ARBEITSPROGRAMM 2010

Synergien nutzen – Fortschritte erzielen

ENDGÜLTIGE FASSUNG – 9.NOVEMBER 2009

Übersetzung. Das Englische Original bleibt die maßgebliche Fassung.

Inhaltsverzeichnis

1 EINLEITUNG 3

1.1. Beziehung zu früheren Versionen 3

1.2. Politischer Rahmen 3

1.3. Zentrale Herausforderungen 4

1.4. Die Rolle der ENISA 4

1.5. Mehrjahresplanung 5

2 THEMATISCHE MEHRJAHRESPROGRAMME 9

2.1. TMP 1: Verbesserung der Widerstandsfähigkeit der europäischen elektronischen Kommunikationsnetze 9

2.1.1 Arbeitspaket 1.1 – Unterstützung der Anstrengungen der Interessenvertreter bezüglich der Umsetzung der Leitfäden zu bewährten Verfahren für den Informationsaustausch und das Berichtswesen für Sicherheitsvorfälle 11
2.1.2 Arbeitspaket 1.2 – Unterstützung der Anbieter bei der Verbesserung der Widerstandsfähigkeit ihrer Netze 13
2.1.3 Arbeitspaket 1.3– Untersuchung innovativer Maßnahmen 15
2.1.4 Arbeitspaket 1.4 – Unterstützung der Interessenvertreter bei der ersten europaweiten Übung 18

2.2. TMP 2: Entwicklung und Fortführung von Kooperationsmodellen 20

2.2.1 Arbeitspaket 2.1 – Plattform für die Zusammenarbeit bei der Sensibilisierung 21
2.2.2 Arbeitspaket 2.2 – Sicherheitskompetenzkreis und Austausch bewährter Verfahren für die CERT-Gemeinschaft 23
2.2.3 Arbeitspaket 2.3 – Institutionalisierte Verbreitung europäischer bewährter Verfahren im Bereich der NIS 27

2.3. TMP 3: Ermittlung aufkommender Risiken zum Zwecke der Vertrauensbildung 30

2.3.1 Arbeitspaket 3.1– Konzept für die Bewertung und Diskussion aufkommender Risiken – Analyse konkreter Szenarien 32
2.3.2 Arbeitspaket 3.2 – Weiterführung der Rahmenstruktur für aufkommende Risiken 34
2.3.3 Arbeitspaket 3.3 – Förderung der nationalen Vorsorgemaßnahmen im Rahmen des Risikomanagements 35

2.4. VM1: „Internet der Zukunft“: Identität, Rechenschaftspflicht und Nutzervertrauen 37

2.4.1 VM: Arbeitspaket 1.1 – Bestandsaufnahme zu den Prozessen der Authentifizierung und des Schutzes der Privatsphäre 40
2.4.2 VM: Arbeitspaket 1.2 – Bestandsaufnahme zu den Dienstmodellen zur Unterstützung der elektronischen Dienste 42

2.5. VM 2: Ermittlung von Antriebskräften und Rahmenstrukturen für die EU-weite sektorale Zusammenarbeit auf dem Gebiet der NIS 43

2.5.1 VM: Arbeitspaket 2.1 – Anreize und Anforderungen im Zusammenhang mit der NIS-Rahmenstruktur für die Zusammenarbeit mehrerer Interessenvertreter in Gemeinschaften von IKT-Anbietern und –Nutzern 47

3 HORIZONTALE MASSNAHMEN 51

3.1. Entwicklung der Strategie und der Verwaltung der öffentlichen Angelegenheiten der ENISA 51

3.2. Verwaltung von Instanzen und Arbeitsgruppen der ENISA 51

3.3. Verwaltung der Beziehungen zu externen Interessenvertretern 51
3.4. Verwaltung der internen Kapazitäten 53
3.5. Verwaltung der internen Kommunikation der ENISA 53
3.6. Erstellung des Arbeitsprogramms 53
4 BERATUNG UND UNTERSTÜTZUNG 56
5 VERWALTUNGSTÄTIGKEITEN 57
5.1. Allgemeine Verwaltung 57
5.2. Finanzen 59
5.3. Humanressourcen 59
5.4. IKT 62
5.5. Rechtsfragen 63
5.6. Rechnungsführung 64
6 TÄTIGKEITEN DER DIREKTION 67
6.1 Beziehungen zu den griechischen Behörden 67
7 ANHANG 1 – OPERATIVE AKTIVITÄTEN IM ZUSAMMENHANG MIT DEM ARBEITSPROGRAMM 2010 68

1 EINLEITUNG

In diesem Arbeitsprogramm werden die thematischen Mehrjahresprogramme (TMP), die horizontalen Maßnahmen, die Beratungs- und Unterstützungsleistungen sowie die Verwaltungstätigkeiten der Europäischen Agentur für Netz- und Informationssicherheit (im Folgenden auch „die Agentur“) für das Jahr 2010 festgelegt und beschrieben. Das Arbeitsprogramm umfasst somit die Hauptaufgaben und den Haushaltsplan der Agentur für das Jahr 2010.

1.1. Beziehung zu früheren Versionen

In dieser Version des Arbeitsprogramms werden mehrere Änderungen berücksichtigt, die erst nach der Amtsübernahme des neuen Direktors der ENISA am 16. Oktober 2009 vereinbart wurden. Diese Änderungen lassen sich wie folgt zusammenfassen:

- eine Neuausrichtung der Organisation der ENISA gemäß der Mitteilung an den Verwaltungsrat vom 3. November 2009;
- eine höhere Priorisierung des TMP 1 sowie eine stärkere Beachtung der in der Mitteilung der Kommission vom 30. März 2009 (KOM(2009)149 endgültig) genannten Anforderungen;
- Herausnahme der europaweiten Erhebung über Informationssicherheit (Information Security Survey) aus dem Arbeitspaket 2.1;
- Streichung des Arbeitspakets 3.3 (Anwendung der Rahmenstruktur für aufkommende Risiken (Emerging and Future Risk Framework) bei den Interessenvertretern) aus dem TMP 3;
- stärkere Förderung der nationalen Vorsorgemaßnahmen im Rahmen des Risikomanagements zur weiteren Unterstützung des Aktionsplans zum Schutz kritischer Informationsinfrastrukturen (CIIP) (Arbeitspaket 3.4).

Diese Änderungen wurden auf Antrag von Mitgliedern des Verwaltungsrats vorgenommen, die eine stärkere Ausrichtung auf die Schwerpunktmaßnahmen gewünscht haben.

1.2. Politischer Rahmen

In der Mitteilung der Kommission „i2010 – Eine europäische Informationsgesellschaft für Wachstum und Beschäftigung“[1] wird die Bedeutung der Netz- und Informationssicherheit für die Schaffung eines einheitlichen europäischen Informationsraums hervorgehoben. Die Verfügbarkeit, Zuverlässigkeit und Sicherheit von Netzen und Informationssystemen spielen für unsere Wirtschaft und Gesellschaft zunehmend eine Schlüsselrolle.

In der Mitteilung „Eine Strategie für eine sichere Informationsgesellschaft“ [2] wird darauf verwiesen, dass eine sichere Informationsgesellschaft auf einer erhöhten Netz- und Informationssicherheit (NIS) und einer weitverbreiteten Sicherheitskultur aufbauen muss. Dies kann nur durch einen dynamischen und integrierten Ansatz erreicht werden, der alle Beteiligten einbezieht und auf Dialog, Partnerschaft und Delegation der Verantwortung setzt. Es muss jedoch betont werden, dass die Schaffung einer leistungsfähigen Kultur der Netz- und Informationssicherheit für alle Beteiligten eine große Herausforderung darstellt.

[1] KOM(2005) 229 endgültig, 1.6.2005.
[2] KOM(2006) 251 endgültig, 31.5.2006.

In einer Entschließung vom Dezember 2006[3] hat der Rat die Agentur aufgefordert, die Strategie der Europäischen Kommission im Rahmen des in der Gründungsverordnung der ENISA festgelegten Auftrags zu unterstützen. Zu diesem Zweck richtet die ENISA ihre Strategie und ihre Jahresarbeitspläne an der Strategie der Europäischen Kommission aus. Um die Wirkung ihrer Maßnahmen zu erhöhen, wird die Agentur im Rahmen eines zielgerichteten und zweckdienlichen Ansatzes bestehende Synergien und Initiativen auf nationaler sowie europäischer Ebene nutzen.

In ihrer Mitteilung „Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität“ [4] vom 30. März 2009 ruft die Kommission die ENISA zur Unterstützung der Kommission und der Mitgliedstaaten bei der Umsetzung des vorgeschlagenen Aktionsplans zur Stärkung der Sicherheit und Robustheit der kritischen Informationsinfrastrukturen (KII) auf. Mit dem vorliegenden Arbeitsprogramm kommt die ENISA dieser Aufforderung insbesondere im Rahmen des TMP 1 nach; jedoch umfassen auch die TMP 2 und 3 Maßnahmen zur Unterstützung dieses Aktionsplans.

1.3. Zentrale Herausforderungen

Da Angreifer sich immer auf die größte Schwachstelle in einem System konzentrieren, besteht die größte Herausforderung für die moderne Informationssicherheit nach wie vor darin, eine kohärente Antwort auf die aufkommenden Bedrohungen für die Netz- und Informationssicherheit zu finden, die alle Akteure dazu verpflichtet, an der Erarbeitung und Umsetzung eines globalen Ansatzes zur Sicherung der Infrastruktur und zur Reaktion auf Vorfälle mitzuwirken.

Eine solche kohärente Antwort erfordert eine Struktur, die zu gemeinschaftlichen Maßnahmen ermutigt und allen relevanten Interessenvertretern die Möglichkeit bietet, gemeinsam entsprechende Prioritäten und Methoden zu erarbeiten, um so eine einheitliche angemessene Netz- und Informationssicherheit in Europa sicherzustellen. Die Notwendigkeit eines gemeinsamen Vorgehens besteht umso mehr aufgrund der äußerst dynamischen Anwendungsumgebung, die laufend erweitert und durch neue Dienste für die Wirtschaft und die Regierung ergänzt wird.

Bei der Erarbeitung und Umsetzung eines solchen Ansatzes muss immer auch den sich rasch ändernden technischen Entwicklungen, wie der Funkfrequenzkennzeichnung (RFID), dem „Internet der Dinge“ und dem „Internet der Zukunft“, Rechnung getragen werden; gleichzeitig dürfen jedoch auch andere wichtige Tendenzen und Herausforderungen, darunter die Computerkriminalität aus finanziellen Gründen und politisch motivierte Cyber-Angriffe, nicht außer Acht gelassen werden.

Zwar zählt auch die Sicherstellung des technologischen Fortschritts weiterhin zu den technischen Herausforderungen, höchste Priorität hat jedoch die Schaffung einer proaktiven Sicherheitskultur. Hierbei sind wiederum mehrere Faktoren zu berücksichtigen, beispielsweise die Beteiligung vieler Interessenvertreter (Multi-Stakeholder-Environment), Lücken im Bereich der Bildung, noch nicht ausgereifte und optimierte Geschäftsmodelle, das unterschiedliche Niveau der Fähigkeiten der Mitgliedstaaten in diesem Bereich sowie die Angleichung der Gesetze und die weltweite Relevanz der Thematik und Probleme im Zusammenhang mit der Netz- und Informationssicherheit.

1.4. Die Rolle der ENISA

Aufgrund ihrer speziellen Rolle kann die ENISA die Mitgliedstaaten in besonderer Weise bei der Verbesserung ihrer Fähigkeiten auf dem Gebiet der Netz- und Informationssicherheit beraten und unterstützen. Dank ihrer Unabhängigkeit kann die Agentur fundiert und objektiv beraten und im

[3] 15768, 1.12.2006.
[4] KOM(2009) 149 endgültig.

Rahmen der Unterstützung der Mitgliedstaaten und der Kommission eine Schlüsselrolle übernehmen, um den Austausch von bewährten Verfahren und Informationen zwischen allen Interessengruppen auf europäischer Ebene zu erleichtern und so Ergebnisse und Wirkung zu optimieren.
Die Agentur fördert den offenen Dialog zwischen allen Beteiligten und unterhält zu diesem Zweck enge Beziehungen zu Industrie, Wissenschaft und Forschung und den Nutzern. Darüber hinaus knüpft und vertieft sie Kontakte zu einem Netz nationaler Verbindungspersonen (National Liaison Officers, NLO) sowie über die Ad-hoc-Arbeitsgruppen auch zu anderen wichtigen Experten. Weniger formell, aber ebenso effizient ist die Zusammenarbeit in den virtuellen Expertengruppen und Plattformen, über die Empfehlungen von Experten zusammengetragen und verbreitet und der Informationsaustausch mit und zwischen Akteuren des öffentlichen und privaten Sektors gefördert werden.

Mit ihrer Fähigkeit, schnell, neutral und fachlich kompetent auf Anfragen von EU-Institutionen und zuständigen Stellen der Mitgliedstaaten zu reagieren, nimmt die Agentur eine Mittlerrolle zwischen der EU und den nationalen Institutionen ein. Diese Rolle ist ein besonderes Merkmal der ENISA, die derzeit weltweit die einzige Einrichtung dieser Art ist.

Durch den kontinuierlichen Ausbau der Kontakte zu Drittländern in aller Welt sowie zu internationalen Einrichtungen (z. B. ITU, IETF, OASIS, OECD) soll außerdem eine umfassendere Beteiligung am weltweiten Dialog erreicht werden. Auf diese Weise sollen die Positionen wichtiger ausländischer Akteure stärker berücksichtigt und die europäischen Ansätze gefördert werden.

1.5. Mehrjahresplanung

Der Verwaltungsrat hat die Agentur angewiesen, sich angesichts ihres Auftrags und der begrenzten Ressourcen auf eine realistische Auswahl strategischer Prioritäten zu konzentrieren. Durch die gezielte Ausrichtung ihrer Arbeit will die Agentur in den Kernbereichen größere Fortschritte erzielen. Um dies zu erreichen, wird die Agentur bestehende Aktivitäten auf nationaler und EU-Ebene wirksam nutzen, Arbeitsüberschneidungen vermeiden und die Ergebnisse optimieren. Zu den Aktivitäten auf europäischer Ebene gehören unter anderem die Forschung zum Schutz kritischer Informationsinfrastrukturen innerhalb des vorrangigen Themenbereichs „Technologien für die Informationsgesellschaft“ des 6. Rahmenprogramms (IST FP6), das Rahmenprogramm für Wettbewerbsfähigkeit und Innovation, die IKT-Priorität im 7. Forschungsrahmenprogramm sowie das Programm IDABC (Interoperabilität europaweiter elektronischer Behördendienste für öffentliche Verwaltungen, Unternehmen und Bürger). Die enge Zusammenarbeit mit diesen Initiativen, die Nutzung ihrer Ergebnisse, die Interaktion mit den beteiligten Akteuren und ihre Einbindung in die Arbeit der ENISA gehört zu den Kernzielen des vorliegenden Arbeitsprogramms.

Die Agentur verfolgt ein mehrjähriges Arbeitsprogramm, um die angestrebte Wirkung zu erreichen und Synergien nutzen zu können. Im Vordergrund dieses Arbeitsprogramms stehen die Umsetzung der vom Verwaltungsrat vorgegebenen vorrangigen Ziele [5] und die Konzentration der

[5] Die vorrangigen Ziele der Agentur sind:
- Stärkung des Vertrauens in das Informationszeitalter durch die Anhebung des Niveaus der NIS in der EU;
- Förderung des Binnenmarkts für elektronische Kommunikation durch die Unterstützung der Institutionen bei der Festlegung einer geeigneten Mischung aus Gesetzesvorschriften und anderen Maßnahmen (unter besonderer Berücksichtigung des wichtigen Beitrags, den die Agentur zur Rahmenrichtlinie leisten kann);
- Intensivierung des Dialogs über NIS zwischen den verschiedenen Akteuren in der EU;
- Ausweitung der Zusammenarbeit zwischen den Mitgliedstaaten mit dem Ziel, die unterschiedlichen Fähigkeiten der Mitgliedstaaten auf diesem Gebiet auf ein einheitliches Niveau zu bringen;
- Unterstützung der Mitgliedstaaten und Bearbeitung der Unterstützungsersuchen von Mitgliedstaaten.

Anstrengungen auf ausgewählte strategische Prioritäten, die sogenannten thematischen Mehrjahresprogramme (TMP). In diesen Programmen werden die Arbeitsschwerpunkte der Agentur für mehrere Jahre festgelegt. Für jedes Programm werden mehrere sogenannte SMART[6]-Ziele bestimmt. Diese Ziele beziehen sich auf die angestrebten Ergebnisse und Wirkungen und können während der Laufzeit des Programms anhand von wichtigen Leistungsindikatoren (Key Performance Indicators, KPI) bewertet und überwacht werden.

Die thematischen Programme bestehen aus mehreren Arbeitspaketen (AP) zur Umsetzung der SMART-Ziele der TMP. In den einzelnen Arbeitspaketen sind die Aufgaben, die beteiligten Akteure, die angestrebten Ergebnisse und die erforderlichen Ressourcen festgelegt.

Die Arbeitspakete können sich auf einen Zeitraum von mehreren Jahren beziehen. Da die TMP im Rahmen des jährlichen Arbeitsprogramms der Agentur durchgeführt werden, betreffen die angegebenen Ressourcen und Haushaltsmittel jedoch nur die jeweiligen Maßnahmen, Ergebnisse und Tätigkeiten eines bestimmten Jahres. Die angegebenen Haushaltsmittel beziehen sich auf externe Aktivitäten, z. B. Workshops, Konferenzen oder Beratungsdienste. Die personellen Ressourcen beziehen sich auf die von den Experten der Agentur geleistete Arbeit.

Darüber hinaus können die Arbeitsprogramme auch vorbereitende Maßnahmen (VM) beinhalten. Eine VM ist eine Maßnahme mit einer Laufzeit von einem Jahr, in deren Rahmen geprüft wird, ob ein neues thematisches Mehrjahresprogramm durchgeführt werden kann. Sobald die Ergebnisse aus der VM verfügbar sind, kann eine diesbezügliche Entscheidung getroffen werden.

Das Arbeitsprogramm 2008 der Agentur enthielt drei TMP und eine VM. Im Jahr 2009 liegt der Schwerpunkt erneut auf den drei bestehenden TMP, die Folgemaßnahmen zu der VM hingegen wurden als Arbeitspakete (AP) in eines dieser TMP integriert. Im Einklang mit den Ergebnissen aus dem informellen Workshop von Verwaltungsrat/SGI, der im Juni 2009 stattfand, wird sich die Agentur auch im Jahr 2010 auf diese drei TMP konzentrieren und zusätzlich zwei neue VM einführen, die im Folgenden kurz beschrieben werden. Das nächste Kapitel enthält eine ausführliche Beschreibung der TMP, der VM sowie der einzelnen AP. Die für 2010 vorgeschlagenen AP beinhalten eigene SMART-Ziele und Leistungsindikatoren (Key Performance Indicators, KPI), die als erster Schritt zur Erreichung der jeweiligen SMART-Ziele betrachtet werden.

