I

*(Entschließungen, Empfehlungen und Stellungnahmen)*

# ENTSCHLIESSUNGEN

# RAT

## ENTSCHLIEBUNG DES RATES

**vom 18. Dezember 2009**

**über ein kooperatives europäisches Vorgehen im Bereich der Netz- und Informationssicherheit (NIS)**

(2009/C 321/01)

DER RAT DER EUROPÄISCHEN UNION —

I. IN ANBETRACHT:

1. der Mitteilung der Kommission vom 31. Mai 2006 mit dem Titel „Eine Strategie für eine sichere Informationsgesellschaft“, in der eine Strategie bestehend aus „Dialog, Partnerschaft und Delegation der Verantwortung“ vorgeschlagen wird, in die Mitgliedstaaten und Privatwirtschaft eingebunden sind,

2. der Mitteilung der Kommission vom 12. Dezember 2006 über ein Europäisches Programm für den Schutz kritischer Infrastrukturen, die auf den verbesserten Schutz kritischer Infrastrukturen in der Europäischen Union und auf die Schaffung eines Unionsrahmens für den Schutz kritischer Infrastrukturen abzielt,

3. der Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern,

4. der Entschließung des Rates vom 22. März 2007 zu einer Strategie für eine sichere Informationsgesellschaft in Europa,

5. der Schlussfolgerungen des Rates vom 19./20. April 2007 zu einem Europäischen Programm für den Schutz kritischer Infrastrukturen,

6. der Mitteilung der Kommission vom 30. März 2009 über den Schutz kritischer Informationsinfrastrukturen (CIIP),

7. der laufenden Debatte — einschließlich der entsprechenden öffentlichen Anhörung — über die Zukunft der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) und ihre Rolle beim Schutz kritischer Informationsinfrastrukturen,

8. der Schlussfolgerungen des Vorsitzes zum Schutz kritischer Informationsinfrastrukturen anlässlich der Ministerkonferenz vom 27./28. April 2009 in Tallinn,

9. der Lissabon-Ziele Wettbewerbsfähigkeit und Wachstum sowie der laufenden Beratungen über die Überarbeitung der Lissabon-Strategie,

10. der im Zuge der Überprüfung des Rechtsrahmens für elektronische Kommunikationsnetze und -dienste vorgeschlagenen Maßnahmen,

11. der Einschätzung in dieser Entschließung, dass — im Interesse der Effizienz der künftigen Politik im Bereich der Netz- und Informationssicherheit (NIS) — derzeit noch keine Schlüsse zu etwa erforderlichen Änderungen der ENISA-Verordnung gezogen wurden. Da sich die künftige NIS-Politik derzeit bei der Kommission noch im Prüfungsstadium befindet, sollte den Ergebnissen dieser Prüfung bezüglich etwaiger Änderungen der ENISA-Verordnung vor ihrer Veröffentlichung durch die Kommission mit dieser Entschließung nicht vorgegriffen werden;

II. EINGEDENK FOLGENDER ASPEKTE:

1. Angesichts der grundlegenden Bedeutung der elektronischen Kommunikationsinfrastrukturen und -dienste für Wirtschaft und Gesellschaft leistet die Netz- und Informationssicherheit (NIS) einen Beitrag zu wichtigen Werten und Zielen der Gesellschaft wie Demokratie, Schutz der Privatsphäre, Wirtschaftswachstum, ungehinderter Austausch von Ideen sowie wirtschaftliche und politische Stabilität.

2. Den informations- und kommunikationstechnologischen Systemen, Infrastrukturen und Diensten einschließlich des Internets kommt eine lebenswichtige Rolle für die Gesellschaft zu, und ihre Störung könnte schwere wirtschaftliche Schäden verursachen, was die Wichtigkeit von Maßnahmen zur Erhöhung des Schutzes und der Stabilität, mit denen die ununterbrochene Bereitstellung kritischer Dienste gewährleistet werden soll, noch unterstreicht.

3. Sicherheitszwischenfälle können das Vertrauen der Nutzer untergraben. Schwere Störungen von Netzen und Informationssystemen könnten zwar erhebliche wirtschaftliche und soziale Auswirkungen haben, aber auch alltägliche Probleme und Beeinträchtigungen können das Vertrauen der Allgemeinheit in Technologien, Netze und Dienste unterminieren.

4. Die Bedrohungslage wandelt und verschärft und macht es zunehmend notwendig, den Endnutzern, Unternehmen und staatlichen Stellen elektronische Kommunikationsinfrastrukturen zur Verfügung zu stellen, die belastbar und automatisch stabil sind, und zu ermitteln, mit welchen Anreizen die Anbieter hier am besten zu einem raschen Handeln veranlasst werden können.

