RAT DER EUROPÄISCHEN UNION

Brüssel, den 12. Mai 2011 (18.05)
(OR. en)

10003/11

TELECOM	**60**
DATAPROTECT	**48**
JAI	**308**
PROCIV	**64**

VERMERK

des	Vorsitzes
für den	AStV
Nr. Komm.dok.:	8548/11 TELECOM 40 DATAPROTECT 27 JAI 213 PROCIV38
Nr. Vordok.:	9753/11 TELECOM 55 DATAPROTECT 41 JAI 282 PROCIV 58
Betr.:	***VORBEREITUNG DER TAGUNG DES RATES (VERKEHR, TELEKOMMUNIKATION UND ENERGIE) AM 27. MAI 2011*** Entwurf von Schlussfolgerungen des Rates über den Schutz kritischer Informationsinfrastrukturen "Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit"

1. Die Kommission hat dem Rat am 1. April 2011 ihre Mitteilung über den Schutz kritischer Informationsinfrastrukturen – "Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit" – übermittelt.

2. Die Mitteilung enthält eine Bestandsaufnahme der Ergebnisse, die seit der Annahme des CIIP-Aktionsplans im Jahr 2009[1] erzielt wurden; mit dem Aktionsplan sollten Sicherheit und Robustheit kritischer Informations- und Kommunikations-Infrastrukturen erhöht werden. Außerdem werden in der Mitteilung die nächsten Schritte beschrieben, die die Kommission in Bezug auf die einzelnen Maßnahmen sowohl auf europäischer als auch auf internationaler Ebene vorschlägt.

[1] Der CIIP-Aktionsplan ist in der Mitteilung der Kommission vom 30. März 2009 über den "Schutz kritischer Informationsinfrastrukturen – Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität" enthalten.

3. Cybersicherheit und der Schutz kritischer Informationsinfrastrukturen sind eine wesentliche Voraussetzung dafür, dass Menschen und Unternehmen Vertrauen in das Internet und andere Netze haben, und sie sind eine zentrale Priorität der Digitalen Agenda für Europa[2]. Die CIIP-Mitteilung konzentriert sich auf die globale Dimension der Herausforderungen und die Bedeutung einer erheblich verstärkten Zusammenarbeit zwischen den Mitgliedstaaten und dem Privatsektor auf nationaler, europäischer und internationaler Ebene in Fragen der weltweiten Wechselbeziehungen. In der Mitteilung wird vorgeschlagen, koordinierte Maßnahmen zur Prävention, Erkennung und Eindämmung von Störungen aller Art – ob vom Menschen oder durch Naturereignisse verursacht – und zur entsprechenden Reaktion zu fördern und alle relevanten Akteure einzubeziehen.

4. Um das Problembewusstsein und die Abwehrbereitschaft in der gesamten EU zu erhöhen, schlägt die Kommission mehrere konkrete Maßnahmen vor. Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) spielt bei vielen dieser Maßnahmen eine wichtige Rolle. In der Mitteilung werden unter anderem Maßnahmen zur Förderung der Grundsätze für die Robustheit und Stabilität des Internets, zum Aufbau strategischer internationaler Partnerschaften und zur Einbringung koordinierter Beiträge in internationalen Foren sowie zur Verbesserung der Abwehrbereitschaft der EU vorgeschlagen.

5. Am 14./15. April 2011 hat der Vorsitz des Rates in Balatonfüred in Zusammenarbeit mit der Kommission eine Ministerkonferenz über den Schutz kritischer Informationsinfrastrukturen veranstaltet. Die Gruppe "Telekommunikation und Informationsgesellschaft" hat die Ergebnisse dieser Konferenz und die entsprechende Erklärung des Vorsitzes zur Kenntnis genommen. In der Erklärung des Vorsitzes wurde hervorgehoben, dass die Mitgliedstaaten ihre Bemühungen zum Ausbau der nationalen Fähigkeiten im Bereich der Netzsicherheit intensivieren müssen. Es wurde auch betont, wie wichtig es ist, die ENISA rasch zu reformieren, zu modernisieren und zu verstärken, um weiterhin den Herausforderungen gewachsen zu sein, und dass die Union ein hohes Maß an Netz- und Informationssicherheit benötigt.