TMP 1: Verbesserung der Widerstandsfähigkeit der europäischen elektronischen Kommunikationsnetze

Schwerpunkte dieses TMP waren 2008 die Bestandsaufnahme, die Ermittlung bewährter Verfahren und eine Schwachstellenanalyse der Maßnahmen der einzelstaatlichen Regulierungsbehörden (National Regulatory Authorities, NRA) und der Netzbetreiber und Diensteanbieter. Im TMP 1 wurde außerdem untersucht, ob die derzeit verwendeten Backbone-Internet-Technologien geeignet sind, um die Integrität und Stabilität von Netzen zu gewährleisten. Im Jahr 2009 wurden im Rahmen des TMP 1 die Ergebnisse mit ähnlichen internationalen Erfahrungen und Erkenntnissen verglichen, Leitlinien herausgegeben und schließlich nach ausführlichen Konsultationen mit den beteiligten Interessenvertretern gemeinsame Empfehlungen formuliert. *Im Jahr 2010 wird sich die Arbeit der Agentur auf diesem Gebiet insbesondere auf Unterstützungsleistungen für die in der jüngsten Mitteilung der Kommission über den Schutz kritischer Informationsinfrastrukturen vom März 2009 beschriebenen Maßnahmen konzentrieren.*

[6] SMART (Specific, Measurable, Agreed, Realistic and Time bound) steht als Abkürzung für „spezifisch, messbar, abgestimmt, realistisch, termingerecht".

TMP 2: Entwicklung und Fortführung der Zusammenarbeit zwischen Mitgliedstaaten

Im Jahr 2008 war dieses TMP folgenden Bereichen gewidmet: a) der Ermittlung europaweiter Kreise für Sicherheitsfachwissen zu Themen wie Sensibilisierung und Reaktion auf Vorfälle und b) der institutionalisierten Verbreitung europäischer bewährter Verfahren im Bereich der NIS[7]. Im Jahr 2009 wurde für die Dauer von einem Jahr eine Maßnahme zur Verbesserung des Kapazitätenaufbaus von Kleinstunternehmen im Bereich der NIS hinzugefügt. 2010 sollen die Zusammenarbeit zwischen den Mitgliedstaaten ausgeweitet und neue Möglichkeiten für eine internationale Zusammenarbeit ermittelt werden, mit dem Ziel, die Fähigkeiten aller Mitgliedstaaten zu verbessern und das Niveau in Bezug auf die Kohärenz des NIS-Ansatzes europaweit anzuheben. Aufgrund ihrer begrenzten Ressourcen wird die Agentur eng mit den Dienststellen der Kommission zusammenarbeiten, um auf diese Weise mit geringstem Aufwand optimale Ergebnisse erzielen zu können.

TMP 3: Ermittlung aufkommender Risiken zum Zwecke der Vertrauensbildung

Die Agentur hat eine Rahmenstruktur entwickelt, die den Entscheidungsträgern helfen soll, die mit neuen Technologien und Anwendungen verbundenen aufkommenden Risiken besser zu verstehen und zu beurteilen. Eines der Hauptziele dieser Rahmenstruktur besteht darin, das gegenseitige Vertrauen der Akteure im Umgang mit diesen aufkommenden Risiken zu stärken. Im Jahr 2008 hat die Agentur zu diesem Zweck einen Machbarkeitsnachweis für eine europäische Kapazität zur Bewertung von Risiken entwickelt, die in zwei bis drei Jahren auftreten könnten, der in ein Forum von Interessenvertretern für den Dialog mit allen beteiligten Entscheidungsträgern des öffentlichen und privaten Sektors eingebunden ist. Im Jahr 2009 wurde der Machbarkeitsnachweis geprüft und mit dem Ziel weiterentwickelt, ihn im Folgejahr in den Mitgliedstaaten umzusetzen. Die Agentur erstellt auch weiterhin Risikobewertungsberichte, in denen sie zu aufkommenden Risiken, die mit neuen Technologien und Anwendungen verbunden sind, Stellung nimmt. Darüber hinaus befasst sich die Agentur mit Themen im Zusammenhang mit dem „Internet der Zukunft“ (Rechenschaftspflicht und Nutzervertrauen). Auf diese Weise soll das vorliegende TMP Entscheidungsträgern in Europa und gegebenenfalls auch in anderen Ländern helfen, absehbare Risiken frühzeitig zu erkennen.

VM 1: „Internet der Zukunft“: Identität, Rechenschaftspflicht und Nutzervertrauen

Im Rahmen der neuesten Entwicklungen im Bereich des Internets hat nun jeder die Möglichkeit, neben seinem realen Leben auch eines oder mehrere Leben in der virtuellen Welt zu führen. Die immer stärkere Verknüpfung dieser beiden Welten und die Bereitstellung von Informationen aus der realen Welt für die Dienste im Internet sind eine Tendenz, die in den letzten Jahren zunächst nur in der Wissensgemeinschaft zu beobachten war, nun aber zunehmend auch Eingang in kommerzielle Angebote findet. Eine weitere, parallel dazu verlaufende Entwicklung ist das sogenannte „Internet der Dinge“, das auf der RFID-Technologie aufbaut und mit RFID-Tags versehene Objekte über Aktoren und Sensoren elektronisch miteinander vernetzt. Als Reaktion auf diese Entwicklungen besteht das übergreifende Ziel dieser vorbereitenden Maßnahme darin, das hohe Sicherheitsniveau sowie das Vertrauen der Nutzer und der Industrie in die IKT-Infrastruktur und die bereitgestellten Dienste in Europa zu stärken und gleichzeitig die Gefahren für die bürgerlichen Freiheiten und die Privatsphäre soweit wie möglich zu beseitigen.

[7] Diese Plattform ist eine Folgemaßnahme der 2007 geleisteten Arbeit zur Festlegung eines Fahrplans für die institutionalisierte Verbreitung europäischer bewährter Verfahren im Bereich der NIS.

VM 2: Ermittlung von Antriebskräften und Rahmenstrukturen für die EU-weite sektorale Zusammenarbeit auf dem Gebiet der NIS

Da immaterielle Vermögenswerte für die Wertschöpfung in Unternehmen zunehmend an Bedeutung gewinnen, sind allgemeine wirtschaftliche und operative Anreize für den Ausbau der Zusammenarbeit des öffentlichen und des privaten Sektors beim Umgang mit Herausforderungen auf dem Gebiet der Netz- und Informationssicherheit mehr und mehr erforderlich. Es ist ein stärker auf Vorbeugung ausgerichteter Ansatz einzuführen, da traditionelle Schutzmechanismen nicht mehr ausreichen, um Angreifer davon abzuhalten, einzudringen und wichtige Informationen zu stehlen oder zu beschädigen. Dieser Ansatz sollte einen allgemeinen Rahmen enthalten, der auf die unterschiedliche organisatorische Ausrichtung der Akteure des öffentlichen und des privaten Sektors verweist und die Unterschiede bei den Lieferketten hervorhebt; Grundlage für diesen Rahmen sollte eine realistische Bewertung der Fähigkeiten der Beteiligten bezüglich des Umgangs mit den Herausforderungen der Netz- und Informationssicherheit bilden, wobei die jeweiligen rechtmäßigen Verantwortlichkeiten und Zuständigkeiten für kommerzielle oder öffentliche Dienste berücksichtigt werden.

Im Rahmen dieser VM soll geklärt werden, *wie* die betroffenen Akteure von einer Beteiligung an einer europaweiten gemeinschaftlichen Maßnahme zum Umgang mit den Herausforderungen der Netz- und Informationssicherheit überzeugt werden können.

Darüber hinaus wird die Agentur weiterhin verschiedene horizontale Maßnahmen durchführen, z. B. in den Bereichen Kommunikation und Einbindung, Sekretariat für ENISA-Gremien, Beziehungen zu externen Interessenvertretern (EU-Einrichtungen, Mitgliedstaaten, Industrie, Hochschulen, Verbraucher, internationale Einrichtungen und Drittländer), Verwaltung der internen Kapazitäten der Agentur, interne Kommunikation und Erstellung des Arbeitsprogramms.

Ferner wird die Agentur auf Ersuchen weiterhin Beratungs- und Unterstützungsleistungen erbringen. Die Verwaltungsabteilung der Agentur ist für die Bereiche allgemeine Verwaltung, Finanzen, Personal, IKT, Rechtsfragen und das Beschaffungswesen zuständig. Im Bereich der Laufbahnentwicklung stehen der Agentur verschiedene Instrumente wie die Einstufung in Besoldungsgruppen, Beförderungen, Fortbildung und Aufstiegsmöglichkeiten innerhalb der Agentur zur Verfügung.

2 THEMATISCHE MEHRJAHRESPROGRAMME

2.1. TMP 1: Verbesserung der Widerstandsfähigkeit der europäischen elektronischen Kommunikationsnetze

BEZEICHNUNG DES PROGRAMMS
TMP 1: Verbesserung der Widerstandsfähigkeit der europäischen elektronischen Kommunikationsnetze
BESCHREIBUNG DES PROBLEMS
Die Verfügbarkeit, Integrität und Kontinuität öffentlicher Kommunikationsnetze hat in einem konvergierenden Umfeld einer festen und mobilen Infrastruktur einen wichtigen Stellenwert. Die Verknüpfung und Vernetzung aller Bereiche bietet viele Vorteile, birgt aber auch zusätzliche Sicherheitsrisiken. Aufgrund der vielschichtigen gegenseitigen Abhängigkeit kann eine Störung in einer Infrastruktur leicht auf andere Infrastrukturen übergreifen und europaweite Auswirkungen entfalten. Der internationale Charakter der Telekommunikationsnetze erfordert ein gemeinsames Handeln in Bereichen wie der Widerstandsfähigkeit und Sicherheit von Netzen. Einige Mitgliedstaaten haben bereits Strategien, Politiken und ordnungspolitische Maßnahmen entwickelt oder sind dabei es zu tun, um diese Probleme in den Griff zu bekommen. Die meisten dieser Strategien basieren auf der Zusammenarbeit mit den Diensteanbietern, dem Informationsaustausch über Vorfälle und drohende Gefahren, der Entwicklung bewährter Verfahren und Vorsorgemaßnahmen und dem Test im Rahmen von Übungen. Trotz dieser Anstrengungen bietet Europa in Bezug auf die Verpflichtungen und Anforderungen, mit denen die Sicherheit und Widerstandsfähigkeit solcher Netze sichergestellt und verbessert werden soll, ein sehr uneinheitliches Bild. Um das reibungslose Funktionieren des Binnenmarkts sicherzustellen und die Erfordernisse weltweit operierender Unternehmen erfüllen zu können, müssen einheitliche Anforderungen, Vorschriften und Verfahren für die gesamte EU geschaffen werden. In ihrer jüngsten Mitteilung (KOM(2009) 149 endgültig) erkennt die Kommission die Bedeutung kritischer Kommunikationsnetze an und ruft die ENISA dazu auf, aktiv an der Sicherstellung angemessener Schutzmechanismen mitzuarbeiten. In dieser Mitteilung werden mehrere Maßnahmen aufgeführt, die in Ergänzung der nationalen Programme sowie der bestehenden bilateralen und multilateralen Kooperationsregelungen zwischen den Mitgliedstaaten die Erarbeitung eines integrierten EU-Konzepts für sicherere und robustere kritische Kommunikationsnetze vorsehen. Die enge Zusammenarbeit mit dem privaten und dem öffentlichen Sektor wird bei jeder dieser Maßnahmen als ein wesentlicher Erfolgsfaktor angesehen. Bestehende Maßnahmen werden nach Möglichkeit ebenfalls genutzt.
BESCHREIBUNG DES ANSATZES ZUR LÖSUNG DES PROBLEMS:
Das Ziel dieses TMP besteht darin, die Mitgliedstaaten und die Kommission bei ihrer Arbeit zur Stärkung der Widerstandsfähigkeit der Kommunikationsnetze zu unterstützen, indem sie „gemeinsam die Sicherheit und Widerstandsfähigkeit mobiler und fester öffentlicher Kommunikationsnetze und Dienste in Europa“ bewerten und erhöhen. Im Jahr 2008 führte die ENISA eine Reihe von Bestandsaufnahmen zu regulatorischen und politischen Kontexten, zu den Maßnahmen der Anbieter und zu den bestehenden Technologien und Standards durch. Im Jahr 2009 analysierte die ENISA die Ergebnisse dieser Bestandsaufnahmen, ermittelte, wo die gegenwärtige Situation gegenüber der gewünschten Situation noch Lücken aufwies und erarbeitete im Rahmen von Workshops oder Experten-Arbeitsgruppen gemeinsam mit den Interessenvertretern bewährte aktuelle Praktiken, um diese Lücken zu schließen. Für das Jahr 2010 sieht die ENISA die folgenden Maßnahmen vor: 1) Unterstützung der Anstrengungen der Interessenvertreter bezüglich der Umsetzung der Leitfäden zu bewährten Verfahren für den Informationsaustausch und das Berichtswesen für Sicherheitsvorfälle.

Gemeinsam mit ausgewählten Interessenvertretern wird die Agentur ihr Wissen über die bestehenden Leitfäden und Empfehlungen für bewährte Verfahren ausbauen. Dies umfasst auch die Erörterung der Ergebnisse und deren Validierung im Rahmen von Workshops und thematischen Arbeitsgruppen sowie die Unterstützung bei der Annahme von Empfehlungen.

2) Unterstützung der Anbieter bei der Verbesserung der Widerstandsfähigkeit ihrer Netze. Dies beinhaltet die Analyse rechtlicher und politischer Beschränkungen für den Informationsaustausch, die Ermittlung geeigneter Parameter in Bezug auf die Widerstandsfähigkeit und die Bereitstellung politischer Empfehlungen im Bereich von Botnets.
3) Vertiefung der bisherigen Arbeiten auf dem Gebiet der Sicherheitsprotokolle, insbesondere DNSSec.
4) Gemeinsam mit Interessenvertretern, die über einschlägige Erfahrungen verfügen, Entwicklung eines ganzheitlichen Rahmens für die Definition, Ausführung und Bewertung von Übungen auf nationaler Ebene und langfristig auch von grenzübergreifenden oder europaweiten Übungen. Dieser Rahmen wird durch eine Reihe von Szenarien zur Ausführung dieser Übungen ergänzt. Er baut unter anderem auf den Erfahrungen der Interessenvertreter auf und soll zudem die Rolle der nationalen/staatlichen CERT in Bezug auf die Planung und Ausführung dieser Tätigkeiten stärken.

ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):

SMART-Ziel: Bis 2010 wird die Kommission die ENISA-Empfehlungen in ihrem politischen Entscheidungsprozess berücksichtigt haben.	**KPI:** Kommission (ja/nein)
SMART-Ziel: Bis 2012 haben mindestens zwei Mitgliedstaaten an einem Pilotprojekt auf Grundlage der Rahmenstruktur teilgenommen.	**KPI:** Zahl der Mitgliedstaaten
SMART-Ziel: Bis 2010 haben sich mindestens 50 % der Mitgliedstaaten an dem europaweiten Forum beteiligt.	**KPI:** % der Mitgliedstaaten
SMART-Ziel: Bis 2012 haben mindestens 50 % der Mitgliedstaaten einen Beitrag zu der Rahmenstruktur geleistet.	**KPI:** % der Mitgliedstaaten, Zahl der gelieferten Beiträge

VORRANGIGE ZIELE, DIE DURCH DAS PROGRAMM UNTERSTÜTZT WERDEN:

Stärkung des Vertrauens in das Informationszeitalter durch die Anhebung des Niveaus der NIS in der EU; Förderung des Binnenmarkts für elektronische Kommunikation durch die Unterstützung der Institutionen bei der Festlegung einer geeigneten Mischung aus Gesetzesvorschriften und anderen Maßnahmen (unter besonderer Berücksichtigung des wichtigen Beitrags, den die Agentur zur Rahmenrichtlinie leisten kann); Ausweitung des Dialogs über NIS zwischen den verschiedenen Interessenvertretern in der EU; Ausweitung der Zusammenarbeit zwischen den Mitgliedstaaten mit dem Ziel, die unterschiedlichen Fähigkeiten der Mitgliedstaaten auf diesem Gebiet auf ein einheitliches Niveau zu bringen.

AKTEURE UND BEGÜNSTIGTE:

Nationale Regulierungsbehörden, Regierungen der Mitgliedstaaten, politische Entscheidungsträger auf EU-Ebene, nationale und staatliche CERT, öffentliche elektronische Kommunikationsnetze und Diensteanbieter (Festnetz-, mobile und IP-basierte Dienste), Internet-Diensteanbieter (Internet Service Providers, ISP), Anbieterverbände (ECTA, ETNO, GSM Europe), Internet-Austauschknoten (Euro IXs), Audit-Vereinigungen (ISACA), Lieferanten von Netzwerk-Komponenten, -Systemen und -Software (EICTA).

WARUM DIE ENISA?

Groß angelegte Computer-Angriffe können nur auf multilateraler Ebene wirksam abgewehrt werden. Dazu ist die Abstimmung von Rechtsvorschriften, Planungen, organisatorischen Aspekten, Infrastrukturen und technischen Maßnahmen erforderlich. Durch ihre Ausrichtung ist die ENISA in der Lage, die gemeinsamen Politiken, Maßnahmen und Verfahren der Europäischen Union in diesem Bereich zu fördern und zu unterstützen.

2.1.1 Arbeitspaket 1.1 – Unterstützung der Anstrengungen der Interessenvertreter bezüglich der Umsetzung der Leitfäden zu bewährten Verfahren für den Informationsaustausch und das Berichtswesen für Sicherheitsvorfälle

Bezeichnung des TMP:	
Verbesserung der Widerstandsfähigkeit der europäischen elektronischen Kommunikationsnetze	
BEZEICHNUNG DES ARBEITSPAKETS:	
Arbeitspaket 1.1: Unterstützung der Anstrengungen der Interessenvertreter bezüglich der Umsetzung der Leitfäden zu bewährten Verfahren für den Informationsaustausch und das Berichtswesen für Sicherheitsvorfälle	
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):	
SMART-Ziel: Mindestens zehn Mitgliedstaaten beteiligen sich an den Diskussionen über die Umsetzung einer Methode für den Informationsaustausch	**KPI**: Zahl der Mitgliedstaaten
SMART-Ziel: Mindestens zehn Mitgliedstaaten beteiligen sich an den Diskussionen über die Entwicklung von harmonisierten Mechanismen für das Berichtswesen für Sicherheitsvorfälle	**KPI**: Zahl der Mitgliedstaaten
SMART-Ziel: Mindestens zehn (größere und kleinere) Anbieter beteiligen sich an den Diskussionen über die Entwicklung von harmonisierten Mechanismen für das Berichtswesen für Sicherheitsvorfälle	**KPI:** Zahl der Anbieter
BESCHREIBUNG DER AUFGABEN:	

Im Jahr 2008 führte die ENISA eine Reihe von Bestandsaufnahmen zu regulatorischen und politischen Fragen der Mitgliedstaaten bezüglich der Widerstandsfähigkeit und Sicherheit ihrer Netze durch. Auf der Grundlage der erzielten Ergebnisse hat die Agentur im Jahr 2009 gemeinsam mit zahlreichen Interessenvertretern aus dem öffentlichen und privaten Sektor Leitfäden zu bewährten Verfahren für den Informationsaustausch zur Netzwerksicherheit (Network Security Information Exchange, NSIE) und zu Mechanismen für das Berichtswesen für Sicherheitsvorfälle erarbeitet. Diese Leitfäden zu bewährten Verfahren sind das Ergebnis der Zusammenarbeit mit zahlreichen relevanten Interessenvertretern, die die Leitfäden der ENISA im Rahmen thematischer Workshops und eines offenen Konsultationsprozesses ausführlich erörtert und validiert haben.