5. Es ist notwendig, die NIS in allen Politikbereichen und in allen Sektoren der Gesellschaft zu verstärken und zu verankern und die Herausforderung zu meistern, dass durch Maßnahmen sowohl auf nationaler als auch auf europäischer Ebene für ein ausreichendes Maß an Fachkenntnissen gesorgt wird und die Nutzer der Informations- und Kommunikationstechnologien (IKT) entsprechend sensibilisiert werden.

6. Die Vollendung und das Funktionieren des Binnenmarkts erfordern es, dass Netzeigentümer und Diensteanbieter grenzübergreifend zusammenarbeiten, da etwaige Störungen in einem Mitgliedstaat auch andere Mitgliedstaaten und die Europäische Union insgesamt in Mitleidenschaft ziehen können.

7. Durch neue Nutzungsstrukturen wie „Cloud Computing" („Rechnen in der Wolke") und „Software as a Service" („Software als Dienst") wird die Bedeutung der Netz- und Informationssicherheit noch bekräftigt.

8. Die NIS dient dem Ziel aller interessierten Kreise in allen Bereichen der Gesellschaft, sich auf die Informationssysteme verlassen zu können; daher bedarf es eines sektoren- und grenzüberschreitenden Vorgehens.

9. Mit der zunehmenden Nutzung der IKT in der Gesellschaft ist die NIS eine Grundvoraussetzung für eine zuverlässige, sichere und gesicherte Erbringung öffentlicher Dienste wie etwa E-Verwaltung.

10. Die ENISA verfügt über das Potenzial, um auf der wichtigen Funktion, die sie für die Netz- und Informationssicherheit bereits wahrnimmt, aufbauen zu können —

III. WEIST AUF FOLGENDES HIN:

1. Es bedarf in der Europäischen Union eines hohen Maßes an Netz- und Informationssicherheit im Interesse

   a) der Freiheiten und Rechte der Bürger einschließlich des Rechts auf Schutz der Privatsphäre;

   b) der Effizienz in der Gesellschaft hinsichtlich der Qualität im Umgang mit Informationen;

   c) der Rentabilität und des Wachstums von Handel und Industrie;

   d) des Vertrauens der Bürger, Unternehmen und Einrichtungen in die Informationsverarbeitung und in die IKT-Systeme.

2. Der IKT-Sektor ist für die meisten Sektoren der Gesellschaft von überragender Bedeutung, weshalb alle Akteure einschließlich der Betreiber, Diensteanbieter, Hardware- und Softwareanbieter, Endnutzer, öffentlichen Stellen und einzelstaatlichen Regierungen eine gemeinsame Verantwortung für die Netz- und Informationssicherheit tragen;

IV. IST SICH DES FOLGENDEN BEWUSST:

1. der Bedeutung einer aktiven und sachkundigen europäischen NIS-Gemeinschaft, die zu einer verstärkten Zusammenarbeit zwischen den Mitgliedstaaten und der Privatwirtschaft beiträgt;

2. der Vorteile einer gegebenenfalls EU-weit harmonisierten Anwendung internationaler Sicherheitsstandards für die Zwecke der Netz- und Informationssicherheit;

3. der Notwendigkeit eines kooperativen europäischen Vorgehens im Bereich der Netz- und Informationssicherheit auf internationaler Ebene, da es sich um eine globale Herausforderung handelt;

4. des Umstands, dass die Mitgliedstaaten und die Organe der Europäischen Union über zuverlässige statistische Daten zum Stand der Netz- und Informationssicherheit in Europa verfügen müssen;

5. des Umstands, dass alle Akteure verstärkt sensibilisiert werden müssen und über Instrumente für das Risikomanagement verfügen müssen;

6. des Umstands, dass es verstärkter Anstrengungen unter den Mitgliedstaaten in Bezug auf Sensibilisierung, Austausch bewährter Verfahren und Orientierungshilfen für die Mitgliedstaaten bedarf;

7. der Bedeutung von Modellen, die — wie im Falle der Partnerschaften zwischen öffentlichem und privatem Sektor — mehrere Akteure einbinden und auf einem langfristig angelegten Bottom-up-Ansatz zur Entschärfung erkannter Risiken beruhen, sofern dies bei dem Bemühen um eine hohe Netzstabilität mit einem Zusatznutzen verbunden ist;

8. der entscheidenden Rolle, die die Anbieter bei der Bereitstellung belastbarer und stabiler elektronischer Kommunikationsinfrastrukturen für die Gesellschaft spielen;