---

[2] Dok. 9981/10.

6. Ein dauerhafter Schutz der europäischen kritischen Informationsinfrastrukturen ist von strategischer Bedeutung. In dem Entwurf der Schlussfolgerungen wird auf die Bedeutung hingewiesen, die dem Aufbau nationaler/staatlicher IT-Notfalldienste (Computer Emergency Response Teams – CERTs), der Ausarbeitung nationaler Notfallpläne für Netzstörungen sowie der Veranstaltung von nationalen Übungen zur Internetsicherheit zukommt. Im Hinblick auf die europäische Zusammenarbeit steht die Notwendigkeit im Mittelpunkt, Impulse für eine Zusammenarbeit zwischen den Mitgliedstaaten zu geben, indem Mechanismen für die Kooperation der Mitgliedstaaten bei Störfällen entwickelt und europaweite Übungen veranstaltet werden und der Dialog über Fragen im Zusammenhang mit der IKT-Sicherheit gefördert wird. Das Engagement der Mitgliedstaaten in internationalen Foren ist sehr wichtig. Im Sinne der Intensivierung der internationalen Zusammenarbeit im Bereich der globalen Netz- und Informationssicherheit und des Aufbaus strategischer internationaler Partnerschaften auf bilateraler und multilateraler Ebene werden die Mitgliedstaaten und die Kommission ersucht, sich bei ihren Arbeiten eng abzustimmen. Die ENISA wird in dem Schlussfolgerungsentwurf aufgefordert, die Mitgliedstaaten aktiv bei ihren Bemühungen zu unterstützen, ihre nationalen Fähigkeiten auszubauen und miteinander zusammenzuarbeiten. In diesem Zusammenhang betonen die Mitgliedstaaten, wie wichtig es ist, die ENISA rasch und angemessen zu modernisieren. Schließlich werden die Beteiligten ersucht, Aktionen zu initiieren, zu fördern und daran teilzunehmen, mit denen die Netz- und Informationssicherheit verbessert und der Schutz der Anwender und ihr Vertrauen in elektronische Kommunikationsnetze und -dienste gestärkt werden.

7. Die Gruppe "Telekommunikation und Informationsgesellschaft" hat den vorgeschlagenen Entwurf von Schlussfolgerungen in mehreren Sitzungen geprüft und eine grundsätzliche Einigung über den beigefügten Text erzielt. DK hat einen Parlamentsvorbehalt, während einige Delegationen und die Kommission noch an Prüfungsvorbehalten (siehe Anlage) festhalten.

8. Der AStV wird ersucht, den beigefügten Entwurf von Schlussfolgerungen zu prüfen, damit diese auf der Tagung des Rates (Verkehr, Telekommunikation und Energie) am 27. Mai 2011 angenommen werden können.

ENTWURF VON SCHLUSSFOLGERUNGEN DES RATES

über den Schutz kritischer Informationsinfrastrukturen
"Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit"[3]

DER RAT DER EUROPÄISCHEN UNION –

I. BEGRÜSST

die Mitteilung der Kommission vom 31. März 2011 über den Schutz kritischer Informationsinfrastrukturen – "Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit" –[4];

II. VERWEIST AUF

1. die Schlussfolgerungen des Rates vom 20. April 2007 zu einem Europäischen Programm für den Schutz kritischer Infrastrukturen[5],
2. die Richtlinie des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern[6],
3. die Mitteilung der Kommission vom 30. März 2009 über den Schutz kritischer Informationsinfrastrukturen – "Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität"–, in der ein Aktionsplan dargelegt wurde, mit dem die Sicherheit und Robustheit kritischer Informations- und Kommunikations-Infrastrukturen (IKT-Infrastrukturen) erhöht werden soll[7];
4. die Schlussfolgerungen des Vorsitzes zum Schutz kritischer Informationsinfrastrukturen anlässlich der Ministerkonferenz vom 27./28. April 2009 in Tallinn[8];