Hauptziel dieses Arbeitspakets ist es, Anreize für öffentliche und private Akteure zu ermitteln, die von der ENISA und ihren Interessenvertretern erarbeiteten Leitfäden zu bewährten Verfahren umzusetzen, und den Akteuren zu helfen, ihr Verständnis der grundlegenden Empfehlungen zu vertiefen. Die Agentur wird in der Vergangenheit erarbeitete Ergebnisse nutzen, Schlussfolgerungen mit den relevanten Interessenvertretern erörtern, sie im Rahmen gezielter Workshops und thematischer Arbeitsgruppen validieren und die Interessenvertreter bei der Annahme von Empfehlungen unterstützen.

In Bezug auf den Informationsaustausch möchte die Agentur 1) die Zahl der Länder in Europa erhöhen, die den NSIE einführen und anwenden und 2) die Entwicklung des Europäischen Forums für den Informationsaustausch zwischen den Mitgliedstaaten (vgl. KOM(2009) 149 endgültig) fördern, das somit der erste europaweite Ansatz für den Informationsaustausch zur Netzwerksicherheit in Europa wäre. Daher wird die ENISA allen Mitgliedstaaten in zielgerichteten Workshops ihre Leitfäden zu bewährten Verfahren vorstellen. Die Agentur wird den Dialog zwischen Experten fördern, relevante öffentliche und private Interessenvertreter zur Teilnahme auffordern und ihre Beteiligung an diesem Prozess sicherstellen, Ergebnisse validieren und die Mitgliedstaaten im Rahmen von Schulungsmaßnahmen bei der Einrichtung und dem Betrieb einer Plattform für den Informationsaustausch unterstützen.

Gleichzeitig wird die ENISA die wichtigsten NSIE-Partner in Europa mit relevanten Beteiligten an nationalen und europaweiten Projekten an einen Tisch bringen, die dann die Möglichkeit der Entwicklung der ersten europaweiten Plattform erörtern. Die von der ENISA vorgeschlagenen Maßnahmen für den Informationsaustausch zur Netzwerksicherheit werden in die von der Kommission

initiierten laufenden Diskussionen über die Einrichtung einer Europäischen öffentlich-privaten Partnerschaft für Robustheit (EÖPPR) einfließen, die im Aktionsplan zum Schutz kritischer Informationsinfrastrukturen (CIIP) – KOM(2009) 149 endgültig – vorgeschlagen wird.

Im Zusammenhang mit den Mechanismen für das Berichtswesen für Sicherheitsvorfälle wird die ENISA die relevanten öffentlichen und privaten Interessenvertreter ermitteln und gemeinsam mit ihnen den offenen Dialog fördern. Dieses Vorgehen steht im Einklang mit den Bestimmungen des neuen gemeinsamen Rechtsrahmens für elektronische Kommunikationsnetze und -dienste bezüglich der Integrität und Verfügbarkeit öffentlicher Kommunikationsnetze (z. B. Artikel 13 Buchstabe a der Rahmenrichtlinie 2002/21/EG).

Im Rahmen eines strukturierten Dialogs mit den relevanten öffentlichen und privaten Interessenvertretern wird die ENISA konkrete und realistische Leitlinien bezüglich der möglichen Umsetzung dieser Bestimmungen (z. B. bei einer Verletzung der Sicherheit, fehlender Integrität oder im Zusammenhang mit der konsolidierten jährlichen Liste der Sicherheitsvorfälle) erarbeiten. Die Agentur wird ihre Empfehlungen sorgfältig und umfassend validieren und somit eine breite Akzeptanz sicherstellen. Die Umsetzung der ENISA-Leitfäden zu bewährten Verfahren in einer frühen Phase des Reformpakets für den Telekommunikationssektor wird sich positiv auf die Harmonisierung der Prozesse und Strategien auf nationaler und europäischer Ebene auswirken.

Die ENISA wird auch in Zukunft mit allen relevanten öffentlichen und privaten Interessenvertretern an der Entwicklung geeigneter Maßnahmen und Strategien zur Verbesserung der Integrität bei der Bereitstellung von Netzen und Diensten arbeiten.

ERGEBNISSE UND TERMINE:

Thematischer Workshop und Schulung zum Informationsaustausch zur Netzwerksicherheit (Q2, Q3 2010); Bericht über den Stand des Informationsaustausches zur Netzwerksicherheit in Europa (Q4 2010); zwei thematische Workshops zu Mechanismen für das Berichtswesen für Sicherheitsvorfälle (Q1, Q3 2010); Entwurf von Richtlinien über die Einführung eines Berichtswesens für größere Sicherheitsvorfälle (Q4 2010).

FOLGENDE INTERESSENVERTRETER SOLLTEN DAS ARBEITSPAKET AKTIV UNTERSTÜTZEN:

Zu den möglichen Interessenvertretern zählen: Nationale Regulierungsbehörden (NRA), nationale politische Stellen, die auf dem Gebiet der Widerstandsfähigkeit öffentlicher Kommunikationsnetze und Dienste tätig sind, Branchenverbände (EICTA, ETNO, EuroISPA, GSM Europe, ISACA und Euro-IX), Telekommunikations-Dienstleister (feste, mobile und IP-basierte Netze) und Internet-Diensteanbieter (Internet Service Providers, ISP).

RESSOURCEN FÜR 2010 (Personenmonate und Haushaltsmittel):

- 100 000 EUR
- 11,5 Personenmonate

VORSCHLAG FÜR DAS ARBEITSPAKET:

ENISA

RECHTSGRUNDLAGE:

ENISA-Verordnung, Artikel 3 Buchstaben a, c, d, f und k

2.1.2 Arbeitspaket 1.2 – Unterstützung der Anbieter bei der Verbesserung der Widerstandsfähigkeit ihrer Netze

Bezeichnung des TMP:	
Verbesserung der Widerstandsfähigkeit der europäischen elektronischen Kommunikationsnetze	
BEZEICHNUNG DES ARBEITSPAKETS:	
Arbeitspaket 1.2 – Unterstützung der Anbieter bei der Verbesserung der Widerstandsfähigkeit ihrer Netze	
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):	
SMART-Ziel: Mindestens zehn Mitgliedstaaten und zehn wichtige private Interessenvertreter beteiligen sich an den Diskussionen über rechtliche und politische Beschränkungen	**KPI:** Zahl der Mitgliedstaaten, Zahl der Anbieter
SMART-Ziel: Mindestens zehn Mitgliedstaaten und zehn wichtige private Interessenvertreter beteiligen sich an den Diskussionen über Parameter und Messtechniken	**KPI:** Zahl der Mitgliedstaaten, Zahl der Anbieter
SMART-Ziel: Mindestens zehn Mitgliedstaaten und zehn wichtige ISP/IX beteiligen sich an den Diskussionen über Parameter und Messtechniken	**KPI:** Zahl der Mitgliedstaaten, Zahl der Anbieter
BESCHREIBUNG DER AUFGABEN:	
Im Jahr 2008 führte die ENISA eine Bestandsaufnahme zu den Maßnahmen der Anbieter bezüglich der Widerstandsfähigkeit und Sicherheit ihrer Netze durch und erarbeitete im Jahr 2009 mehrere Empfehlungen und bewährte Verfahren zu einer Reihe von diesbezüglichen Problemen. Diese Probleme umfassen unter anderem rechtliche und politische Beschränkungen für die Anbieter bezüglich des Austauschs sensibler Informationen, wirksame Mittel zum Messen der Widerstandsfähigkeit und Sicherheit der Netze der Anbieter sowie wirksame Strategien im Kampf gegen Botnets. Rechtliche und politische Beschränkungen behindern in erheblichem Maß die Möglichkeiten der privaten Betreiber zum Austausch von Informationen mit den relevanten Interessenvertretern. Es bleibt weiterhin unklar, wie bestehende Gesetze und Strategien zu Aspekten wie dem Schutz der Privatsphäre und personenbezogener Daten auf Informationsnetze angewendet werden oder wie der Geheimhaltungspflicht in öffentlich-privaten Partnerschaften im Zusammenhang mit dem Schutz kritischer Informationsinfrastrukturen Rechnung getragen wird. Der Großteil dieser Gesetze wurde vor Beginn des Informationsgesellschaft und der Abhängigkeit von Informationsnetzen verabschiedet. Nach wie vor gibt es keinen klaren Rechtsrahmen für den zeitnahen und wirksamen Austausch von Informationen zum Schutz kritischer Informationsinfrastrukturen, einschließlich der verantwortungsbewussten und zeitnahen Ermittlung von Schwachstellen. Im Rahmen dieser Maßnahme sollen diesbezügliche Lücken in den Gesetzen und Strategien aufgedeckt werden, um im Anschluss daran zu analysieren, inwieweit sich diese Defizite auf die wirksame Umsetzung des Informationsaustauschs im Zusammenhang mit dem Schutz kritischer Informationsinfrastrukturen auswirken. Obgleich die Zahl der Strategien, Maßnahmen und Methodiken, die den gesamten Lebenszyklus aller Vorfälle im Zusammenhang mit der Sicherheit und Widerstandsfähigkeit der Netze abdecken, immer mehr zunimmt, gibt es keine geeigneten Mittel, mit denen sich die Widerstandsfähigkeit und Sicherheit von Netzen messen lässt. In Bezug auf die Parameter und Messtechniken zum Ermitteln der Verfügbarkeit und Integrität bestimmter Netze (einschließlich Service-Level-Vereinbarungen, SLA) konnten wesentliche Fortschritte erzielt werden. Ein Großteil von ihnen befasst sich jedoch nicht mit dem Problem im Allgemeinen und geht dieses Thema nicht aus politischer Sicht an. Noch immer stehen den politischen Entscheidungsträgern und den Regulierungsbehörden keine zuverlässigen Parameter und somit keine eindeutigen Mechanismen zum Messen der Widerstandsfähigkeit und der Sicherheit öffentlicher Kommunikationsnetze zur Verfügung. Die ENISA möchte alle relevanten Interessenvertreter (Industrie, Hochschulen, politische Entscheidungsträger, internationale Organisationen, Normungsgremien) an einen Tisch bringen, um Untersuchungen auf diesem Gebiet anzustellen, die aktuellen Entwicklungen und relevante Projekte (z. B. das von der EU finanzierte Projekt **AMBER**) zu ermitteln und gemeinsam mit diesen Interessenvertretern geeignete Messtechniken und zugehörige Parameter zum Ermitteln der Widerstandsfähigkeit zu erarbeiten. Langfristig plant die ENISA zudem die Einführung von Leistungsindikatoren – zunächst auf nationaler Ebene und schließlich auch europaweit –, mit denen die Widerstandsfähigkeit und Sicherheit unserer öffentlichen Kommunikationsnetze endlich gemessen werden könnten.	

Botnets gelten als große Gefahr für das Internet und damit auch für unsere kritischen Kommunikationsdienste. Insbesondere auf Personal Computern (PCs) finden diese Botnets zunehmend Möglichkeiten, sich zu verbreiten und in die Netze einzudringen. Die ENISA wird sich mit diesem Phänomen der Botnets befassen, auf einzelstaatlicher Ebene eine Bestandsaufnahme zu den vorhandenen Regelungen über Botnets vornehmen, gemeinsam mit relevanten Interessenvertretern (ISP, IX, EuroISPA, Euro IX, ETNO usw.) verschiedene politische Empfehlungen erarbeiten und konkrete Vorschläge für geeignete und realisierbare Messtechniken machen. Die ENISA möchte mit allen relevanten Interessenvertretern eine offene Diskussion über eine mögliche Zusammenarbeit auf europäischer Ebene (z. B. gegenseitige Unterstützung, Austausch von Informationen) führen.
ERGEBNISSE UND TERMINE:
Rechtliche und politische Beschränkungen für den Austausch sensibler Informationen im Zusammenhang mit dem Schutz kritischer Informationsinfrastrukturen (Q3 2010); Analyse der Parameter und Messtechniken unter Anwendung moderner Analysemethoden (Q4 2010); Botnets: politische Empfehlungen (Q4 2010)
FOLGENDE INTERESSENVERTRETER SOLLTEN DAS ARBEITSPAKET AKTIV UNTERSTÜTZEN:
Nationale Regulierungsbehörden (NRA), nationale politische Stellen, die auf dem Gebiet der Widerstandsfähigkeit öffentlicher Kommunikationsnetze und Dienste tätig sind, Branchenverbände (EICTA, ETNO, EuroISPA, GSM Europe, ISACA und Euro-IX), Telekommunikations-Dienstleister (feste, mobile und IP-basierte Netze) und Internet-Diensteanbieter (Internet Service Providers, ISP).
RESSOURCEN FÜR 2010 (Personenmonate und Haushaltsmittel):
150 000 EUR; 13,5 Personenmonate
VORSCHLAG FÜR DAS ARBEITSPAKET:
ENISA
RECHTSGRUNDLAGE:
ENISA-Verordnung, Artikel 3 Buchstaben a, c, d, f und k

2.1.3 Arbeitspaket 1.3 – Untersuchung innovativer Maßnahmen

Bezeichnung des TMP:	
Verbesserung der Widerstandsfähigkeit der europäischen elektronischen Kommunikationsnetze	
BEZEICHNUNG DES ARBEITSPAKETS:	
Arbeitspaket 1.3: Untersuchung innovativer Maßnahmen	
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):	
SMART-Ziel: Mindestens zehn Akteure der beteiligten Sektoren nehmen an einem Pilotprojekt zur Anwendung der Empfehlungen und Leitlinien bezüglich der DNSSec-Umsetzung teil.	**KPI:** Zahl der Akteure der beteiligten Sektoren
SMART-Ziel: Abdeckung von mindestens 200 Millionen Nutzern durch Anbieter, die im Rahmen der Folgenabschätzung zu Routing-Protokollen überprüft wurden	**KPI:** Zahl der Nutzer
SMART-Ziel: Mindestens zehn Akteure der beteiligten Sektoren validieren den Bericht über die Grundsätze für Architekturentwürfe, die zu einer wirklich durchgängigen Sicherheit (e2e-Sicherheit) führen	**KPI:** Zahl der Akteure der beteiligten Sektoren
SMART-Ziel: Organisation eines Workshops „Open Doors to Technologies Enhancing Network Resilience“ (Die Türen öffnen für Technologien zur Verbesserung der Widerstandsfähigkeit von Netzen) für die wissenschaftlichen Referenten der Europäischen Kommission mit Vertretern aller betreffenden Sektoren der Interessenvertreter (Händler, Betreiber, Regulierungsbehörden, Endnutzer usw.). Mindestens 30 Teilnehmer aus mindestens drei verschiedenen Sektoren.	**KPI:** Zahl der Teilnehmer Zahl der teilnehmenden Sektoren
BESCHREIBUNG DES ARBEITSPAKETS:	
In den Jahren 2008 und 2009 hat die ENISA mehrere Technologien, Protokolle und Architekturen (IPv6, Multiprotocol Label Switching (MPLS) und DNS Security Extensions (DNSSec)) hinsichtlich ihres Potenzials zur Verbesserung der Widerstandsfähigkeit öffentlicher Kommunikationsnetze analysiert. In diesem Kontext wurden auch Anreize (für markt- und/oder politikbezogene Aspekte) mit Blick auf ihre Wirkung auf Geschäftsgebaren betrachtet. Die erarbeiteten Empfehlungen und Leitfäden zu bewährten Verfahren richteten sich in erster Linie an die politischen Entscheidungsträger auf nationaler Ebene sowie auf Ebene der EU. Die Agentur beschränkte sich hierbei nicht auf Technologien, Architekturen und Protokolle, sondern bewertete auch die Auswirkungen der Entwicklungen im Bereich der Netztechnologien (z. B. Cloud Computing, Sensorennetze, Online-Überwachungs- und Diagnosesysteme) auf die Sicherheit und Verfügbarkeit von Netzressourcen und legte die Richtung für künftige Forschungen fest. Diese Aufgaben wurden in enger Zusammenarbeit mit zwei Expertengruppen durchgeführt, in denen Akteure aus allen relevanten Sektoren vertreten waren. Basierend auf den Erfahrungen aus dem Jahr 2009 wird die Agentur sich auch in Zukunft auf die Arbeit dieser beiden Expertengruppen stützen. Im Jahr 2009 hat die ENISA Leitfäden zu bewährten Verfahren für die Einführung von DNSSec erarbeitet. Darin sind die wesentlichen Überlegungen aufgeführt, die die Anbieter, die diese Technologie einsetzen, anstellen müssen, sowie die Aspekte, die in die politischen und praktischen Erklärungen für Trust Anchor Repositories eingebunden werden sollten. Hauptziele dieses Arbeitspakets sind das Testen bzw. Umsetzen der Empfehlungen in echten Arbeitsumgebungen, um so Rückmeldungen bezüglich ihrer Wirksamkeit, Gültigkeit und Eignung zu erhalten. Die ENISA will diese Empfehlungen, die sich in erster Linie an politische Entscheidungsträger in der EU und auf nationaler Ebene richten, einer breiten Öffentlichkeit bekannt machen, damit die besonders viel versprechenden Maßnahmen so schnell wie möglich aufgegriffen werden. Darüber hinaus sollen die Erfahrungen auf diesem Gebiet auch	

Informationen für die Abteilung Sensibilisierung – die Awareness Raising Section – der ENISA liefern, damit diese eine Informationskampagne für Nutzer im Allgemeinen oder für bestimmte Nutzergruppen vorbereiten kann, die über die Gefahren im Zusammenhang mit dem DNS und DNSSec in informellen Web-Anwendungen wie dem Online-Banking oder dem Online-Shopping aufklärt.

Die Absicherung des DNS trägt zur Gewährleistung eines hohen Maßes an Widerstandsfähigkeit und Sicherheit der öffentlichen Kommunikationsnetze bei. Eine weitere zentrale Form der Infrastruktur in den öffentlichen elektronischen Kommunikationsnetzen, deren Widerstandsfähigkeit sichergestellt werden muss, ist die Routing-Infrastruktur. In diesem Zusammenhang möchte die ENISA die Auswirkungen der Einführung widerstandsfähiger Routing-Technologien bewerten. Diese Bewertung bildet dann die Grundlage für Leitlinien und Empfehlungen für politische Entscheidungsträger zum Einsatz solcher Technologien.

