvermittlung in Fragen der Netz- und Informationssicherheit für alle Nutzer, u.a. durch Förderung des Austausches empfehlenswerter Verfahren zur Warnung der Nutzer, insbesondere von Warnsystemen gegen Computerangriffe, sowie der Synergie zwischen Initiativen des öffentlichen und des privaten Sektors;

wie folgt zu ändern:

(d) Förderung der Synergie zwischen Initiativen des öffentlichen und des privaten Sektors

(e) auf Anforderung der Kommission und der nationalen Regulierungsbehörden Unterstützung bei der Analyse der Einhaltung der im Gemeinschaftsrecht niedergelegten Anforderungen an Betreiber und Diensteanbieter hinsichtlich der Netz- und Informationssicherheit – einschließlich Anforderungen an den Datenschutz;

wie folgt zu ändern:

(e) Aktive Förderung der Selbstregulierung auf nationaler Ebene

(f) Beitrag zur Bewertung von Standards für Netz- und Informationssicherheit;

wie folgt zu ändern:

(f) Förderung der Interoperabilität von Lösungen der Netz– und Informationssicherheit insbesondere unter Berücksichtigung der Ergebnisse der Forschungsprogramme der Europäischen Union und auf Basis internationaler Standards

(g) Förderung der Risikobewertung und interoperabler Lösungen für das Risikomanagement innerhalb Organisationen;

wie folgt zu ändern:

(g) Förderung von Projekten zur Verbesserung der Risikobewertung und des Risikomanagements

(h) Beitrag zum Gemeinschaftskonzept der Zusammenarbeit mit Drittländern, einschließlich der Förderung der Kontakte zu internationalen Gremien;

keine Änderung

(i) Durchführung anderweitiger Aufgaben, die ihr von der Kommission im Rahmen ihrer Zielsetzungen zugewiesen werden.

Zu ersetzen durch:

(i) Unterstützung pragmatischer Ansätze im Sinne von Investitionssicherheit und der Wahrung von IT-Grundschutz (z.B. European Bridge-CA), die sich in Projekten bereits bewährt haben

(j) Beitrag zum Gemeinschaftskonzept der Zusammenarbeit mit Drittländern, einschließlich der Förderung der Kontakte zu internationalen Gremien

(k) Förderung der Umsetzung von Netz- und Informationssicherheitslösungen, die sich schon in Projekten bewährt haben

(l) Förderung von auf Zielgruppen orientierten „Awareness-Kampagnen“ zur IT-Sicherheit mit nationalen Industrievereinigungen/-verbänden (z. B. CERT-Bund - das "Computer Emergency Response Team" für deutsche Bundesbehörden, die vom BMI im Jahr 2000 eingesetzte Task Force "Sicheres Internet", die IT-Sicherheits-CD des BSI)

(m) Harmonisierung der grundlegenden IT-Sicherheitsanforderungen bei Services für den EU-Bürger

(n) Ansprechpartner bei der EU-weiten Vergabe von IT-Sicherheitsprojekten

(o) Identifizierung von Risiken und Konzeption von Schutzmaßnahmen, die aus transnationaler Vernetzung und – Abhängigkeit entstehen, aber bisher vorwiegend aus nationalem Blickwinkel betrachtet wurden

(p) Unterstützung bei der Analyse der Einhaltung der im Gemeinschaftsrecht niedergelegten Anforderungen an Betreiber, Diensteanbieter und Behörden hinsichtlich der Netz- und Informationssicherheit auf Anforderung der Europäischen Kommission, der nationalen Regulierungsbehörden und der nationalen Wirtschaftsvertretungen