---

3 DK: Parlamentsvorbehalt; Kommission: allgemeiner Prüfungsvorbehalt.
4 Dok. 8548/11.
5 Dok. 7743/07.
6 ABl. L 345 vom 23.12.2008, S. 75-82.
7 Dok. 8375/09.
8 http://www.riso.ee/tallinnciip/
http://www.riso.ee/tallinnciip/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf

5. die einschlägigen Bestimmungen zur Informations- und Netzsicherheit des neuen Rechtsrahmens für elektronische Kommunikation[9];
6. die Entschließung des Rates vom 18. Dezember 2009 über ein kooperatives europäisches Vorgehen im Bereich der Netz- und Informationssicherheit (NIS)[10];
7. die Mitteilung der Kommission vom 19. Mai 2010 mit dem Titel "Eine digitale Agenda für Europa"[11], in der die Notwendigkeit hervorgehoben wird, die Sicherheit in der digitalen Gesellschaft zu verbessern und so für mehr Vertrauen in Netze zu sorgen;
8. die Schlussfolgerungen des Rates vom 31. Mai 2010 über die Digitale Agenda für Europa[12];
9. die Mitteilung der Kommission vom 22. November 2010 mit dem Titel "EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa"[13];
10. die Erklärung des Vorsitzes zum Schutz kritischer Informationsinfrastrukturen anlässlich der Ministerkonferenz vom 14./15. April 2011 in Balatonfüred[14];

III. IST SICH DES FOLGENDEN BEWUSST:

1. IKT-Systeme, -Infrastrukturen und -Dienste und insbesondere das Internet erhalten für die europäischen Bürger und Unternehmen und für die europäische Wirtschaft insgesamt immer größere Bedeutung, was zeigt, wie weit Europa in gesellschaftlicher, politischer und wirtschaftlicher Hinsicht von IKT abhängig ist, und außerdem deutlich macht, dass die Informatiksysteme und -netze gegen Störungen jeder Art, seien sie versehentlich oder vorsätzlich hervorgerufen, widerstandsfähig gemacht und abgesichert werden müssen.
2. Neben schweren Störungen von Netzen und Informationssystemen können auch Netzsicherheitsverletzungen das Vertrauen der Nutzer in Technik, Netze und Dienste erschüttern, so dass sie das volle Potenzial und die verbreitete Nutzung von IKT nicht mehr voll ausschöpfen können und entsprechend weniger zu Wirtschaftswachstum und einer besseren Lebensqualität beitragen.

---

9 ABl. L 337 vom 18.12.2009, S. 11-68.
10 Dok. 15841/09.
11 Dok. 9981/10.
12 Dok. 10130/10.
13 Dok. 16797/10.
14 http://www.eu2011.hu/document/presidency-statement-en-ministerial-conference-critical-information-infrastructure-protecti