Neben den genannten Maßnahmen wird die ENISA ihre Arbeit zur Bewertung der Auswirkungen von netztechnischen Entwicklungstrends auf die Widerstandsfähigkeit öffentlicher Kommunikationsnetze weiter intensivieren, indem sie die Grundsätze für Architekturentwürfe ermittelt und verbreitet, die zu einer wirklich durchgängigen Sicherheit (e2e-Sicherheit) führen. Der Schwerpunkt lag hierbei zunächst auf den Technologien bezüglich der Transportschicht der Kommunikationsnetze. Öffentliche Kommunikationsnetze bilden jedoch die Grundlage für zahlreiche Anwendungen und Dienste von Diensteanbietern, die in vielen Fällen unabhängig vom Netzbetreiber agieren. In diesem Zusammenhang spielt daher neben einem widerstandsfähigen und sicheren Transportnetz insbesondere der Aspekt der durchgängigen Widerstandsfähigkeit und Sicherheit eine entscheidende Rolle für die Nutzer von IKT-Diensten. Die Ermittlung der Grundsätze für Architekturentwürfe ist damit wichtiger als die Ermittlung leistungsstarker Architekturen. Einzelne Architekturen können stark von der jeweiligen Technologie abhängen, die Grundsätze hingegen bleiben in der Regel auch über technologische Beschränkungen hinweg gleich.

Schließlich werden diese Maßnahmen auch mit dem zielgerichteten Workshop „Open Doors to Technologies Enhancing Network Resilience“ (Die Türen öffnen für Technologien zur Verbesserung der Widerstandsfähigkeit von Netzen) kombiniert. Diese Maßnahme soll den wissenschaftlichen Referenten der Kommission (GD Informationsgesellschaft und Medien, GD Unternehmen und Industrie, GD Justiz, Freiheit und Sicherheit, GD MARKT und GD Forschung) Einblick in das Thema Widerstandsfähigkeit von Kommunikationsnetzen und in die Maßnahmen der ENISA auf diesem Gebiet geben. Ausgehend von den im Jahr 2009 gewonnenen Erfahrungen in diesem Bereich könnte diese Maßnahme auch über den Anwendungsbereich des Arbeitspakets 1.3 (Technologien) hinaus erweitert und auf alle Aspekte des TMP 1 (einschließlich politischer Strategien) angewendet werden.

ERGEBNISSE UND TERMINE:

Plan zur Vorbereitung einer Informationskampagne für Nutzer im Allgemeinen oder für bestimmte Nutzergruppen, die über die Gefahren im Zusammenhang mit dem DNS und DNSSec in informellen Web-Anwendungen wie dem Online-Banking oder dem Online-Shopping aufklärt (Q3 2010).
Bericht über Pilotprojekt(e) zur Verbreitung der im Rahmen des Arbeitspakets 1.3. in den Jahren 2008-2009 geleisteten Arbeit zur Verbesserung der Widerstandsfähigkeit des DNS (Q4 2010).
Bewertung der Auswirkungen des Einsatzes widerstandsfähiger Routing-Technologien und Erarbeitung von entsprechenden Leitlinien und Empfehlungen (Q4 2010).
Bericht über die Grundsätze für Architekturentwürfe, die zu einer wirklich durchgängigen Widerstandsfähigkeit und Sicherheit öffentlicher Kommunikationsnetze führen (Q4 2010).
Workshop „Open Doors to Technologies Enhancing Network Resilience“ (Die Türen öffnen für Technologien zur Verbesserung der Widerstandsfähigkeit von Netzen) (Q4 2010)

FOLGENDE INTERESSENVERTRETER SOLLTEN DAS ARBEITSPAKET AKTIV UNTERSTÜTZEN:

Netzwerkgeräte-Händler, nationale Regulierungsbehörden (NRA), Netzbetreiber, virtuelle Netzbetreiber, Experten für widerstandsfähige Backbone- und Internettechnologie, FuE-Einrichtungen der Industrie, Universitäten und Forschungszentren, Europäische Technologieplattformen (z. B. eMobility, NEM, NESSI).

RESSOURCEN FÜR 2009 (Personenmonate und Haushaltsmittel):

- 195 000 EUR (Workshops, Beratungsdienste, Arbeit von Expertengruppen, elektronische und gedruckte Veröffentlichungen).

• 17,5 Personenmonate
VORSCHLAG FÜR DAS ARBEITSPAKET:
ENISA
RECHTSGRUNDLAGE:
ENISA-Verordnung, Artikel 3 Buchstaben a, b, c, f und k

2.1.4 Arbeitspaket 1.4 – Unterstützung der Interessenvertreter bei der ersten europaweiten Übung

Bezeichnung des TMP:	
Verbesserung der Widerstandsfähigkeit der europäischen elektronischen Kommunikationsnetze	
BEZEICHNUNG DES ARBEITSPAKETS:	
Arbeitspaket 1.4 – Unterstützung der Interessenvertreter bei der ersten europaweiten Übung	
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):	
SMART-Ziel: Mindestens 50 % der Mitgliedstaaten beteiligen sich an den Diskussionen über die erste europaweite Übung	**KPI:** % der Mitgliedstaaten
SMART-Ziel: Mindestens drei Mitgliedstaaten setzen im Rahmen der Übungen den ENISA-Leitfaden für bewährte Verfahren um	**KPI:** Zahl der Übungen
SMART-Ziel: Mindestens 30 % der Mitgliedstaaten unterstützen den ENISA-Rahmen für die Ausführung der Übungen	**KPI:** % der Mitgliedstaaten
BESCHREIBUNG DER AUFGABEN:	
Der Leitfaden der ENISA für bewährte Verfahren im Zusammenhang mit Tätigkeiten auf nationaler Ebene verdeutlicht die Bedeutung der Übungen, mit denen die Einhaltung der Vorsorgemaßnahmen im Notfall durch öffentliche und private Interessenvertreter überprüft wird. In der jüngsten Mitteilung der Kommission über den Schutz kritischer Informationsinfrastrukturen wird insbesondere auf den Stellenwert der Übungen bei der Verbesserung der Vorsorgemaßnahmen für den Notfall eingegangen. Bis jetzt haben nur wenige Mitgliedstaaten Übungen durchgeführt, um ihre Vorsorgemaßnahmen zu überprüfen. Im Rahmen dieses Arbeitspakets möchte die ENISA auf europäischer Ebene den Dialog über die Übungsmaßnahmen erleichtern. Die Agentur unterstützt die Mitgliedstaaten dabei, die Interessenvertreter zusammenzubringen, die die erste europaweite Übung gemeinsam konzipieren, entwickeln, durchführen und bewerten sollen. Um dieses Ziel zu erreichen, wird die ENISA intensiv mit der Kommission und den Mitgliedstaaten zusammenarbeiten und so eine enge Kooperation mit den relevanten Interessenvertretern und geeigneten europaweiten Projekten (z. B. über das Europäische Programm für den Schutz kritischer Infrastrukturen (EPSKI) finanzierte Projekte) sicherstellen. Dies umfasst unter anderem die Zusammenarbeit mit den wichtigsten Interessenvertretern, um so deren Wissen über die Leitfäden zu bewährten Verfahren für nationale Übungsmaßnahmen auszubauen, die Inhalte im Rahmen zielgerichteter Diskussionen und thematischer Arbeitsgruppen zu validieren und die Interessenvertreter schließlich bei ihrer Teilnahme an der ersten europaweiten Übung zu unterstützen. Über diesen Dialog möchte die ENISA eine Reihe möglicher Szenarien erarbeiten, die für die Durchführung der ersten europaweiten Übungen (z. B. die Ermittlung kritischer Vorgehensweisen) herangezogen werden können, und zudem ein ganzheitliches Rahmenwerk für die Durchführung von nationalen, grenzübergreifenden oder sogar europaweiten Übungen schaffen. Im Zusammenspiel mit den möglichen Szenarien wird dieser Rahmen es den öffentlichen und privaten Interessenvertretern ermöglichen, Vorsorgemaßnahmen zu erarbeiten, zu organisieren und durchzuführen. Zu möglichen Bestandteilen des Rahmens zählen die Profile der Interessenvertreter (Zielgruppen und Veranstalter), die Art der Übungen, zu testende Vorsorgemaßnahmen, mögliche Szenarien, Bewertungsmethoden usw. Die ENISA wird den vorgeschlagenen Rahmen und mögliche Szenarien in einem thematischen Workshop und in Zusammenarbeit mit Experten validieren. In diesem Zusammenhang wird die ENISA ihre Zusammenarbeit bei den Maßnahmen und Projekten im Bereich der Notfallvorsorge weiterhin fortsetzen. Die Agentur wird sich auf eine über das EPSKI finanzierte Studie stützen, die untersucht, inwieweit die Vorsorgemaßnahmen für den Notfall in Europa greifen. Außerdem bewertet die Studie mögliche künftige Strategien, Maßnahmen und Leitfäden. die zu einer Verbesserung der Notfallvorsorge und der Zusammenarbeit innerhalb des Telekommunikationssektors in Europa führen. Darüber hinaus arbeitet die ENISA auch weiterhin intensiv mit der Europäischen Kommission und den Mitgliedstaaten an der Durchführung der in der	

Mitteilung KOM(2008) 130 endgültig („Stärkung der Katastrophenabwehrkapazitäten der Europäischen Union“) genannten Maßnahmen. Gemeinsam mit den relevanten Interessenvertretern wird die ENISA den Dialog über die Verbesserung der Zusammenarbeit, des Informationsaustauschs und der gegenseitigen Unterstützung bei der Katastrophenabwehr zwischen den Interessenvertretern im Telekommunikationssektor vereinfachen. Ausgehend von den Erkenntnissen und Ergebnissen dieser Maßnahmen wird die ENISA die nächsten möglicherweise zu ergreifenden Schritte im Bereich der Notfallvorsorge und Katastrophenabwehr mit den geeigneten Interessenvertretern abstimmen. Auf der Grundlage dieser Beiträge formuliert die ENISA eine Reihe politischer Empfehlungen für zusätzliche Maßnahmen in diesem Bereich.
ERGEBNISSE UND TERMINE:
Thematische(r) Workshop(s) zum Rahmen für die Ausführung der Übungen (Q2 2010) Rahmen für die Ausführung der Übungen (Q4 2010) Politische Empfehlungen in Bezug auf die Notfallvorsorge und die Wiederherstellung von Daten im Notfall
AKTEURE:
Nationale Regulierungsbehörden (NRA), nationale politische Stellen, die auf dem Gebiet der Widerstandsfähigkeit öffentlicher Kommunikationsnetze und Dienste tätig sind, Branchenverbände (EICTA, ETNO, EuroISPA, GSM Europe, ISACA und Euro-IX), Telekommunikations-Dienstleister (feste, mobile und IP-basierte Netze) und Internet-Diensteanbieter (Internet Service Providers, ISP), Europäische Kommission, CERT-Gemeinschaften.
RESSOURCEN FÜR 2010 (Personenmonate und Haushaltsmittel):
• 100 000 EUR • 13,5 Personenmonate
VORSCHLAG FÜR DAS ARBEITSPAKET:
ENISA, Verwaltungsrat, KOM
RECHTSGRUNDLAGE:
ENISA-Verordnung, Artikel 3 Buchstaben a, c, d, f und k

2.2. TMP 2: Entwicklung und Fortführung von Kooperationsmodellen

BEZEICHNUNG DES PROGRAMMS	
TMP 2: Entwicklung und Fortführung von Kooperationsmodellen	
BESCHREIBUNG DES PROBLEMS	
Viele Mitgliedstaaten stehen vor der Notwendigkeit, ihre Fähigkeiten in verschiedenen Bereichen der Netz- und Informationssicherheit (NIS) zu erweitern. Einige Mitgliedstaaten arbeiten bereits zusammen und tauschen Informationen und bewährte Verfahren aus, doch ein Rahmen für eine strukturierte Zusammenarbeit fehlt bislang. Das hat zur Folge, dass die auf europäischer Ebene bestehenden Möglichkeiten zur Schaffung von Synergien und zur Verbesserung der Effizienz und Effektivität ungenutzt bleiben.	
BESCHREIBUNG DES ANSATZES ZUR LÖSUNG DES PROBLEMS:	
Mit diesem TMP will die ENISA auf diese Bedürfnisse eingehen und ihre Rolle als Vermittler, Kompetenzzentrum und Beratungsstelle ausbauen. Die technischen Sachverständigen der ENISA werden mehr Modelle für die Zusammenarbeit in vorher festgelegten Bereichen (Sensibilisierung, Reaktion auf Vorfälle und Kapazitätenaufbau von Kleinstunternehmen im Bereich der NIS) entwickeln und dabei auf der bereits geleisteten Arbeit aufbauen. Zudem wird die Agentur die institutionalisierte Verbreitung europäischer bewährter Verfahren im Bereich der NIS weiterentwickeln, unter anderem mit Hilfe von Instrumenten wie der Online-Plattform zur Förderung des Dialogs, einem Who-is-Who-Verzeichnis, Länderseiten und Länderberichten über die Aktivitäten in den Mitgliedstaaten. Ein Highlight werden verschiedene thematische Workshops zur Stärkung der Beziehungen zu bestehenden Gemeinschaften von NIS-Akteuren (z. B. Computer Emergency Response Teams, CERT) oder der Aufbau neuer Gemeinschaften sein, die ein gemeinsames Interesse an spezifischen NIS-Themen (z. B. Sensibilisierung) haben. Die Agentur wird ihre Kontakte und Netzwerke nutzen, z. B. das Netz nationaler Verbindungspersonen und ausgewählte nationale Stellen.	
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):	
SMART-Ziel: Bis 2010 haben sich mindestens zehn Mitgliedstaaten an mindestens drei verschiedenen Kooperationsmodellen beteiligt.	**KPI:** Zahl der beteiligten Mitgliedstaaten, Zahl der Kooperationsmodelle
VORRANGIGE ZIELE, DIE DURCH DAS PROGRAMM UNTERSTÜTZT WERDEN:	
Stärkung des Vertrauens in das Informationszeitalter durch die Verbesserung der Fähigkeiten der Mitgliedstaaten im Bereich der NIS.	
Ausweitung der Zusammenarbeit zwischen den Mitgliedstaaten mit dem Ziel, die unterschiedlichen Fähigkeiten der Mitgliedstaaten auf diesem Gebiet auf ein einheitliches Niveau zu bringen. Intensivierung des Dialogs über NIS zwischen den verschiedenen Akteuren in der EU.	
AKTEURE UND BEGÜNSTIGTE:	
Regierungen der Mitgliedstaaten (und nationale Regulierungsbehörden), Kommission, Industrie, Hochschulen, sonstige Gruppen von Interessenvertretern	
WARUM DIE ENISA?	
Aufgrund ihrer besonderen Rolle kann die ENISA die Mitgliedstaaten und die Kommission bei der Verbesserung ihrer Fähigkeiten auf dem Gebiet der Netz- und Informationssicherheit beraten und unterstützen. Die ENISA bietet eine unabhängige europaweite Plattform zur Förderung der Zusammenarbeit zwischen den Mitgliedstaaten und fungiert dabei als vertrauenswürdiger Vermittler. Die Agentur hat bereits wertvolle Arbeit geleistet, unter anderem in den Bereichen Sensibilisierung und CSIRT, mit der Durchführung einer Machbarkeitsstudie über ein europäisches Informationsaustausch- und Warnsystem und durch ihre Vermittlungsfunktion zwischen den Mitgliedstaaten und Kleinstunternehmen.	
VORSCHLAG FÜR DAS PROGRAMM:	
ENISA, Verwaltungsrat, Ständige Gruppe der Interessenvertreter	
RECHTSGRUNDLAGE:	
ENISA-Verordnung, Artikel 3 Buchstaben c, d und e	

2.2.1 Arbeitspaket 2.1 – Plattform für die Zusammenarbeit bei der Sensibilisierung

Bezeichnung des TMP:	
Entwicklung und Fortführung von Kooperationsmodellen	
BEZEICHNUNG DES ARBEITSPAKETS:	
Arbeitspaket 2.1: Plattform für die Zusammenarbeit bei der Sensibilisierung	
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):	
SMART-Ziel: Bis zum 4. Quartal 2010 sind mit der Unterstützung der Sensibilisierungsgemeinschaft mindestens fünf Weißbücher erarbeitet worden. Bei der Auswahl der Themen werden die Zusammensetzung der Sensibilisierungsgemeinschaft (z. B. die Interessen der Mitglieder) sowie von der Agentur durchgeführte Forschungen und Erhebungen berücksichtigt.	**KPI:** Zahl der Weißbücher
SMART-Ziel: Bis zum 2. Quartal 2010 wird eine Konferenz mit mindestens 100 Teilnehmern aus mindestens zehn verschiedenen EU-Mitgliedstaaten organisiert.	**KPI:** Zahl der Teilnehmer, Zahl der vertretenen EU-Mitgliedstaaten
BESCHREIBUNG DES ARBEITSPAKETS:	
Ziel dieses Arbeitspakets ist es, die Sensibilisierungsgemeinschaft weiterzuentwickeln und zu stärken und sie als wertvolle Plattform für die Zusammenarbeit bei der Sensibilisierung für Netz- und Informationssicherheit und für die europaweite Verbreitung bewährter NIS-Verfahren zu etablieren. Zudem soll die Sensibilisierungsgemeinschaft die ENISA bei ihrer Aufgabe unterstützen, eine Kultur der Informationssicherheit zu fördern. Zur Erreichung dieses Ziels wurden zwei wichtige Komponenten benannt: Sensibilisierungsgemeinschaft und Sensibilisierungskonferenz. **Sensibilisierungsgemeinschaft** Die ENISA wird die Sensibilisierungsgemeinschaft auch nach zwei Jahren des raschen Wachstums weiter ausbauen und stärken. Die Agentur wird den Dialog, den Austausch von bewährten Verfahren und Wissen unter Zuhilfenahme verschiedener Kommunikationsmittel fördern. Dabei sollen aktuelle Themen, wichtige Fragen und neue bewährte Verfahren im Bereich der Sensibilisierung vorgestellt und diskutiert werden. Die Mitglieder der Sensibilisierungsgemeinschaft werden aufgefordert, die Abteilung Sensibilisierung der ENISA in ihrer Aufgabe, eine Kultur der Informationssicherheit zu fördern, zu unterstützen. Die Mitglieder fungieren als Kontaktstelle für Fragen im Bereich der Sensibilisierung für die Informationssicherheit im Allgemeinen oder in Bezug auf das jeweilige Land, die jeweilige Branche oder den jeweiligen Tätigkeitsbereich. Außerdem unterstützen die Mitglieder die Arbeit der Agentur unter anderem durch die Beteiligung an Diskussionen, die Erarbeitung von Weißbüchern für spezifische Sicherheitsfragen (einschließlich der Sensibilisierung der KMU) und durch ihre Teilnahme an virtuellen Arbeitsgruppen, die auf der vorhandenen Arbeit aufbauen. Sachdienliches Material wird über das Sensibilisierungsportal zur Verfügung gestellt (z. B. Berichte, Schulungsmaterial und Merkblätter). **Sensibilisierungskonferenz** Im 2. Quartal 2010 wird die ENISA eine Konferenz zu aktuellen bewährten Verfahren im Bereich der Sensibilisierung organisieren. Die Themen für diese Konferenz werden auf der Grundlage der Erkenntnisse der ENISA und der Sensibilisierungsgemeinschaft auf dem Gebiet der Sensibilisierung für Fragen der Informationssicherheit ausgewählt.	
ERGEBNISSE UND TERMINE:	
Konferenz zum Thema Sensibilisierung mit dem Ziel, Informationsmaterial und Empfehlungen über bewährte Verfahren vorzustellen und die Zusammenarbeit zwischen den Mitgliedstaaten zu fördern (Q2 2010). Interne Kontaktliste von Experten für Sensibilisierungsfragen, die an der einschlägigen Arbeit der ENISA-Sensibilisierungsgemeinschaft beteiligt sind (noch nicht abgeschlossen; Q4 2010).	