9. des Nutzens europaweiter NIS-Simulationsübungen, die Netzbetreibern und Diensteanbietern sowie staatlichen Stellen wertvolle Erkenntnisse liefern können;

10. des Umstands, dass nationale oder staatliche IT-Notfalldienste oder andere der Abwehr von Bedrohungen und der Beseitigung von Schwachstellen dienende Reaktionsmechanismen zu hoher Stabilität und Abwehr- und Entstörungsbereitschaft in Bezug auf Netze und Informationssysteme beitragen können;

11. des Umstands, dass die strategischen Wirkungen, Risiken und Aussichten im Hinblick auf die Einrichtung von IT-Notfalldiensten für die Organe der Europäischen Union und die mögliche künftige Rolle der ENISA in dieser Frage untersucht werden müssen;

12. der von der ENISA auf dem Gebiet der Netz- und Informationssicherheit bisher geleisteten Arbeit und der Notwendigkeit, die ENISA zu einer effizienten Stelle weiterzuentwickeln, die für die Netz- und Informationssicherheit in Europa eindeutige Vorteile erbringt;

V. BETONT FOLGENDES:

1. Eine erweiterte und ganzheitliche europäische Strategie für Netz- und Informationssicherheit, bei der der Europäischen Kommission, den Mitgliedstaaten und der ENISA klar festgelegte Aufgaben zugewiesen werden, ist für die Bewältigung gegenwärtiger und zukünftiger Herausforderungen von ausschlaggebender Bedeutung.

2. Nach angemessener Konsultation und Analyse sollte im Gesetzgebungsprozess erwogen werden, die ENISA zu modernisieren und auszubauen und hierzu mit einem Mandat auszustatten, das einerseits Flexibilität bietet und die Aufsicht durch die Mitgliedstaaten und die Kommission sicherstellt und andererseits eine effiziente Rolle für die Vertretung der privatwirtschaftlichen Akteure gewährleistet. Dieses Mandat sollte dem Rechtsrahmen für elektronische Kommunikationsnetze und -dienste Rechnung tragen, den anspruchsvollen Vorgaben der Lissabon-Agenda entsprechen und Zielvorgaben für Forschung, Innovation, Wettbewerbsfähigkeit, Wirtschaftswachstum und Vertrauenssicherung einschließen.

3. Die ENISA könnte die Kommission und die Mitgliedstaaten in ihrer Politikgestaltungs- und Durchführungsaufgabe unterstützen — und zwar insbesondere beim Brückenschlag zwischen Technologie und Politik — und sollte eng mit den Mitgliedstaaten und anderen Akteuren zusammenarbeiten, damit ihre Tätigkeiten gründlich auf die Prioritäten der Europäischen Union abgestimmt sind.

4. Die ENISA sollte im Rahmen eines überarbeiteten Mandats als Kompetenzzentrum der Europäischen Union für EU-bezogene Netz- und Informationssicherheit dienen. Die Organe der Europäischen Union sollten als solche die Stellungnahme der Agentur einholen und so weit wie möglich berücksichtigen, wenn es um die Ausarbeitung und Durchführung von Strategien geht, die Auswirkungen auf dem Gebiet der Netz- und Informationssicherheit zeitigen könnten.

5. Die ENISA könnte ferner in die Lage versetzt werden, auf Anforderung die Mitgliedstaaten bei der Verbesserung ihrer eigenen NIS-Kapazitäten und bei der Stärkung ihrer Fähigkeit zur Bewältigung von Sicherheitszwischenfällen zu unterstützen;

VI. ERSUCHT DIE MITGLIEDSTAATEN:

1. mit Sensibilisierungskampagnen weiter an der Stärkung des Vertrauens der Endnutzer in die IKT zu arbeiten;

2. nationale NIS-Simulationsübungen abzuhalten und/oder an regulären europäischen NIS-Simulationsübungen teilzunehmen und dabei zu berücksichtigen, dass aufgrund der fachlichen Komplexität und der Einbeziehung der Privatwirtschaft umfangreiche Planungsarbeiten erforderlich sind. Auf Anforderung könnte die ENISA die Mitgliedstaaten diesbezüglich unterstützen. Umfang und geografische Abgrenzung der Übungen sollten sich im Laufe der Zeit organisch weiterentwickeln und sich an den ermittelten Risiken orientieren;

3. IT-Notfalldienste in denjenigen Mitgliedstaaten einzurichten, in denen es derartige Dienste noch nicht gibt, und die Zusammenarbeit zwischen den nationalen IT-Notfalldiensten auf europäischer Ebene auszubauen. Die ENISA könnte die Mitgliedstaaten diesbezüglich unterstützen;