3. Diesbezügliche Anstrengungen sollten nicht nur zur Generierung von Wachstum und zur Schaffung von Arbeitsplätzen beitragen, sondern die Union auch in die Lage versetzen, ihre vitalen Interessen wirksam zu schützen.
4. Die Risiken für IKT-Netze und -Dienste und insbesondere für das Internet durch neue und immer ausgeklügeltere Bedrohungen nehmen zu; ihnen kann unter anderem dadurch begegnet werden, dass auf der Grundlage gezielter Forschung und Innovation neue und technisch ausgereiftere selbstschützende Systeme entwickelt werden, aber sie machen einen wirksamen Schutz auch notwendiger denn je.
5. Der europäischen Wirtschaft kann durch Störungsanfälligkeit oder Störungen von IKT-Systemen,-Infrastrukturen und -Diensten großer Schaden entstehen, denn eine wesentliche Störung in einem Mitgliedstaat hat auch Auswirkungen auf andere Mitgliedstaaten und die gesamte EU.
6. Daher ist es im Rahmen eines gemeinsamen Ziels für Europa erforderlich, eine hohe Abwehrbereitschaft, Sicherheit und Robustheit zu fördern und zu unterstützen und die technischen Kompetenzen zu verbessern, damit Europa in der Lage ist, sich der Herausforderung des Schutzes von Netz- und Informationsinfrastrukturen zu stellen.
7. Bestehende allgemein anerkannte Mindestanforderungen, Grundsätze und Standards auf dem Gebiet der Netz- und Informationssicherheit müssen aufgegriffen und weiter-entwickelt werden, um konzeptionsintegrierte Sicherheit (security by design) sowie Produkte und Dienste zu fördern, die so weit wie möglich automatisch sicher (secure by default) sind.
8. Das Vertrauen und die Sicherheit aller beteiligten Akteure muss gefördert werden. Dies ist eine Voraussetzung für die Förderung einer verbesserten Zusammenarbeit beim Schutz lebenswichtiger Infrastrukturen und für das in der "Digitalen Agenda für Europa" festgelegte Ziel, die Informationstechnologie jedem europäischen Bürger zugänglich zu machen.
9. Angesichts der umfangreichen Nutzung von IKT und Internet durch Nutzer aller Art für alle erdenklichen Zwecke muss im Bereich der Netz- und Informationssicherheit kooperativ vorgegangen werden, um die Nutzer für die Sicherheitsproblematik zu sensibilisieren und ihnen diese Problematik bei der Nutzung bewusst zu machen.
10. Öffentliche und private Akteure müssen bei der Verbesserung ihrer eigenen Fähigkeiten und ihrer eigenen Abwehrbereitschaft im Hinblick auf die Prävention und Aufdeckung von Sicherheitsbedrohungen, die sich potenziell auf die Verfügbarkeit elektronischer Kommunikationsnetze und -dienste auswirken können, und im Hinblick auf ihre Reaktion auf solche Bedrohungen zusammenarbeiten und Verantwortung übernehmen.

11. Angesichts der Vernetzung der Systeme, Infrastrukturen und Dienste der Informations- und Kommunikationstechnologien muss das Ziel der Störungsprävention nicht nur auf nationaler und europäischer Ebene, sondern auch auf internationaler Ebene weltweit verfolgt werden;

IV. BETONT

1. die strategische Bedeutung der europäischen IKT- und NIS-Industrie im Hinblick auf einen nachhaltigen Schutz der europäischen kritischen Informationsinfrastrukturen;
2. im Hinblick auf die nationalen Fähigkeiten die Bedeutung, die dem Aufbau nationaler/staatlicher IT-Notfalldienste (Computer Emergency Response Teams – CERTs), der Ausarbeitung nationaler Notfallpläne für Netzstörungen sowie der Veranstaltung von nationalen Übungen zur Internetsicherheit zukommt;
3. im Hinblick auf die europäische Zusammenarbeit die Notwendigkeit, Impulse für eine Zusammenarbeit zwischen den Mitgliedstaaten zu geben, indem Mechanismen für die Kooperation der Mitgliedstaaten bei Störfällen entwickelt und europaweite Übungen veranstaltet werden, der Dialog über Fragen im Zusammenhang mit der IKT-Sicherheit (gegebenenfalls zum Beispiel über die für europäische kritische Infrastrukturen geltenden IKT-Kriterien) oder über die Stabilität und die Robustheit des Internets gefördert wird und gemeinsam mit der Privatwirtschaft Anreize für eine robuste IT-Sicherheitsindustrie geschaffen werden;
4. die beträchtlichen Fortschritte, die das Europäische Forum der Mitgliedstaaten (EFMS) bei der Förderung von Gesprächen und Austausch der Mitgliedstaaten untereinander sowie zwischen den Mitgliedstaaten und der Union über bewährte Maßnahmen für die Sicherheit und Robustheit von IKT-Infrastrukturen aufzuweisen hat;
5. die Bedeutung der Anstrengungen unterschiedlicher Akteure beispielsweise im Zusammenhang mit der europäischen öffentlich-privaten Partnerschaft für Robustheit (EP3R), bei der es sich um einen sich entwickelnden europaweiten Zusammenarbeitsrahmen für die Robustheit von IKT-Infrastrukturen handelt;
6. die bedeutende Rolle, die der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) in Bezug auf die von den Mitgliedstaaten sowie von öffentlichen und privaten Akteuren in der Union durchgeführten Maßnahmen im Bereich der Netz- und Informationssicherheit, insbesondere im Hinblick auf den Aufbau gut funktionierender nationaler/staatlicher IT-Notfalldienste (CERTs), zukommt;