FOLGENDE INTERESSENVERTRETER SOLLTEN DAS ARBEITSPAKET AKTIV UNTERSTÜTZEN:
Mitgliedstaaten, Ständige Gruppe der Interessenvertreter (SGI), Industrieverbände, Sensibilisierungsgemeinschaft
RESSOURCEN FÜR 2010 (Personenmonate und Haushaltsmittel):
• 24 Personenmonate; • 60 000 EUR
VORSCHLAG FÜR DAS ARBEITSPAKET:
ENISA
RECHTSGRUNDLAGE:
ENISA-Verordnung, Artikel 3 Buchstaben c, d und e

2.2.2 Arbeitspaket 2.2 – Sicherheitskompetenzkreis und Austausch bewährter Verfahren für die CERT-Gemeinschaft

Bezeichnung des TMP:	
Entwicklung und Fortführung von Kooperationsmodellen	
BEZEICHNUNG DES ARBEITSPAKETS:	
Arbeitspaket 2.2: Sicherheitskompetenzkreis und Austausch bewährter Verfahren für die CERT-Gemeinschaft	
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):	
SMART-Ziel: Bis zum 4. Quartal 2010 mindestens zehn Bezugnahmen auf Informationsmaterial über bewährte Verfahren der ENISA, „CERT-Dienste“, auf externen Websites, in amtlichen Veröffentlichungen, Diskussionen über Mailing-Listen oder sonstigen Medien.	**KPI:** Zahl der Bezugnahmen
SMART-Ziel: Bis zum 4. Quartal 2010 mindestens zehn Bezugnahmen auf Referenzmaterial der ENISA zur Unterstützung der europaweiten Zusammenarbeit nationaler und staatlicher CERT auf externen Websites, in amtlichen Veröffentlichungen, Diskussionen über Mailing-Listen oder sonstigen Medien.	**KPI:** Zahl der Bezugnahmen
SMART-Ziel: Mindestens 50 % der EU-Bevölkerung wird durch die Teilnehmer auf dem CERT-Workshop vertreten.	**KPI:** % der vertretenen EU-Bevölkerung
SMART-Ziel: Die Workshop-Teilnehmer bewerten den CERT-Workshop mit mindestens einer 3 auf einer Skala von 1 bis 5.	**KPI:** Durchschnittliches Feedback auf einer Skala von 1 bis 5
SMART-Ziel: Bis zum 4. Quartal 2010 werden mindestens drei Präsentationen über die Arbeit der ENISA im Bereich CERT auf Veranstaltungen der CERT-/CSIRT-Gemeinschaften vorgestellt.	**KPI:** Zahl der Präsentationen
SMART-Ziel: Bis zum 4. Quartal 2010 wurden 80 % der Aktualisierungen im ENISA-Verzeichnis der CERT-Tätigkeiten in Europa bestätigt.	**KPI:** % der bestätigten Aktualisierungen
SMART-Ziel: Bis zum 4. Quartal 2010 wurden mindestens zwei TRANSITS-Schulungen mit Unterstützung der ENISA organisiert.[8]	**KPI:** Zahl der unterstützten Schulungen

[8] Unter der Voraussetzung, dass der Veranstalter der vorhergehenden regelmäßigen TRANSITS-Kurse seine Tätigkeit fortsetzt.

BESCHREIBUNG DER AUFGABEN:

Die Arbeit der ENISA auf dem Gebiet der CERT-Zusammenarbeit und -Unterstützung ist an einem Wendepunkt angekommen: fast alle EU-Mitgliedstaaten verfügen über mindestens ein Response Team, das bei der Verwaltung und Meldung von Sicherheitsvorfällen als Zwischenkontakt fungieren kann, oder haben Projekte zur Einrichtung eines solchen Teams initiiert. Einige Mitgliedstaaten haben jedoch noch immer kein offizielles nationales oder staatliches CERT mit einem offiziellen Auftrag zur Durchführung von Diensten zum Schutz der nationalen Informationsinfrastruktur und zur Zusammenarbeit mit den nationalen und staatlichen CERT in anderen Mitgliedstaaten eingerichtet. Daher konzentriert sich die Arbeit der ENISA in diesem Jahr auf die weitere Vereinfachung der Einrichtung, Schulung und des Einsatzes nationaler und staatlicher CERT und deren Zusammenarbeit auf europäischer Ebene. Besonderer Schwerpunkt wird hierbei auf die Förderung der Zusammenarbeit nationaler und staatlicher CERT gelegt. Hierzu werden Diskussionen mit den Interessenvertretern angeregt und Vereinbarungen bezüglich der Fähigkeiten, Anforderungen, Bedürfnisse, Hindernisse und sonstigen Problempunkte getroffen, damit alle Mitgliedstaaten sich an den Maßnahmen zum Austausch von Informationen über Sicherheitsvorfälle, Schwachstellen und andere Aspekte zum Schutz kritischer Informationsinfrastrukturen beteiligen können.

Bewährte Verfahren bei der Bereitstellung von CERT-Diensten

Ausgehend von der Erhebung aus dem Jahr 2009, in deren Rahmen eine Reihe von grundlegenden Fähigkeiten für nationale und staatliche CERT in Europa erarbeitet wurde, wird eine weiterführende gründliche Analyse der bewährten Verfahren für die Bereitstellung der CERT-Dienste angefertigt. Die ENISA wird einen Leitfaden für bewährte Verfahren für einen bestimmten Dienst erarbeiten, der in der Liste als bedeutsam hervorgehoben wurde und für den bisher noch keine bewährten Verfahren verfügbar sind. Zu den vielversprechenden Diensten zählen unter anderem die Folgenden:

- Überwachungs- und Frühwarnsystem (sowie verwandte Themen wie die Erkennung von Anomalien, die Korrelation von Ereignissen, Sensorennetze usw.)
- Ermittlung und Offenlegung von Schwachstellen
- Analyse von Malware (sowie verwandte Themen wie Honeypots und Honeynets, Malware-Datenbanken usw.)

Die Zusammenarbeit und den Informationsaustausch verbessern

Die Zusammenarbeit und der Austausch von Informationen auf europäischer Ebene spielen für die nationalen und staatlichen CERT im Rahmen der europaweiten Verwaltung von Sicherheitsvorfällen eine wichtige Rolle. Die ENISA wird daher Überlegungen anstellen, wie sie die Gemeinschaft auch weiterhin darin unterstützen kann, die Zusammenarbeit und den Informationsaustausch zu erleichtern. Ausgangspunkt dieser Überlegungen ist ein Referenzdokument über die Unterstützung der europaweiten Zusammenarbeit von nationalen und staatlichen CERT, das wiederum auf dem Bericht „CERT cooperation and its further facilitation by relevant stakeholders“ („Zusammenarbeit von CERT und weitere Förderung der Zusammenarbeit durch maßgebliche Akteure“) aus dem Jahr 2006 basiert. Der genannte Bericht wird mit besonderem Blick auf die organisatorischen Bedürfnisse der Mitgliedstaaten im Bereich des Informationsaustauschs aktualisiert. Erfahrungen mit Einrichtungen wie der European Government CERT Group (EGC) und sektorbezogenen Aktionszentren „Informationsgesellschaft“ (ISAC) fließen ebenfalls in dieses Dokument ein. Das Dokument bietet der ENISA auch einen Einblick in die entscheidenden Schritte, mit denen sich die Gemeinschaft für die kommenden Jahre rüsten kann. Die relevanten Interessenvertreter begleiten und erörtern die Erarbeitung dieses neuen Dokuments im Rahmen geeigneter Instrumente wie den Ad-hoc-Arbeitsgruppen, Präsentationen auf CERT-Sitzungen usw.

Die Fähigkeiten der Mitgliedstaaten verbessern – Folgemaßnahmen zu EISAS

Im Zeitraum 2006-2007 führte die ENISA eine an die Bürger und KMU gerichtete Studie zur Bewertung der Machbarkeit eines Europäischen Informations- und Warnsystems (European Information Sharing and Alerting System, EISAS) durch. In den Jahren 2009 und 2010 werden zur Umsetzung der Ergebnisse dieser Studie zwei sich ergänzende Pilotprojekte durchgeführt, die finanziell von der Europäischen

Kommission gefördert werden. In ihrer Mitteilung KOM(2009) 149 endgültig forderte die Europäische Kommission die ENISA auf, eine Bestandsaufnahme der Ergebnisse dieser Vorhaben und anderer nationaler Initiativen bis Ende 2010 vorzunehmen und einen Fahrplan zu erstellen, um die Entwicklung und Einführung des EISAS zu unterstützen. Im Jahr 2009 begann die ENISA damit, die Fortschritte dieser beiden Projekte zu überwachen; abhängig von der Verfügbarkeit der Projektleiter werden die Fortschritte auch im Jahr 2010 weiter überwacht. Die ENISA plant, bis Ende 2010 einen Entwurf des Fahrplans vorzulegen und bei dessen Erstellung die Ergebnisse aus den Projekten und anderen (nationalen) Initiativen zu berücksichtigen. Der Fahrplan soll für die Bürger und KMU als eine Art Wegweiser für die weiteren Entwicklungen auf dem Gebiet des Informationsaustauschs dienen.

5. ENISA-Workshop „CERT in Europa"

Im Rahmen dieses Workshops für wichtige Akteure in den Mitgliedstaaten und der Europäischen Kommission sucht die ENISA den Dialog mit den Interessenvertretern. Der 5. Workshop zu „CERT in Europa" behandelt insbesondere die Rolle der nationalen und staatlichen CERT im Zusammenhang mit Übungsmaßnahmen auf nationaler und internationaler Ebene; im Mittelpunkt steht hierbei der Austausch von Informationen zu bewährten methodologischen und organisatorischen Verfahren für die nationalen und staatlichen CERT, die mit der Durchführung von Übungen zum Schutz kritischer Informationsinfrastrukturen in ihrem jeweiligen Mitgliedstaat befasst sind. Darüber hinaus wird im Rahmen dieses Workshops auch die Beteiligung an internationalen Übungen wie ASEAN, Cyberstorm usw. erörtert. Die Ergebnisse aus diesem Workshop dienen als Grundlage für die Bewertung der weiteren Schritte, die die ENISA gemeinsam mit den relevanten Interessenvertretern ergreifen kann, um die Fähigkeiten der nationalen und staatlichen CERT im Rahmen von Übungen auf nationaler und internationaler Ebene zu stärken. Zudem soll mit Hilfe der gewonnenen Erkenntnisse der Übungsrahmen leichter definiert werden können, der unter dem Arbeitspaket 1.4 zu TMP 1 („Verbesserung der Widerstandsfähigkeit der europäischen elektronischen Kommunikationsnetze") beschrieben ist.

Die Einrichtung von CERT/CSIRT weiter fördern und enge Beziehungen zu den verschiedenen CERT-/CSIRT-Gemeinschaften unterhalten

Die ENISA hat Hilfsmittel (wie die Leitfäden für die Einrichtung und den Betrieb eines CSIRT, den Kooperationsleitfaden und die Sammlung von CSIRT-Übungen) zur Unterstützung der CERT-Gemeinschaft und ihrer Zusammenarbeit entwickelt und wird diese Arbeit fortsetzen. Dabei konzentriert sie sich auf die Unterstützung der Einrichtung neuer staatlicher/nationaler CERT in den Mitgliedstaaten. Zu diesem Zweck wird die Unterstützung der sehr erfolgreichen, zweimal im Jahr veranstalteten TRANSITS-Schulungen für CSIRT-Teammitglieder fortgesetzt. Anfragen der Mitgliedstaaten für spezielle Schulungen für CERT-Teammitglieder können – wie in der Vergangenheit geschehen – aufgegriffen werden, um Lücken bei den CERT-Diensten in Europa, speziell bei den staatlichen/nationalen CERT zu schließen. Das ENISA-Verzeichnis der CERT-Tätigkeiten in Europa wird entsprechend den europaweiten Entwicklungen aktualisiert.

Präsentation und Repräsentation

Die ENISA wird ihre Rolle als bewährter unabhängiger Kontaktvermittler für verschiedene europäische und internationale CERT-Gemeinschaften wie TF-CSIRT und FIRST weiter festigen. Sie erreicht dies durch die Vorstellung ihrer Tätigkeit bei von diesen Gemeinschaften organisierten Veranstaltungen. Die Gemeinschaften können ihrerseits durch ihre Rückmeldung Einfluss auf die Arbeit der Agentur ausüben.

ERGEBNISSE UND TERMINE:

- ENISA-Leitfaden für bewährte Verfahren bei der Bereitstellung eines CERT-Diensts (Q4)
- ENISA-Referenzdokument über die europaweite Zusammenarbeit von nationalen und staatlichen CERT (Q4)
- Entwurf des Fahrplans zu „EISAS" (Q4 2010)
- 5. ENISA-Workshop „CERT in Europa" (Q2)
- Aktualisiertes „ENISA-Verzeichnis der CERT-Tätigkeiten in Europa" (Q2 und Q4 2009)
- Unterstützung von mindestens zwei TRANSITS-Schulungen bis Q4

FOLGENDE INTERESSENVERTRETER SOLLTEN DAS ARBEITSPAKET AKTIV UNTERSTÜTZEN:

EU-Mitgliedstaaten (insbesondere nationale CSIRT), Europäische Kommission, CERT-Gemeinschaft

RESSOURCEN FÜR 2009 (Personenmonate und Haushaltsmittel):
• 135 000 EUR (Workshop, Sitzungen, Beratung, Unterstützung von Übungen, Unterstützung für die TRANSITS-Schulungen) • 24 Personenmonate
VORSCHLAG FÜR DAS ARBEITSPAKET:
ENISA, Europäische Kommission
RECHTSGRUNDLAGE:
ENISA-Verordnung, Artikel 3 Buchstaben c, d und e

2.2.3 Arbeitspaket 2.3 – Institutionalisierte Verbreitung europäischer bewährter Verfahren im Bereich der NIS

Bezeichnung des TMP:	
Entwicklung und Fortführung von Kooperationsmodellen	
BEZEICHNUNG DES ARBEITSPAKETS:	
Arbeitspaket 2.3: Institutionalisierte Verbreitung europäischer bewährter Verfahren im Bereich der NIS	
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):	
SMART-Ziel: Bis zum 3. Quartal 2010 Veröffentlichung von Länderberichten und des Who-is-Who-Verzeichnisses bezüglich der relevanten NIS-Strategien, der ordnungspolitischen Praktiken (Governance-Praktiken) und Kontakte auf dem Gebiet der Robustheit kritischer Informationsinfrastrukturen, der elektronischen Identität und der Meldung von Verletzungen des Schutzes personenbezogener Daten in allen Mitgliedstaaten (einschließlich EWR- und EFTA-Länder)	**KPI:** Zahl der ermittelten bewährten Verfahren bezüglich der Robustheit kritischer Informationsinfrastrukturen, elektronischer Identitäten und der Meldung von Verletzungen des Schutzes personenbezogener Daten
SMART-Ziel: Bis zum 4. Quartal 2010 Einleitung von Projekten zur institutionalisierten Verbreitung bewährter Verfahren bezüglich der Robustheit kritischer Informationsinfrastrukturen, der elektronischen Identität und der Meldung von Verletzungen des Schutzes personenbezogener Daten für jene Länder, für die in den Länderberichten ein diesbezügliches Erfordernis festgestellt wurde	**KPI:** Zahl der Interessenvertreter und Zahl der Länder, die sich an Projekten zur institutionalisierten Verbreitung bewährter Verfahren bezüglich der Robustheit kritischer Informationsinfrastrukturen, der elektronischen Identität und der Meldung von Verletzungen des Schutzes personenbezogener Daten beteiligen, unter Berücksichtigung der in den Länderberichten festgestellten Erfordernisse auf diesem Gebiet
BESCHREIBUNG DER AUFGABEN:	

Seit 2007 fördert die ENISA im Rahmen der institutionalisierten Verbreitung europäischer bewährter Verfahren im Bereich der NIS gemeinsame Projekte zwischen den EU-Mitgliedstaaten.

Frühere Verbreitungsmaßnahmen umfassten Folgendes:

- Im Bereich der *CERT* hat die ENISA Kooperationsprojekte zwischen Ungarn und Bulgarien für den Aufbau eines CERT der bulgarischen Regierung sowie zwischen dem CERT-FI (Finnland) und dem CSIR/MERAKA (Südafrika) bezüglich des Austauschs bewährter Verfahren und des Aufbaus eines CSIRT in Südafrika unterstützt.
- Im *Finanzbereich* hat die ENISA die Entwicklung einer öffentlich-privaten Partnerschaft für den strukturierten Austausch von Informationen im Zusammenhang mit Computerkriminalität zwischen dem Finanzsektor und den Regierungen mit Hilfe der Zentren für Finanzinformationen und -analysen (Financial Information and Analysis Centers, FI-ISAC) gefördert. An dieser Partnerschaft sind mehr als 15 Länder sowie relevante Interessenvertreter aus dem privaten Sektor vertreten.
- Im Bereich der *Sensibilisierung* hat die ENISA im Jahr 2009 eine Sitzung der lokalen Regierungen in Skandinavien zum Thema Informationssicherheit auf den Weg gebracht, in der die Erarbeitung von Methoden zum Austausch bewährter Verfahren für die Verwaltung der Informationssicherheit in den Gemeinden und Regionen in Dänemark, Schweden und Norwegen erörtert wurde.
- In den Bereichen *Widerstandsfähigkeit und CERT* möchte die ENISA Ende 2009 oder Anfang 2010 ein Kooperationsprojekt zwischen Malta und einem oder gar mehreren anderen Ländern ins Leben rufen.

Um das allgemeine Niveau der NIS in Europa anzuheben, ist eine wesentliche Verbesserung der Zusammenarbeit zwischen den Mitgliedstaaten und dem privaten Sektor von grundlegender

Bedeutung. In ihrer Mitteilung über den Schutz kritischer Informationsinfrastrukturen („Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität“) aus dem Jahr 2009 fordert die Europäische Kommission ein neues europäisches ordnungspolitisches Modell unter Mitwirkung aller Beteiligten, in dessen Rahmen „der Privatsektor stärker an der Festlegung ordnungspolitischer Ziele [...] beteiligt werden [könnte]“ (vgl. Kapitel 3.4.2 der Mitteilung). Aufbauend auf seinen ersten Erfolgen im Finanzsektor wird die ENISA die institutionalisierte Verbreitung nicht nur in den Mitgliedstaaten (einschließlich EWR-Länder) und in Drittländern weiterentwickeln, sondern auch in den größeren Organisationen des öffentlichen und privaten Sektors. Hierdurch soll Folgendes erreicht werden:

1. die Vermittlung bewährter Verfahren zwischen Ländern mit bereits entwickelten Strukturen und Ländern ohne solche Strukturen;
2. die Ermittlung und Entwicklung neuer Governance-Praktiken, die infolge neu aufkommender Bedrohungen in einigen oder gar in allen Ländern erforderlich werden.