4. ihre NIS-Maßnahmen im Rahmen von Ausbildungs-, Schulungs- und Forschungsprogrammen zu verstärken, damit in der Europäischen Union die erforderlichen technischen und beruflichen Kompetenzen verfügbar sind und eine stärkere Professionalisierung in diesem Bereich erzielt wird;

5. bei grenzüberschreitenden Zwischenfällen gemeinsam zu reagieren und ihre Fähigkeit zu angemessenem Vorgehen zu verbessern; hierzu muss der Dialog zwischen den beteiligten Entscheidungsträgern — insbesondere bezüglich der Geheimhaltung — ausgebaut werden;

VII. ERSUCHT DIE KOMMISSION:

1. die Mitgliedstaaten gegebenenfalls bei der Umsetzung dieser Entschließung zu unterstützen;

2. das Europäische Parlament und den Rat über die EU-Initiativen auf dem Gebiet der Netz- und Informationssicherheit regelmäßig zu unterrichten;

3. in Zusammenarbeit mit der ENISA eine an die europäische Öffentlichkeit und die Akteure der Privatwirtschaft gerichtete Sensibilisierungskampagne über die Wichtigkeit eines angemessenen NIS-Risikomanagements einzuleiten;

4. weiterhin im Benehmen mit den Mitgliedstaaten zu ermitteln, mit welchen Anreizen die Betreiber von elektronischen Kommunikationsinfrastrukturen dazu veranlasst werden können, den Endnutzern, Unternehmen und staatlichen Stellen belastbare und automatisch stabile Infrastrukturen bereitzustellen;

5. in Zusammenarbeit mit den Mitgliedstaaten Methoden zu entwickeln, die es gestatten, auf EU-Ebene eine vergleichende Bewertung der sozioökonomischen Auswirkungen von Zwischenfällen und der Effizienz der Präventivmaßnahmen vorzunehmen;

6. sich für multilaterale Modelle, die für Endnutzer und Industrie mit einem eindeutigen Zusatznutzen verbunden sein müssen, einzusetzen und an deren Verbesserung zu arbeiten;

7. eine ganzheitliche NIS-Strategie zu entwickeln, einschließlich [1] Vorschläge für ein verstärktes und flexibles Mandat für die ENISA sowie eine verstärkte Aufsicht seitens der Mitgliedstaaten und der Kommission;

8. in Zusammenarbeit mit den Mitgliedstaaten eine Untersuchung zu den IT-Notfalldiensten durchzuführen, um zu ermitteln, in welchen Bereichen eine weitergehende Zusammenarbeit angezeigt ist;

9. die Überlegungen über ein gemeinsames bzw. abgestimmtes Vorgehen der Organe der Europäischen Union bei der Beschaffung gesicherter IKT-Systeme und -Dienste fortzuführen;

VIII. FORDERT DIE ENISA AUF:

1. die Mitgliedstaaten, die Europäische Kommission und andere relevante Akteure bei der Verwirklichung der europäischen NIS-Politik und bei der Durchführung des CIIP-Aktionsplans weiterhin aktiv zu unterstützen;

2. mit den Mitgliedstaaten, der Kommission und den statistischen Ämtern bei der Entwicklung eines Rahmens für statistische Daten zum Stand der Netz- und Informationssicherheit in Europa zusammenzuarbeiten;

IX. ERSUCHT DIE BETROFFENEN AKTEURE:

1. ihre Bemühungen zur Verbesserung der Netz- und Informationssicherheit — insbesondere mit Blick auf die Bereitstellung zuverlässiger, vertrauenswürdiger und nutzerfreundlicher Produkte und Dienste — zu intensivieren;

2. die Nutzer ordnungsgemäß über die mit Produkten und Diensten verbundenen Sicherheitsrisiken und darüber zu unterrichten, wie sie sich selbst schützen können;

3. alle geeigneten technischen und organisatorischen Maßnahmen zu ergreifen, um die Kontinuität, Integrität und Vertraulichkeit bei elektronischen Kommunikationsnetzen und -diensten aufrechtzuerhalten;

4. in dem Streben nach harmonisierten und interoperablen Lösungen weiter an der Standardisierung der Netz- und Informationssicherheit zu arbeiten;

5. gemeinsam mit den Mitgliedstaaten an Simulationsübungen teilzunehmen, damit geeignete Notfallmaßnahmen gewährleistet sind.

---

[1] KOM schlägt vor, an dieser Stelle die Worte „gegebenenfalls auch“ einzufügen.