7. den Erfolg der ersten europaweiten Übung zur Internetsicherheit vom 4. November 2010, die den gemeinsamen Willen zur grenzüberschreitenden Zusammenarbeit der Mitgliedstaaten unter Beweis gestellt hat;
8. den Nutzen, der für die Netz- und Informationssicherheit aus einer nationalen, europäischen und globalen Kultur der Risikoanalyse und des Risikomanagements auf allen Ebenen und durch alle Akteure entsteht, wobei deren Schwerpunkt auf der Unterstützung koordinierter Maßnahmen zur Prävention, Erkennung und Eindämmung von Störungen aller Art und zur entsprechenden Reaktion liegt;
9. die Chancen für die Wettbewerbsfähigkeit der Wirtschaft durch Nutzung des Potenzials neuer Erkenntnisse über Netz- und Informationssicherheitssysteme, insbesondere über Anwendungen, die auf konzeptionsintegrierter Sicherheit basieren, und über neue selbstschützende Systeme;
10. den potenziellen Nutzen einer weiteren Förderung eines kohärenten und kooperativen Konzepts für die Netz- und Informationssicherheit in den Mitgliedstaaten, den Organen der EU und der Privatwirtschaft mit der Unterstützung der ENISA;

V. HEBT HERVOR,

wie wichtig eine rasche und aufgabengerechte Modernisierung der ENISA ist, damit die Agentur ihre Aufgaben besser und gezielter wahrnehmen und weiter zur Verbesserung der Netz- und Informationssicherheit in Europa beitragen kann;

VI. ERSUCHT DIE MITGLIEDSTAATEN,

1. sich verstärkt um die Förderung einer Kultur des Risikomanagements sowie um die Förderung von Aus- und Fortbildungs- und Forschungsprogrammen im Bereich der Netz- und Informationssicherheit zu bemühen;
2. einen CERT einzurichten, falls sie eine solche Fähigkeit noch nicht aufgebaut haben;
3. die Zusammenarbeit zwischen bereits eingerichteten oder noch einzurichtenden nationalen/staatlichen CERTs und anderen international anerkannten CERTs, die in den Mitgliedstaaten tätig sind, zu fördern;
4. bis 2012 ein gut funktionierendes Netz von nationalen/staatlichen CERTs und anderen international anerkannten CERTs, die in den Mitgliedstaaten tätig sind, je nach Bedarf mit Unterstützung der ENISA, aufzubauen;