Im Jahr 2010 soll das Arbeitspaket für die institutionalisierte Verbreitung von bewährten Verfahren noch stärker in die im Rahmen von TMP 1 und VM 1 geleistete Arbeit integriert werden. Bei Kooperationsprojekten liegt der Schwerpunkt daher insbesondere auf der Entwicklung von Methoden zum Austausch von bewährten Verfahren in Bezug auf *widerstandsfähige, nachhaltige und sichere Infrastrukturen und Dienste*, den weiteren Ausbau nationaler und staatlicher *Computer Emergency Response Teams (CERT),* die *Entwicklung öffentlich-privater Kooperationsforen wie EISAS und das FI-ISAC* und Bezug auf die Bereiche *elektronische Identität, Authentifizierung, Datenschutz, Privatsphäre und Nutzervertrauen.* Ziel ist es, zentrale Maßnahmen für die Mitgliedstaaten zu erarbeiten und so ein hohes Maß an Sicherheit und Nutzervertrauen in einer Reihe wirtschaftlich bedeutender, sich schnell ändernder Sektoren zu erhalten.

Im Hinblick auf die Ermittlung bewährter Verfahren und potenzieller Partner für Kooperationsprojekte in diesen wesentlichen Bereichen wird die Agentur auf dem bereits erarbeiteten Fachwissen aufbauen und die Schwerpunkte der vorhandenen Länderberichte stärker auf die Strategien und Governance-Praktiken bezüglich der Robustheit kritischer Informationsinfrastrukturen, der elektronischen Identität, der Authentifizierung und der Verwaltung personenbezogener Daten (insbesondere die Meldung von Verletzungen des Schutzes solcher Daten) ausrichten. Die Berichte stellen somit ein Verzeichnis aller vorhandenen bewährten Verfahren im Bereich der NIS dar und werden durch ein Who-is-Who-Verzeichnis mit ähnlich verlagertem Schwerpunkt ergänzt, in dem alle relevanten Interessenvertreter (öffentlich und privat) in diesen Bereichen aufgeführt sind.

Die institutionalisierte Verbreitung europäischer bewährter Verfahren im Bereich der NIS wird durch eine Online-Plattform unterstützt (in Form eines Extranets für relevante Interessenvertreter, dessen Entwicklung die ENISA für September 2009 geplant hat). Diese Plattform enthält Informationen zu abgeschlossenen und laufenden Kooperationsprojekten, ein Verzeichnis der bewährten Verfahren im Bereich der NIS sowie die Online-Ausgaben der Länderberichte und des Who-is-Who-Verzeichnisses. Die Online-Plattform soll als Informationsquelle für bewährte Verfahren im Bereich der NIS und als Instrument dienen, mit dessen Hilfe die richtigen potenziellen Ansprechpartner für die Kooperationsprojekte ermittelt und kontaktiert werden können.

ERGEBNISSE UND TERMINE:

Gemeinsame Projekte (Q4 2010)
Länderberichte und das Who-is-Who-Verzeichnis (Q3 2010)
Online-Plattform (laufendes Projekt, Q2 2010)

FOLGENDE INTERESSENVERTRETER SOLLTEN DAS ARBEITSPAKET AKTIV UNTERSTÜTZEN:

Mitgliedstaaten: Verwaltungsrat, nationale Verbindungspersonen, SGI, Netzwerke verschiedener „sektorbezogener Themengemeinschaften im privaten Sektor“ (z. B. Industrie, Nutzer/Verbraucher und Hochschulen)

RESSOURCEN FÜR 2010 (Personenmonate und Haushaltsmittel):

- 120 000 EUR
- 7 Personenmonate

VORSCHLAG FÜR DAS ARBEITSPAKET:
ENISA
RECHTSGRUNDLAGE:
ENISA-Verordnung, Artikel 3 Buchstaben c und d

2.3. TMP 3: Ermittlung aufkommender Risiken zum Zwecke der Vertrauensbildung

BEZEICHNUNG DES PROGRAMMS:
Ermittlung aufkommender Risiken zum Zwecke der Vertrauensbildung
BESCHREIBUNG DES PROBLEMS
Entscheidungsträger im öffentlichen wie auch im privaten Sektor haben häufig nur unklare Vorstellungen über die Art und die Auswirkungen neu aufkommender Probleme der Netz- und Informationssicherheit in der Informationsgesellschaft. Diese Herausforderungen sind mit den Sicherheitsrisiken neuer und künftiger Anwendungen und Technologien verbunden, die auf den europäischen Markt kommen. Durch ein besseres Verständnis der aufkommenden Risiken wären die Akteure des öffentlichen und privaten Sektors besser in der Lage, fundierte Entscheidungen zu treffen und somit eine zweckmäßigere Grundlage für die politische Entscheidungsfindung zu schaffen. Im Jahr 2010 wird die ENISA für bestimmte Anwendungs- und Technologieszenarien Risikobewertungsberichte zu neu aufkommenden Risiken bereitstellen. Diese Szenarien spiegeln die Ansichten verschiedener Interessenvertreter aus ganz Europa wider, tragen gleichzeitig jedoch auch Tätigkeiten der ENISA mit Bezug auf die Ermittlung aufkommender Risiken als Querschnittsthema (z. B. im Rahmen von VM 1) Rechnung.
BESCHREIBUNG DES ANSATZES ZUR LÖSUNG DES PROBLEMS:
In den Jahren 2008 und 2009 hat die Agentur mit der *Rahmenstruktur für aufkommende Risiken* ein Konzept entwickelt, das den Interessenvertretern helfen soll, die mit neuen Technologien und Anwendungen verbundenen aufkommenden Risiken besser zu erkennen und zu verstehen. Darüber hinaus hat die ENISA in den Jahren 2008 und 2009 Expertengruppen eingerichtet, die die eingereichten Szenarien aus Risikosicht validieren und analysieren sollen. Das ENISA-Forum von Interessenvertretern stand der Agentur bei ihren Tätigkeiten zu aufkommenden Risiken mit entsprechenden Empfehlungen und Rückmeldungen zur Seite und war somit richtungsweisend. Das Forum von Interessenvertretern zu aufkommenden Risiken wird seine Tätigkeit auch im Jahr 2010 fortsetzen. Neben dem Forum von Interessenvertretern werden Gruppen von Sachverständigen (z. B. virtuelle Expertengruppen, Sachverständige) mit ihrem spezifischen Know-how und Fachwissen die Analyse und Ermittlung aufkommender Risiken für ausgewählte Technologien und Anwendungen unterstützen, wie im Arbeitsprogramm 2009 vorgesehen. Beide Gruppen sind im Rahmen des Arbeitsprogramms 2010 an weiteren ENISA-Aktivitäten beteiligt (insbes. VM 1). Mit der Rahmenstruktur für aufkommende Risiken unterstützt die Agentur das Arbeitsprogramm, indem sie Risikobewertungsberichte zu Szenarien aus Bereichen erstellt, die sich auf das TMP 1 und die VM 1 beziehen. Die Arbeit der ENISA zur Entwicklung der Rahmenstruktur für aufkommende Risiken ist auf die Förderung eines proaktiven Ansatzes für den Umgang mit den neuen und künftigen Herausforderungen neu aufkommender Technologien und Anwendungen ausgerichtet. Mit dieser Maßnahme soll das Vertrauen der Nutzer in die Informationsgesellschaft, insbesondere in zentralen Bereichen wie der Widerstandsfähigkeit von Netzen und der Vertrauensbildung, gestärkt werden. In diesem Zusammenhang findet die Rahmenstruktur bei der Ermittlung aufkommender Risiken mehr und mehr auch in andere TMP der ENISA Eingang und bietet so bereichsübergreifende Unterstützung. Innerhalb dieses TMP legt die ENISA ein Verfahren für die Ermittlung von zu analysierenden Themen und möglichen Szenarien fest (d. h. ein konzeptioneller Fahrplan für die Auswahl von Themen, die Auswahl von Szenarien und die Kommunikation). Dieses Verfahren wird der ENISA bei der Auswahl helfen, welche Szenarien aus welchen thematischen Bereichen analysiert werden sollen. Zur Unterstützung der Tätigkeit der Kommission auf dem Gebiet des Schutzes kritischer Informationsinfrastrukturen und insbesondere im Hinblick auf die europaweiten Übungen wird die ENISA eine erste Bewertung all jener Elemente vornehmen, die für die nationalen Vorsorgemaßnahmen im Rahmen des Risikomanagements relevant sind. Daraus ergibt sich eine Sammlung von Bereichen und

Aspekten, die als Teil des Portfolios der nationalen Vorsorgemaßnahmen im Rahmen des Risikomanagements gelten. Anschließend werden die zentralen Schwerpunktbereiche und Komponenten, die Bestandteil einer europaweiten Übung sein können, auf der Grundlage des jeweiligen Risikoprofils ermittelt. Darauf aufbauend können verschiedene Übungsszenarien erarbeitet werden. Diese Aktivität wird von einer Gruppe einschlägiger Experten – einer Arbeitsgruppe – aus ganz Europa durchgeführt und im Rahmen der Maßnahmen zum Arbeitspaket 1.4 koordiniert.

Schließlich sollte noch darauf hingewiesen werden, dass innerhalb dieses TMP bestehende ähnliche Initiativen sowohl zu aufkommenden Risiken und Bedrohungen als auch zum Schutz kritischer Informationsinfrastrukturen Berücksichtigung finden. Schnittstellen zu relevanten Forschungsprogrammen und -aktivitäten der Europäischen Kommission wurden erstellt, und die ENISA steht bei der Ermittlung weiterer maßgeblicher Initiativen (z. B. die Zusammenarbeit mit den Mitgliedstaaten bezüglich der geplanten Empfehlung zu RFID) auch weiterhin in engem Kontakt mit der Kommission.

VORRANGIGE ZIELE, DIE DURCH DAS PROGRAMM UNTERSTÜTZT WERDEN:

Förderung des Binnenmarkts für elektronische Kommunikation durch die Unterstützung der europäischen Akteure bei der Festlegung einer geeigneten Mischung aus technischen, organisatorischen und ordnungspolitischen Maßnahmen (unter besonderer Berücksichtigung des wichtigen Beitrags, den die Agentur zur Rahmenrichtlinie leisten kann); Intensivierung des Dialogs über NIS zwischen den verschiedenen Akteuren in der EU; Stärkung des Vertrauens in das Informationszeitalter durch die Anhebung des Niveaus der NIS in der EU

ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):

SMART-Ziel: Bis Ende 2010 werden mindestens 20 Interessenvertreter oder Interessenvertreter-Organisationen aus mindestens zehn Mitgliedstaaten in der Diskussion über Art und Auswirkungen neuer Sicherheitsherausforderungen der Informationsgesellschaft auf die ENISA Bezug nehmen.	**KPI:** Zahl der Interessenvertreter, Zahl der Mitgliedstaaten

AKTEURE UND BEGÜNSTIGTE:

Entscheidungsträger im öffentlichen und privaten Sektor, wie zum Beispiel Regierungen der Mitgliedstaaten, Industrie, FuE-Einrichtungen, Softwareentwickler, Systemintegratoren und Normungsgremien, die zu analysierende Szenarien über aufkommende Risiken beisteuern

WARUM DIE ENISA?

Die ENISA kann die relevanten Akteure zusammenbringen, um den Dialog und den Informationsaustausch auf europäischer Ebene zu fördern.

In den Jahren 2008 und 2009 nahm die ENISA eine Bewertung der mit neuen Anwendungen verbundenen Risiken für die Informationssicherheit vor, setzte einen Fahrplan um und führte Studien über Mechanismen zur Beschaffung, Verarbeitung und Weitergabe von Informationen über aufkommende Risiken durch. Gleichzeitig wurde eine Reihe von Positionspapieren über Technologietrends und Risiken für neu entstehende Bereiche verfasst, und die hierfür erforderlichen Beratergruppen (d. h. Sachverständige) wurden eingerichtet.

Die ENISA hat ein Forum von Interessenvertretern eingerichtet, dem bei der Bewertung und Analyse aufkommender Risiken eine tragende Rolle zukommt, und verfügt über einen Pool von Sachverständigen, die in der Lage sind, die Risiken neuer Anwendungs- und Technologieszenarien zu bewerten.

Die ENISA trägt zu der Arbeit zum Schutz kritischer Informationsinfrastrukturen bei und kann wertvolle Beiträge für die europaweiten Übungen leisten.

VORSCHLAG FÜR DAS PROGRAMM:

ENISA, Verwaltungsrat, Ständige Gruppe der Interessenvertreter

RECHTSGRUNDLAGE:

ENISA-Verordnung, Artikel 3 Buchstaben a, c, d, e, f, g, i und k

2.3.1 Arbeitspaket 3.1 – Konzept für die Bewertung und Diskussion aufkommender Risiken – Analyse konkreter Szenarien

Bezeichnung des TMP:	
Ermittlung aufkommender Risiken zum Zwecke der Vertrauensbildung	
BEZEICHNUNG DES ARBEITSPAKETS:	
Arbeitspaket 3.1 – Konzept für die Bewertung und Diskussion aufkommender Risiken – Analyse konkreter Szenarien	
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):	
SMART-Ziel: Bis zum 4. Quartal 2010 soll die Zufriedenheit der Interessenvertreter, die an der Analyse von Szenarien zu aufkommenden Risiken beteiligt sind, bei mindestens 3 liegen (auf einer Skala von 1-5, wobei 1 = gering und 5 = sehr hoch).	**KPI:** Zufriedenheitsquote (1-5, 1 = gering, 5 = sehr hoch)
SMART-Ziel: Bis zum 4. Quartal 2010 Analyse von mindestens zwei Szenarien	**KPI:** Zahl der analysierten Szenarien und Qualität der Bewertungen
SMART-Ziel: Bis zum 4. Quartal 2010 mindestens sechs Bezugnahmen auf veröffentlichte Dokumente zu den analysierten Szenarien	**KPI:** Zahl der Bezugnahmen
BESCHREIBUNG DER AUFGABEN:	
Dieses Arbeitspaket dient der Ermittlung aufkommender Risiken für spezifische Technologien und Anwendungsbereiche unter Zuhilfenahme der Rahmenstruktur für aufkommende Risiken, die im Zuge vorhergehender Arbeitsprogramme (2008 und 2009) erarbeitet und validiert wurde. In diesem Zusammenhang wird eine Reihe von Bewertungen durchgeführt, um aufkommende Risiken für Anwendungs- und Technologieszenarien (im Folgenden als *Szenarien* bezeichnet) zu ermitteln. Die Interessenvertreter oder Organisationen schlagen Szenarien vor, von denen mindestens zwei ausgewählt und mit Hilfe der Rahmenstruktur der ENISA für aufkommende Risiken analysiert werden (beispielsweise durch das Forum von Interessenvertretern, die SGI oder die virtuelle Expertengruppe). Die zu analysierenden Szenarien werden in ähnlicher Weise wie schon bereits im Jahr 2009 überprüft und von den Ausschüssen der ENISA (z. B. dem Forum von Interessenvertretern, der SGI oder dem ENISA-Verwaltungsrat) priorisiert. Mit Hilfe dieser Bewertungen sollen insbesondere aufkommende Risiken bezüglich der Widerstandsfähigkeit von Informationsinfrastrukturen und des Datenschutzes ermittelt werden. Um die Synergien zu maximieren und bessere Fortschritte zu erzielen, dient die im Rahmen des TMP 1 geleistete Arbeit als Informationsquelle für die Erstellung des Szenarios zur Widerstandsfähigkeit von Infrastrukturen. In ähnlicher Weise dienen die Arbeit der Kommission und insbesondere die jüngste Empfehlung der Kommission zur Funkfrequenzkennzeichnung (RFID) (http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf) als Informationsquelle für das Szenario zum Datenschutz. Im Zuge der Analyse der Szenarien müssen politische Herausforderungen, einschließlich Bedenken hinsichtlich des Schutzes der Privatsphäre und weiterer sozialer Aspekte, berücksichtigt werden. Zu diesem Zweck werden in den Analysephasen relevante Meilensteine festgelegt, um Entscheidungen bezüglich der genauen Herangehensweise an die politischen Herausforderungen (z. B. Gründlichkeit der Analyse, Zielgruppen der Interessenvertreter und Qualität) treffen zu können. Hierfür werden relevante Aktivitäten der Europäischen Kommission oder anderer politischer Entscheidungsträger herangezogen. Darüber hinaus wird diese Arbeit mit den relevanten Tätigkeiten aus anderen Arbeitspaketen (z. B. VM 1.1) mit Bezug auf die Szenarioanalyse abgestimmt. Jede Szenarioanalyse wird mit Unterstützung von Sachverständigen durchgeführt. Zu diesem Zweck werden die im Jahr 2009 erstellten Reservelisten der Sachverständigen herangezogen; selbstverständlich sollen aber auch Sachverständige, die sich neu bewerben, die Möglichkeit erhalten, in diese Reservelisten aufgenommen zu werden. Ein Teil der Haushaltsmittel wird für die Entlohnung der involvierten Sachverständigen verwendet. Das Forum von Interessenvertretern zu aufkommenden Risiken leistet in	

Form von geeigneten Rückmeldungen und durch die Überwachung der Ergebnisse der geleisteten Arbeit (Qualitätssicherung in Bezug auf die analysierten Szenarien, Prüfungen, Bemerkungen zum Bewertungskonzept) ebenfalls einen Beitrag zu diesem Arbeitspaket.

Im Rahmen dieses Arbeitspakets wird die ENISA ihre Tätigkeit überprüfen und mit bestehenden oder ähnlichen Aktivitäten auf EU-Ebene abstimmen, um wertvolle Beiträge zu leisten, Empfehlungen zu unterbreiten und Doppelarbeit zu vermeiden. Interessierte Vertreter der Generaldirektionen der Europäischen Kommission können im ENISA-Forum von Interessenvertretern zu aufkommenden Risiken eine Beobachterrolle übernehmen und als Kontaktstelle zwischen der ENISA und den Generaldirektionen für verschiedene Themenbereiche wertvolle Beiträge für die Arbeit der Agentur leisten.

Außerdem hat die ENISA bereits den Kontakt zu ähnlich gelagerten Tätigkeiten und Koordinierungsmaßnahmen hergestellt, die über das 7. Rahmenprogramm der Europäischen Kommission (FP7) finanziert werden, wie beispielsweise FORWARD und WOMBAT. Der Informationsaustausch mit anderen Interessenvertretern in der EU, wie beispielsweise der GD ESTAT, wird weiterhin fortgesetzt. Neben Gemeinschaftstätigkeiten kann es andere relevante Initiativen geben, über die externe Experten und/oder Mitglieder der SGI, die wir als Berater heranzuziehen beabsichtigen, während der Planung des Arbeitsprogramms berichten können. Zu diesem Zweck wird ein ständiger Kommunikationskanal mit den Experten eingerichtet.

ERGEBNISSE UND TERMINE:

Mindestens zwei Risikobewertungen ausgewählter Szenarien (Q3 und Q4 2010) in Form von Risikobewertungsberichten
Präsentation der erarbeiteten Dokumente im Rahmen von Veranstaltungen zum Thema Sicherheit
Verwaltung des Forums von Interessenvertretern und des Pools von Sachverständigen

FOLGENDE INTERESSENVERTRETER SOLLTEN DAS ARBEITSPAKET AKTIV UNTERSTÜTZEN:

ENISA-Forum von Interessenvertretern zu aufkommenden Risiken, Industrie, Hochschulen, Normungsgremien, Mitglieder der SGI

RESSOURCEN FÜR 2010 (Personenmonate und Haushaltsmittel):

- 120 000 EUR
- 16 Personenmonate

VORSCHLAG FÜR DAS ARBEITSPAKET:

ENISA

RECHTSGRUNDLAGE:

ENISA-Verordnung, Artikel 3 Buchstaben a, c, d, e, f, g, i und k

2.3.2 Arbeitspaket 3.2 – Weiterführung der Rahmenstruktur für aufkommende Risiken

Bezeichnung des TMP:	
Ermittlung aufkommender Risiken zum Zwecke der Vertrauensbildung	
BEZEICHNUNG DES ARBEITSPAKETS:	
Arbeitspaket 3.2 – Weiterführung der Rahmenstruktur für aufkommende Risiken	
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):	
SMART-Ziel: Bis 2011 mindestens zwei Bezugnahmen in relevanten Veröffentlichungen und mindestens eine Präsentation auf einer relevanten Veranstaltung zum Prognosemodell	**KPI:** Zahl der Bezugnahmen, Zahl der Präsentationen auf relevanten Veranstaltungen, Datum
SMART-Ziel: Bis 2011 haben mindestens zwei Interessenvertreter Interesse an der Anwendung der erarbeiteten Funktionalität bekundet.	**KPI:** Zahl der an der Arbeitsgruppe beteiligten Interessenvertreter
BESCHREIBUNG DES ARBEITSPAKETS:	
Ziel dieses Arbeitspakets ist es, die in der Rahmenstruktur für aufkommende Risiken enthaltenen Funktionen zu verbessern. Dies umfasst auch die Erarbeitung zusätzlicher Funktionen für die Verwaltung und Verbreitung der gesammelten Informationen und die Einrichtung von Schnittstellen zu weiteren relevanten Quellen (z. B. Vorfälle, Bedrohungen und Schwachstellen). Die Inhalte dieses Arbeitspakets werden mit der Unterstützung von Experten erarbeitet, die zu einer Ad-hoc-Arbeitsgruppe zusammengefasst sind. Das zentrale Produkt dieses Arbeitspakets besteht in einem ***konzeptionellen Fahrplan für die Auswahl von Szenarien und die Weiterführung der Rahmenstruktur für aufkommende Risiken***: Da es sich bei dieser Rahmenstruktur um einen dynamischen Prozess handelt, sollen die Rückmeldungen zu ihrer Anwendung unter dem Arbeitspaket 3.1 und im Rahmen früherer Aktivitäten unter dem Arbeitsprogramm 2009 dazu verwendet werden, die Funktionalität weiter zu verbessern. Von besonderer Bedeutung wird hierbei die Aktualisierung des Verfahrens für die Ermittlung und Auswahl der geeigneten Bereiche und Szenarien (Technologien und Anwendungen) sein, das den gesamten Prozess auslöst. Der Grundgedanke ist, dass diese Auswahl einem konzeptionellen Modell unterliegen sollte, mit dessen Hilfe ein Szenario und der entsprechende relevante Bereich korrekt ermittelt und ausgewählt werden können (z. B. technologiegestützte vs. sonstige (politische, soziologische usw.) Konzepte). Dieser Aspekt ist von wesentlicher Bedeutung, da die Auswahl eines geeigneten Szenarios maßgeblich für den erzielten Fortschritt und somit ein wichtiger Erfolgsfaktor für diese Arbeit ist. Die hier gewonnenen Erkenntnisse tragen zu einer schnellen, transparenten und systematischen Vorgehensweise bei der Ermittlung thematischer Bereiche und Szenarien bei.	
ERGEBNISSE UND TERMINE:	
• Ein konzeptionelles Modell und ein Verfahren für die Auswahl von thematischen Bereichen und Szenarien (bis zum 1. Quartal 2010), einschließlich einer Regelung zur Gewichtung und Priorisierung	
FOLGENDE INTERESSENVERTRETER SOLLTEN DAS ARBEITSPAKET AKTIV UNTERSTÜTZEN:	
Verwaltungsrat, SGI, NRO, Mitglieder der Arbeitsgruppe (aus Industrie, Hochschule, Forschung), ENISA-Forum von Interessenvertretern zu aufkommenden Risiken	
RESSOURCEN FÜR 2010 (Personenmonate und Haushaltsmittel):	
• 35 000 EUR • 3 Personenmonate	
VORSCHLAG FÜR DAS ARBEITSPAKET:	
ENISA	
RECHTSGRUNDLAGE:	
ENISA-Verordnung, Artikel 3 Buchstaben a, c, d, e, f, g, i und k	

2.3.3 Arbeitspaket 3.3 – Förderung der nationalen Vorsorgemaßnahmen im Rahmen des Risikomanagements

Bezeichnung des TMP:	
Ermittlung aufkommender Risiken zum Zwecke der Vertrauensbildung	
BEZEICHNUNG DES ARBEITSPAKETS:	
Arbeitspaket 3.3 – Förderung der nationalen Vorsorgemaßnahmen im Rahmen des Risikomanagements: Unterstützung europaweiter Übungen	
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):	
SMART-Ziel: Ermittlung europäischer Experten auf dem Gebiet der nationalen Vorsorgemaßnahmen im Rahmen des Risikomanagements	**KPI:** Zahl der an der Arbeitsgruppe beteiligten Experten
SMART-Ziel: Bis Ende 2010 Erstellung einer Liste der zentralen Bereiche, die als Teil der nationalen Vorsorgemaßnahmen zum Schutz kritischer Informationsinfrastrukturen im Rahmen des Risikomanagements berücksichtigt werden sollten. Hiervon ausgehend wird eine Liste relevanter Bereiche und Komponenten zum Schutz kritischer Informationsinfrastrukturen (anhand von Risikoaspekten) erstellt und dokumentiert. Diese dient als Grundlage für die Übungsszenarien.	**KPI**: Vollständigkeit der zu erarbeitenden Liste der relevanten Themenbereiche für die nationalen Vorsorgemaßnahmen im Rahmen des Risikomanagements; Ausarbeitung von Übungsszenarien auf der Grundlage der ermittelten Bereiche und Komponenten.
SMART-Ziel: Bis Ende 2010 haben mindestens zwei Mitgliedstaaten Interesse an diesen Ergebnissen bekundet und sich zu Folgemaßnahmen bereit erklärt.	**KPI**: Zahl der interessierten Mitgliedstaaten
BESCHREIBUNG DES ARBEITSPAKETS:	

Der Schutz kritischer Informationsinfrastrukturen und die Widerstandsfähigkeit von Kommunikationsnetzen erstrecken sich über zahlreiche Bereiche, von der Technologie über die Politik und die organisationenübergreifende Koordinierung bis hin zur Kommunikation, und zahlreiche Interessenvertreter sind involviert. Die proaktive Verwaltung von Risiken im Bereich der Informationssicherheit ist ein wesentlicher Aspekt für den Aufbau und die Erhaltung widerstandsfähiger Informationsinfrastrukturen. Beim Blick auf die mit den Informationsbeständen (technisch und organisatorisch) verbundenen Risikobestandteile sind je nach Art, Relevanz und Wirkung im Zusammenhang mit dem Schutz kritischer Informationsinfrastrukturen unterschiedliche Aspekte zu berücksichtigen. Darüber hinaus sind bei der Einführung und Verbesserung nationaler Vorsorgemaßnahmen im Rahmen des Risikomanagements auf Ebene der Mitgliedstaaten verschiedene Interessenvertreter sowohl aus dem privaten als auch aus dem öffentlichen Sektor einzubinden.

Mit diesem Arbeitspaket soll eine erste Identifizierung der Bereiche, die für die nationalen Vorsorgemaßnahmen im Rahmen des Risikomanagements relevant sind, sowie der beteiligten Interessenvertreter aus den EU-Mitgliedstaaten erreicht werden. Unabdingbar für die Identifizierung dieser Bereiche sind die Aspekte zum Schutz kritischer Informationsinfrastrukturen, andere direkt zugehörige Bereiche werden jedoch ebenfalls berücksichtigt. Im Mittelpunkt stehen maßgebliche Abhängigkeiten zwischen diesen Bereichen und zentralen Komponenten. Das endgültige Ergebnis soll einen ersten Überblick über die Bereiche und Komponenten sowie über die beteiligten Interessenvertreter und ihre Rollen im Zusammenhang mit den nationalen Vorsorgemaßnahmen im Rahmen des Risikomanagements geben.

Erreicht wird dieses Ziel durch die Einrichtung einer Arbeitsgruppe, die sich aus nationalen Experten aus dem Bereich des Risikomanagements zusammensetzt, die sowohl aus öffentlichen als auch aus privaten Organisationen stammen. Die Aufgabe dieser Arbeitsgruppe besteht in der Ermittlung und Beschreibung aller relevanten Bestandteile der nationalen Vorsorgemaßnahmen im Rahmen des Risikomanagements in Bezug auf die Widerstandsfähigkeit öffentlicher elektronischer Kommunikationsnetze. Zu den verschiedenen relevanten Bestandteilen gehören z. B. zugehörige Komponenten (wie die Art der geschützten Infrastrukturen), die entsprechenden Interessenvertreter (z. B. die Eigentümer oder Betreiber von Infrastrukturen, Regulierungsbehörden, öffentliche und private Notfallteams), Nutzer der Infrastruktur, zugehörige kritische Einsatzbereiche für die entsprechende Infrastruktur (z. B. Energie,

Gesundheitswesen), Zuständigkeiten der beteiligten Interessenvertreter im Zusammenhang mit dem Risikomanagement, erforderliche Koordinierungsmaßnahmen und erforderliche nationale Eskalationskonzepte. Im Rahmen des Arbeitspakets wird eine erste Rangliste dieser Bestandteile, geordnet nach ihrem Wert, ihrer Wirkung und ihres Risikoprofils, erarbeitet.

Das hier erarbeitete Material fließt in das Arbeitspaket 1.4 ein und unterstützt die Beteiligten bei der Definition der Szenarien, die im Rahmen der europaweit durchzuführenden Übungen zur Widerstandsfähigkeit erforderlich sind. In diesem Zusammenhang müssen auch Schnittstellen zu den Aktivitäten des TMP 1 geschaffen werden, und zwar sowohl hinsichtlich der Koordinierung der Arbeitsgruppe als auch hinsichtlich der Terminplanung und der Strukturierung der Ergebnisse der Arbeitsgruppe.

Mit diesen Informationen können interessierte Interessenvertreter die nationalen Entwicklungen auf diesem Gebiet verfolgen und die Maßnahmen festlegen, die für die Einführung und die Verbesserung nationaler Vorsorgemaßnahmen im Rahmen des Risikomanagements erforderlich sind. Darüber hinaus bilden diese Informationen die Grundlage für Bestandsaufnahmen in den verschiedenen Mitgliedstaaten sowie für die Erarbeitung eines Fahrplans für künftige Maßnahmen in diesem Bereich. Für die europaweite Übung zur Widerstandsfähigkeit stellt die anhand der ermittelten Risiken erarbeitete Liste der verschiedenen Aspekte des Schutzes kritischer Informationsinfrastrukturen einen zentralen Bestandteil für die Definition von Übungsszenarien dar.

ERGEBNISSE UND TERMINE:

Dokumentation der ermittelten Komponenten und Bereiche in Bezug auf die nationalen Vorsorgemaßnahmen im Rahmen des Risikomanagements (bis zum 4. Quartal 2010)

FOLGENDE INTERESSENVERTRETER SOLLTEN DAS ARBEITSPAKET AKTIV UNTERSTÜTZEN:

Verwaltungsrat, SGI, NRO, Europäische Kommission, Mitgliedstaaten, Sachverständige (aus Industrie, Hochschule, Forschung)

RESSOURCEN FÜR 2010 (Personenmonate und Haushaltsmittel):

- 80 000 EUR
- 11 Personenmonate

VORSCHLAG FÜR DAS ARBEITSPAKET:

ENISA

RECHTSGRUNDLAGE:

ENISA-Verordnung, Artikel 3 Buchstaben a, c, d, e, f, g, i und k

2.4. VM1: „Internet der Zukunft“: Identität, Rechenschaftspflicht und Nutzervertrauen

BEZEICHNUNG DES PROGRAMMS
VM 1: Nutzervertrauen und Schutz der Privatsphäre im „Internet der Zukunft“
BESCHREIBUNG DES PROBLEMS:
Mit dem Vormarsch des Internets hat nun jeder die Möglichkeit, neben seinem realen Leben auch eines oder mehrere Leben in der virtuellen Welt zu führen. Die immer stärkere Verknüpfung dieser beiden Welten und die Bereitstellung von Informationen aus der realen Welt für die Dienste im Internet sind eine Tendenz, die in den letzten Jahren zunächst nur in der Wissensgemeinschaft zu beobachten war, nun aber zunehmend auch Eingang in kommerzielle Angebote findet. Dies führt dazu, dass es sich bei den vernetzten Knoten im „Internet der Zukunft“ vor allem um Sensor-Aktor-Knoten handelt, die den „realen“ Teil des Internets bilden und gleichzeitig das Volumen der über das Internet durchsuchbaren und zugänglichen Informationen erhöhen. Neben dem „realen“ Internet (Real World Internet) bildet das sogenannte „Internet der Dinge“ eine weitere parallele Entwicklungslinie des „Internets der Zukunft“. Als Weiterentwicklung der modernen RFID-Technologie besteht das „Internet der Dinge“ aus Netzwerken von Knoten, die mit Objekten kommunizieren, die mit Tags versehen sind. *Das „Internet der Zukunft“ setzt sich zwar auch aus einzelnen Schichten zusammen, doch bestehen nun zahlreiche übergreifende Abhängigkeiten, die eine höhere Komplexität und eine stärkere Aufteilung der Zuständigkeiten zur Folge haben. Das „Internet der Zukunft“ bietet im Vergleich zum herkömmlichen Internet umfassende neue Möglichkeiten, was in erster Linie auf die Einbindung zahlreicher vernetzter Einheiten verschiedenster Art und somit auf die enorme Ausdehnung des Geltungsbereichs zurückzuführen ist. Diese Art des Internets kann spontane neue Verhaltensweisen und ungeahnte neue Anwendungsmöglichkeiten hervorrufen. Neue Einheiten, Dienste und Geschäftsszenarien werden vielmehr die Regel als die Ausnahme darstellen. Das „Internet der Zukunft“ wird sich zu einer weitverbreiteten digitalen Umgebung entwickeln, die sich aus vielen verschiedenen heterogenen Infrastrukturen, Terminals und Technologien zusammensetzt, die alle miteinander vernetzt sind. Die Nutzer interagieren über diese Form des Internets in allen Lebensbereichen miteinander und nehmen hierbei in verschiedenen Gemeinschaften und sozioökonomischen Kontexten jeweils unterschiedliche Rollen ein. Jede dieser Situationen erfordert die Verwendung verschiedener Identitäten, Schutzmaßnahmen und Vertraulichkeitseinstellungen.*[9] Zweifellos sind die Aspekte der Sicherheit, der Privatsphäre und des Vertrauens maßgeblich für jeden Dienst, jede Anwendung und jede Transaktion, die über öffentliche Kommunikationsnetze bereitgestellt werden. Es wird erwartet, dass ihre Bedeutung in großen dezentralen Systemen, die – wie eben das „Internet der Zukunft“ – über Links auf die „reale“ Welt verweisen, noch weiter zunimmt. Die wichtigsten Herausforderungen sind in diesem Zusammenhang die Sicherstellung der Integrität von Informationen, der Schutz der Informationsquelle und die Stärkung des Vertrauens sowohl in Personen als auch in Objekte, Sensoren und Aktoren.

[9] Positionspapier zu Vertrauensbildung und Identität (Trust & Identity) im „Internet der Zukunft“, Future Internet Assembly, Madrid, 9. Dezember 2008.

BESCHREIBUNG DES ANSATZES ZUR LÖSUNG DES PROBLEMS:

Das übergreifende Ziel dieser vorbereitenden Maßnahme besteht darin, das hohe Sicherheitsniveau sowie das Vertrauen der Nutzer und der Industrie in die IKT-Infrastruktur und die bereitgestellten Dienste in Europa zu stärken und gleichzeitig die Gefahren für die bürgerlichen Freiheiten und die Privatsphäre soweit wie möglich zu beseitigen.

Die ENISA wird die folgenden Maßnahmen ergreifen, um dieses Ziel zu erreichen:

1) Überprüfung und Bewertung der möglichen Auswirkungen und Folgen von Bedrohungen, die sich aus der Einführung neuer Technologien ergeben, sowie Ermittlung der Bedeutung des Vertrauens und der Rechenschaftspflicht (einschließlich des Vertrauens in Infrastrukturen). Die ENISA wird hierzu die Modelle elektronischer Dienste in Bezug auf die Sicherheit untersuchen und in diesem Zusammenhang die verfügbaren Methoden für die nutzerbestimmte Verwaltung personenbezogener Daten und deren Zurücknahme, die Verbreitung solcher Methoden für die nutzerbestimmte Datenverwaltung in multiplen Umgebungen und deren mögliche Verwendung in Dienstszenarien zum „Internet der Zukunft“ berücksichtigen.
2) Beobachtung der Entwicklung und Einführung der Technologien, die den sicheren Zugang zu Daten ermöglichen, der Mechanismen, mit denen die Offenlegung der Daten auf ein Mindestmaß reduziert wird, fortschrittlicher Identitätsregelungen, der Bereitstellung von Identity-Diensten bei gleichzeitigem Schutz der Privatsphäre, der Formulierung und Umsetzung politischer Anforderungen sowie der auf Vertrauen und einer durchgängigen Sicherheit basierenden Verwendungskontrolle. Durchführung einer Bestandsaufnahme bezüglich wichtiger Entwicklungen und/oder Aspekten der Privatsphäre.
3) Erarbeitung politischer Strategien und bewährter Verfahren mit dem Ziel, ein Gleichgewicht von Transparenz, Rechenschaftspflicht und Verantwortung zu erreichen. Dies umfasst auch die Ausarbeitung von Anforderungen bezüglich der Angleichung der bestehenden Modelle der elektronischen Authentifizierung sowie die Entwicklung von Leitlinien und Empfehlungen zu notwendigen Verordnungen, nach Bedarf mit Blick auf den Schutz der Privatsphäre und die Vertrauensbildung, und eines ordnungspolitischen Modells für die Überwachung und Zulassung.
4) Enge Zusammenarbeit mit der Kommission (sowie insbesondere mit dem Referat F5 der GD INFSO und dem Referat H2 der GD INFSO), um so im Verlauf der Initiative den regelmäßigen Austausch von Informationen und die Nutzung aller Synergien sicherzustellen.