5. sich darüber zu verständigen, wie ein Europäisches Informations- und Warnsystem (EISAS) im Hinblick auf die Einrichtung nationaler Informations- und Warnsysteme durch die Mitgliedstaaten, gegebenenfalls mit Unterstützung der ENISA, aufgebaut werden kann;
6. die Annahme einer nationalen Strategie zur Netzsicherheit zu erwägen, sofern eine solche Strategie noch nicht vorhanden ist;
7. nationale Notfallplanungen im Hinblick auf Netzstörungen auszuarbeiten, um im Falle schwerwiegender Störungen handlungsfähig zu sein und gegebenenfalls Verbindung zu den Mitgliedstaaten aufnehmen zu können;
8. die Zusammenarbeit zwischen den Mitgliedstaaten zu fördern und – gestützt auf die nationalen Erfahrungen und Ergebnisse bei der Krisenbewältigung und in Zusammenarbeit mit der ENISA – bei der Ausarbeitung eines Europäischen Mechanismus zur Zusammenarbeit bei Netzstörungen mitzuwirken, der im Rahmen der nächsten "CyberEurope"-Übung im Jahr 2012 getestet werden sollte;
9. nationale oder grenzübergreifende Übungen zur Cyber-Sicherheit durchzuführen, um die Abwehrbereitschaft in Bezug auf Störungen der Netz- und Informationssicherheit zu testen und nach einem zweckmäßigen und durchführbaren Zeitplan in geeigneter Weise bei der Organisation von europäischen Übungen zur Cyber-Sicherheit und anderen Maßnahmen zum Aufbau von Kapazitäten in der Union mitzuwirken und daran teilzunehmen;
10. im Rahmen des EFMS und in Zusammenarbeit mit EP3R die Ausarbeitung der Kriterien für die Ermittlung europäischer kritischer Infrastrukturen im IKT-Sektor, insbesondere für Festnetz- und Mobilfunkkommunikation und für das Internet, fortzuführen;
11. einander bei grenzüberschreitenden Sicherheitsvorfällen auf freiwilliger Basis gegenseitig Hilfe zu leisten;
12. ihre Bemühungen um eine Intensivierung der internationalen Zusammenarbeit im Bereich der globalen Netz- und Informationssicherheit und um den Aufbau einer strategischen internationalen Partnerschaft auf bilateraler und multilateraler Ebene in internationalen Foren wie der OECD, den VN (ITU, IGF OSZE usw.), der NATO, dem Meridian-Prozess[15] usw. fortzusetzen und hierbei mit den Organen der Union zusammenzuarbeiten, indem sie sich beispielsweise in enger Abstimmung mit der Kommission an der Tätigkeit der Arbeitsgruppe EU-USA zum Thema Cybersicherheit und Cyberkriminalität beteiligen;[16]
13. Anreize für die Zusammenarbeit mit der Privatwirtschaft sowohl auf nationaler als auch auf europäischer Ebene zu geben und diese Zusammenarbeit zu unterstützen;

15 http://www.meridian2007.org/.

[16] GR hat einen Prüfungsvorbehalt und CY einen Vorbehalt zu diesem Punkt.

VII. ERSUCHT DIE KOMMISSION,

1. die Robustheit und Stabilität des Internets auf allen Ebenen in Zusammenarbeit mit öffentlichen und privaten Akteuren zu fördern;
2. ein kohärentes und effizientes NIS-Konzept der EU zu fördern, um Doppelarbeit zu vermeiden und ein gemeinsames Verständnis der verschiedenen bestehenden Herausforderungen sicherzustellen;
3. zusammen mit den Mitgliedstaaten und der ENISA die Einführung bestehender und die Weiterentwicklung allgemein anerkannter Mindestanforderungen, Grundsätze und Standards auf dem Gebiet der Netz- und Informationssicherheit zu fördern, um konzeptionsintegrierte Sicherheit (security by design) sowie Produkte und Dienste zu fördern, die so weit wie möglich automatisch sicher (secure by default) sind;
4. eng mit den Mitgliedstaaten zusammenzuarbeiten und ihre Bemühungen aufgrund dieser Schlussfolgerungen gegebenenfalls zu unterstützen;
5. die Bemühungen der Mitgliedstaaten im Rahmen des EFMS und der EP3R in Bezug auf die Arbeit an den Kriterien für die Ermittlung europäischer kritischer Infrastrukturen im IKT-Sektor, insbesondere für Festnetz- und Mobilfunkkommunikation sowie für das Internet, fortzuführen;
6. den Privatsektor so weit wie möglich in ihre Aktionen zur Förderung globaler Netz- und Informationssicherheit einzubeziehen;
7. ein ehrgeiziges FuE-Programm über die Sicherheit von Netzen und Informations-systemen sowie Anwendungen zu fördern und es wirksam mit den Abwehrplänen zum Schutz kritischer Informationsinfrastrukturen zu verknüpfen;
8. die Mitgliedstaaten bei ihren Bemühungen zu unterstützen, die Möglichkeit der Entwicklung eines Europäischen Mechanismus zur Zusammenarbeit bei Netzstörungen zu sondieren, der im Rahmen der nächsten "CyberEurope"-Übung im Jahr 2012 getestet werden sollte;
9. die Entwicklung der besten Verwaltungsstrategien für neu aufkommende Technologien von globaler Bedeutung (einschließlich Cloud-Computing) zu überwachen;

10. die Abwehrbereitschaft der EU zu stärken, indem ein CERT für die Organe der Union eingerichtet wird;
11. in enger Abstimmung mit den Mitgliedstaaten und zusammen mit den zuständigen Gremien der Union darauf hinzuwirken, dass die internationale Zusammenarbeit auf dem Gebiet der Netz- und Informationssicherheit mit relevanten internationalen Partnern und mit verschiedenen relevanten Foren wie der Arbeitsgruppe EU-USA zum Thema Cybersicherheit und Cyberkriminalität verstärkt wird;[17]
12. das Europäische Parlament und den Rat regelmäßig über die EU-Initiativen auf dem Gebiet der Netz- und Informationssicherheit zu unterrichten;

VIII. RUFT DIE ENISA AUF,

1. die Mitgliedstaaten weiterhin aktiv bei ihren Bemühungen zu unterstützen, ihre nationalen Fähigkeiten auszubauen und miteinander zusammenzuarbeiten;
2. ihr technisches Fachwissen auf dem Gebiet der Netz- und Informationssicherheit auszubauen und zu einem besseren Verständnis neuer Herausforderungen für die Netz- und Informationssicherheit in Europa beizutragen;

IX. ERSUCHT DIE BETEILIGTEN,

1. Aktionen zu initiieren, zu fördern und daran teilzunehmen, mit denen die Netz- und Informationssicherheit verbessert und der Schutz der Anwender und ihr Vertrauen in elektronische Kommunikationsnetze und -dienste gestärkt werden;
2. gemeinsame Anstrengungen mit öffentlichen Akteuren in Bezug auf Herausforderungen für die Netz- und Informationssicherheit zu unternehmen und die Bestimmung individueller Verantwortlichkeiten, insbesondere von Endnutzern, zu unterstützen;
3. sicherere und zuverlässigere IKT-Produkte und -Dienste sowie Hardware- und Software-Lösungen zu entwickeln und herzustellen und somit zum Schutz unserer Volkswirtschaften, die in hohem Maße von den IKT abhängig sind, beizutragen;
4. sich an öffentlich-privaten Partnerschaften zu beteiligen, um zur Entwicklung robuster und sicherer Netze sowie einer starken europäischen IT-Sicherheitsbranche beizutragen. Diese Partnerschaften sollten auch den Dialog unterschiedlicher Akteure und das Verständnis aller bestehenden Herausforderungen verbessern;

[17] PT: Prüfungsvorbehalt.

5. die Anwender für Risiken für die Netz- und Informationssicherheit zu sensibilisieren und sie zu informieren, wie sie diese Risiken am besten vermeiden und/oder darauf reagieren können;
6. die Mitgliedstaaten bei ihren Bemühungen zu unterstützen, nationale Notfallpläne für Netzstörungen zu erstellen und gegebenenfalls Übungen zur Cyber-Sicherheit durchzuführen;
7. alle geeigneten technischen und organisatorischen Maßnahmen zu ergreifen, um die Verfügbarkeit und Sicherheit elektronischer Kommunikationsnetze und -dienste aufrechtzuerhalten;
8. an der Erstellung und Einführung von Mindestanforderungen und international allgemein anerkannten Standards für die Netz- und Informationssicherheit mitzuwirken.