Die ENISA führt in den kommenden Jahren die vorbereitenden Maßnahmen durch und überprüft in diesem Zusammenhang zahlreiche Technologien in diesem Bereich, den Stand der Umsetzung dieser Technologien und die entsprechenden politischen Initiativen mit Bezug auf die Privatsphäre und die Vertrauensbildung. Angesichts der Komplexität dieser Thematik erstreckt sich diese vorbereitende Maßnahme über insgesamt zwei Jahre (2010 und 2011).

ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):

SMART-Ziel: Bis 2012 haben die Kommission und mindestens 50 % der Mitgliedstaaten die ENISA-Empfehlungen in ihren politischen Entscheidungsprozessen berücksichtigt.	**KPI:** Kommission (ja/nein), % der Mitgliedstaaten

VORRANGIGE ZIELE, DIE DURCH DAS PROGRAMM UNTERSTÜTZT WERDEN:

EU-weite Stärkung des Vertrauens der Öffentlichkeit und der IKT-Branche in das „Internet der Zukunft“; Förderung des Binnenmarkts für elektronische Kommunikation durch die Unterstützung der Institutionen bei der Festlegung geeigneter Gesetzesvorschriften und anderer Maßnahmen;
Intensivierung des Dialogs über den Schutz der Privatsphäre und das Nutzervertrauen (einschließlich des Vertrauens in die Infrastrukturen) zwischen den verschiedenen Akteuren in der EU;
Ausweitung der Zusammenarbeit zwischen den Mitgliedstaaten mit dem Ziel, die Unterschiede bei den politischen Initiativen dieser Länder zu verringern

AKTEURE UND BEGÜNSTIGTE:
Nationale Regulierungsbehörden (NRA), Regierungen der Mitgliedstaaten, politische Entscheidungsträger auf EU-Ebene, Netzbetreiber und Diensteanbieter, Verbände von Anbietern und Prüfern, Netzwerkgeräte-Händler
WARUM DIE ENISA?
Die ENISA kann in besonderer Weise dazu beitragen, das hohe Sicherheitsniveau sowie das Vertrauen der Öffentlichkeit und der Industrie in die IKT-Infrastruktur und die bereitgestellten Dienste zu stärken. Naturgemäß macht das Internet auch vor Landesgrenzen nicht halt; die Herausforderungen an das Internet können daher nicht im Alleingang und ohne eine Zusammenarbeit der EU-Mitgliedstaaten bewältigt werden. Durch ihre Ausrichtung ist die ENISA in der Lage, die gemeinsamen Politiken, Maßnahmen und Verfahren der Europäischen Union in diesem Bereich zu fördern und zu unterstützen.

2.4.1 VM: Arbeitspaket 1.1 – Bestandsaufnahme zu den Prozessen der Authentifizierung und des Schutzes der Privatsphäre

Bezeichnung des TMP:	
Nutzervertrauen und Schutz der Privatsphäre im „Internet der Zukunft“	
BEZEICHNUNG DES ARBEITSPAKETS:	
VM: Arbeitspaket 1.1 – Bestandsaufnahme zu den Prozessen der Authentifizierung und des Schutzes der Privatsphäre	
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):	
SMART-Ziel: mehr als fünf Bezugnahmen auf die Ergebnisse	**KPI:** Zahl der Bezugnahmen
SMART-Ziel: mehr als 20 Mitgliedstaaten, die sich an den Bestandsaufnahmen beteiligen	**KPI:** Zahl der Mitgliedstaaten
BESCHREIBUNG DES ARBEITSPAKETS:	
Das Konzept der Identität in IKT-Anwendungen und -Diensten entwickelt sich in rasanter Geschwindigkeit, und viele verwandte Konzepte wie das des „Vertrauens“ könnten die Art und Weise, wie Infrastrukturen und Dienste künftig abgesichert werden, grundlegend beeinflussen. Der Erfolg von Websites für die soziale Vernetzung macht unter anderem deutlich, dass der unangemessene Umgang mit personenbezogenen Informationen viel Spielraum für Datenmissbrauch lässt. Wenn diese Probleme nicht angegangen werden, kann dies zu einem Verlust des öffentlichen Vertrauens in die IKT-Dienste führen und so zu einem Hindernis für Innovation und Wachstum werden. Die von der ENISA auf diesem Gebiet bereits geleistete Arbeit zeigt, dass eines der größten Probleme, das mittelfristig behoben werden muss, die unterschiedlichen Anforderungen der EU-Mitgliedstaaten an die Sicherheit und Privatsphäre für unterschiedliche Anwendungen betrifft. Die ENISA wird ihre Arbeit zu diesem Thema in Zusammenarbeit mit führenden europäischen Initiativen, darunter das Programm IDABC, das STORK-Konsortium und CEN-Arbeitsgruppen, fortsetzen. Ziel ist es, die Grundlagen für sichere Dienste in Europa zu ermitteln, anhand derer bewährte Verfahren und Empfehlungen für Technologien erarbeitet werden können, die einen direkten Bezug zu sicheren Diensten und die elektronische Authentifizierung, Genehmigung und Rechenschaftspflicht haben. In diesem Zusammenhang müssen mehrere Authentifizierungsmethoden, einschließlich webgestützter ID-Frameworks und auf Hardware-Token basierender Authentifizierungsmethoden, unter Beachtung der Anforderungen an wichtige elektronische Dienste in Europa miteinander verglichen werden. Von besonderem Interesse ist auch die Verwaltung mehrerer Identitäten. „Identität“ ist in diesem Zusammenhang im weitesten Sinne zu verstehen (also als elektronische ID (eID), Verbundidentität, RFID, Avatare usw.). Mögliche zu untersuchende Anwendungsbereiche wären beispielsweise virtuelle Welten, in denen das Konzept der Anonymität analysiert werden könnte. Eine weitere wichtige Entwicklung, die das Niveau der Datensicherheit in Europa erhöhen und das Vertrauen der Bürger in die Sicherung und den Schutz ihrer personenbezogenen Daten durch die auf dem Sektor der elektronischen Kommunikation tätigen Betreiber stärken könnte, ist schließlich die Einführung einer Bestimmung für den Sektor der elektronischen Kommunikation, die im Zuge der Überprüfung der Richtlinie 2002/58/EG (Verarbeitung personenbezogener Daten und Schutz der Privatsphäre in der elektronischen Kommunikation) eingeführt wurde und die Meldung von Verletzungen des Schutzes personenbezogener Daten regelt. Vor diesem Hintergrund möchte die ENISA die aktuelle Situation analysieren und eine Reihe konsistenter Leitlinien zu den Maßnahmen und Verfahren bei der technischen Umsetzung gemäß Artikel 4 der überprüften Richtlinie 2002/58/EG erarbeiten.	
ERGEBNISSE UND TERMINE:	
• Bericht über die Methoden für die Verwaltung mehrerer Identitäten (Q4 2010) • Bericht über den aktuellen Stand der Umsetzung von eIDs in den privaten und öffentlichen Sektoren in den Mitgliedstaaten, Nennung von Trends und möglichen Anreizen (Q4 2010) • Bestandsaufnahme zu den vorhandenen Vorgehensweisen in Bezug auf die Meldung von Verletzungen des Schutzes personenbezogener Daten in verschiedenen Sektoren (Q4 2010)	

Die nächsten Schritte, die – sofern diese vorbereitende Maßnahme in ein thematisches Mehrjahresprogramm umgesetzt wird – im Rahmen der oben genannten Aktivitäten im Jahr 2011 durchgeführt werden sollen, umfassen Folgendes: • Bewährte Verfahren und Empfehlungen für Technologien, die sich auf sichere Dienste und die elektronische Authentifizierung beziehen • Leitlinien zu den Maßnahmen und Verfahren bei der technischen Umsetzung gemäß Artikel 4 der Richtlinie 2002/58/EG
FOLGENDE INTERESSENVERTRETER SOLLTEN DAS ARBEITSPAKET AKTIV UNTERSTÜTZEN:
Netzwerkgeräte-Händler, nationale Regulierungsbehörden (NRA), Diensteanbieter, FuE-Einrichtungen der Industrie, Universitäten und Forschungszentren, Europäische Technologieplattformen.
RESSOURCEN FÜR 2010 (Personenmonate und Haushaltsmittel):
• 9 Personenmonate[10]
VORSCHLAG FÜR DAS ARBEITSPAKET:
ENISA
RECHTSGRUNDLAGE:
ENISA-Verordnung, Artikel 3 Buchstaben a, b, c, f und k

[10] Zum Zeitpunkt der Erstellung des vorliegenden Dokuments ist die Agentur nicht in der Lage, finanzielle Mittel für diese vorbereitende Maßnahme bereitzustellen. Die erforderlichen Ressourcen in Höhe von 90 000 EUR können jedoch im Laufe des Jahres bezogen werden.

2.4.2 VM: Arbeitspaket 1.2 – Bestandsaufnahme zu den Dienstmodellen zur Unterstützung der elektronischen Dienste

Bezeichnung des TMP:
Nutzervertrauen und Schutz der Privatsphäre im „Internet der Zukunft“
BEZEICHNUNG DES ARBEITSPAKETS:
VM: Arbeitspaket 1.2 – Bestandsaufnahme zu den Dienstmodellen zur Unterstützung der elektronischen Dienste
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):
SMART-Ziel: Ermittlung und Bewertung von mehr als fünf Dienstmodellen **KPI:** Zahl der bewerteten Dienstmodelle **SMART-Ziel:** mehr als fünf Bezugnahmen auf die Ergebnisse **KPI:** Zahl der Bezugnahmen
BESCHREIBUNG DES ARBEITSPAKETS:
Hauptziel dieser Maßnahme ist eine Bestandsaufnahme zu den vorhanden Modellen für elektronische Dienste und deren Sicherheitsmerkmalen, in deren Rahmen das Gleichgewicht zwischen Privatsphäre und Rechenschaftspflicht, zwischen Einverständnis und Überwachung bewertet wird. Die heutigen Online-Anwendungsumgebungen zeichnen sich durch zahlreiche an den individuellen Bedarf angepasste Sicherheitsmodelle aus, die optimal auf die verschiedenen Anwendungsklassen, in denen sie zum Einsatz kommen, zugeschnitten sind. Es muss daher untersucht werden, wie die Nutzer die verschiedenen Arten elektronischer Dienste verwenden sollten. Im Jahr 2010 wird die ENISA Sicherheitsmodelle für elektronische Dienste und deren Leistung in hochgradig verteilten Umgebungen, wie beispielsweise dem heutigen Internet, analysieren. Darüber hinaus wird die ENISA verschiedene Möglichkeiten untersuchen, mit denen die Privatsphäre und die Rechenschaftspflicht im Internet sichergestellt werden können, die bekanntesten Methoden überprüfen, ihre Abbildung in den zugrundeliegenden Architekturen erforschen und das Maß ihrer Wirksamkeit und Leistung bewerten. Die ENISA befasst sich zudem mit der Entwicklung von Empfehlungen für die Verwendung spezifischer Dienstmodelle in vorhandenen Umgebungen und Architekturen. Dies umfasst auch die Erarbeitung von Leitlinien für erforderliche Maßnahmen in Bezug auf den Schutz der Privatsphäre und die Vertrauensbildung.
ERGEBNISSE UND TERMINE:
• Katalog aktueller Dienstmodelle und die damit verbundenen Sicherheitsaspekte in verschiedenen Architekturen (Q4 2010) • Bewertung der ermittelten Dienstmodelle und Empfehlungen für spezifische Architekturen (Q4 2010)
FOLGENDE INTERESSENVERTRETER SOLLTEN DAS ARBEITSPAKET AKTIV UNTERSTÜTZEN:
Nationale Regulierungsbehörden (NRA), Europäische Kommission, Diensteanbieter, Universitäten und Forschungszentren, EDSB, Europäische Technologieplattformen.
RESSOURCEN FÜR 2010 (Personenmonate und Haushaltsmittel):
• 9 Personenmonate[11]
VORSCHLAG FÜR DAS ARBEITSPAKET:
ENISA
RECHTSGRUNDLAGE:
ENISA-Verordnung, Artikel 3 Buchstaben a, b, c, f und k

[11] Zum Zeitpunkt der Erstellung des vorliegenden Dokuments ist die Agentur nicht in der Lage, finanzielle Mittel für diese vorbereitende Maßnahme bereitzustellen. Die erforderlichen Ressourcen in Höhe von 90 000 EUR (für Workshops, Beratungsdienste, die Arbeit der Expertengruppen, elektronische und gedruckte Veröffentlichungen) können jedoch im Laufe des Jahres über Beiträge der EWR-Länder bezogen werden.

2.5. VM 2: Ermittlung von Antriebskräften und Rahmenstrukturen für die EU-weite sektorale Zusammenarbeit auf dem Gebiet der NIS

BEZEICHNUNG DES PROGRAMMS
VM 2: Ermittlung von Antriebskräften und Rahmenstrukturen für die EU-weite sektorale Zusammenarbeit auf dem Gebiet der NIS
BESCHREIBUNG DES PROBLEMS:
Eine wachsende Anzahl der Bedrohungen auf dem Gebiet der Netz- und Informationssicherheit bezieht sich auf komplizierte Kombinationen aus Netz- und Dienstprotokollen. Traditionelle Schutzmechanismen, die ausschließlich auf starken „Firewalls“ für einzelne Unternehmensnetze aufbauen, reichen nicht mehr aus, um Angreifer davon abzuhalten, einzudringen und wichtige elektronische Informationen von Unternehmen und anderen Organisationen zu stehlen oder zu beschädigen. Dieses Problem ist somit eine der grundlegenden Herausforderungen für Organisationen, die ihre Geschäfte über das Internet abwickeln, und die Zusammenarbeit von Netz- und Diensteanbietern im Rahmen der Entwicklung und Bereitstellung von NIS-Diensten wurde infolge der Marktnachfrage nach Lösungen zu diesem Problem weiter intensiviert. Da immaterielle Vermögenswerte für die Wertschöpfung zunehmend an Bedeutung gewonnen haben, bestehen sowohl für große als auch für kleine Unternehmen, die über hoch entwickelte Technologien verfügen, weiterhin gute Gründe, gemeinsam mit den öffentlichen Behörden an Lösungen für die NIS-Herausforderungen zu arbeiten. In Einzelunternehmen bestehen selbstverständlich rechtliche Verpflichtungen für eine Zusammenarbeit mit den öffentlichen Behörden in Bereichen wie dem Datenschutz und der Datenhaltung. Die Komplexität und die teilweise rechtlich ambivalente Natur von Angriffen im Bereich der Netz- und Informationssicherheit erfordern jedoch (zumindest in der Anfangsphase) auf freiwilliger Basis umfassendere und proaktive Formen der Zusammenarbeit zwischen den Sektoren entlang der Lieferketten zu schaffen, um zu vermeiden, dass der Missbrauch möglicher Sicherheitslücken in den Lieferketten sich nicht nachteilig auf die Wirtschaft auswirkt und möglicherweise zu weitreichenden Störungen führt. Für ein erfolgreiches Ergebnis müssen diese Formen der Zusammenarbeit jedoch auf einer realistischen Einschätzung der Fähigkeit der Beteiligten aufbauen, diese Herausforderungen der Netz- und Informationssicherheit unter Berücksichtigung ihrer jeweiligen Verantwortlichkeiten und Zuständigkeiten im kommerziellen und ordnungspolitischen Bereich zu meistern. Andernfalls fallen die Reaktionen der Beteiligten unter Umständen uneinheitlich, unangemessen oder unverhältnismäßig aus oder sind bezüglich der Anforderungen oder Leistungen der Beteiligten unrealistisch. Wenn der Schwerpunkt ausschließlich auf die Zusammenarbeit auf Anbieterseite gelegt wird, können Probleme für zahlreiche Aspekte der öffentlichen Politik entstehen, wenn die Antriebskräfte auf Nachfrageseite nicht positiv definiert und ein Versagen des Marktes nicht eindeutig identifiziert wird. Es ist jedoch recht wenig über die operativen, kommerziellen und/oder ordnungspolitischen Bedingungen bekannt, die die Zusammenarbeit der verschiedenen Sektoren im Bereich der Netz- und Informationssicherheit verhindern oder auch fördern oder entsprechende Anreize schaffen, und über die Situationen, in denen eine Zusammenarbeit mit den Behörden des öffentlichen Sektors bei der Entwicklung von Diensten, entsprechenden Instrumenten oder Kooperationsrahmen aus kommerzieller Sicht sowie aus Sicht der öffentlichen Politik wünschenswert oder von gegenseitigem Nutzen wäre. Wenn für Organisationen kohärente, klare und wirksame ordnungspolitische Bestimmungen geschaffen werden sollen und die öffentlich-private Koordinierung optimiert werden soll, setzt dies die Integration verschiedener Konzepte auf nationaler, europäischer und internationaler Ebene voraus. Angesichts der steigenden Komplexität der Sicherheitsbedrohungen ist es nicht möglich, dass eine einzelne Organisation auf nur einer Ebene gegen eine solche Bedrohung vorgeht. Maßnahmen von Akteuren mit unterschiedlichen Verantwortlichkeiten und auf verschiedenen Ebenen können dazu beitragen, die Fähigkeit anderer zu stärken, ebenfalls Maßnahmen zu ergreifen, und somit zu einer höheren

Gesamteffizienz beitragen. Versuche für eine europa- und weltweite Zusammenarbeit können unter Umständen im Widerspruch zu nationalen gesetzlichen Vorschriften stehen, sofern die entsprechenden Partnerschaften nicht explizit rechtlich anerkannt sind oder auf Ebene der EU und international von Stellen des öffentlichen Sektors unterstützt werden.

Obwohl im Allgemeinen vielfältige Anreize für eine Zusammenarbeit im privaten Sektor sowie für die Zusammenarbeit zwischen den öffentlichen und privaten Sektoren geschaffen wurden, bestehen unter Umständen jedoch auch wesentliche Hindernisse für eine erfolgreiche Umsetzung. Eine Analyse dieser Hindernisse kann dabei helfen, Möglichkeiten zu ermitteln, durch europaweit gültige Rahmenstrukturen kommerzielle, wirtschaftliche und ordnungspolitische Anreize für verschiedene Akteure in der Lieferkette (Netzbetreiber, Software- und Diensteanbieter, Nutzerverbände und öffentliche Stellen) zu schaffen, damit sie im Rahmen ihrer Zusammenarbeit bestehende Antriebskräfte für den Markt stärken und im Falle von Marktversagen die politischen Bestimmungen vollständig einhalten können. Im Rahmen der hier vorgeschlagenen VM soll geklärt werden, *wie* die betreffenden Akteure am besten von einer Beteiligung an einer europaweiten gemeinschaftlichen Maßnahme zum Umgang mit den Herausforderungen der Netz- und Informationssicherheit überzeugt werden können.

BESCHREIBUNG DES ANSATZES ZUR LÖSUNG DES PROBLEMS:

Im Rahmen dieser VM werden die Stärken und Schwächen der kommerziellen, wirtschaftlichen und/oder ordnungspolitischen Beschränkungen und Antriebskräfte in Bezug auf die sektorale Zusammenarbeit und der Anreize für die Schaffung von Partnerschaften zwischen dem öffentlichen und dem privaten Sektor bei der Entwicklung verschiedener NIS-Dienste in der Lieferkette aufgezeigt. Gemäß der Beschreibung im Arbeitspaket zur VM 2.1 bildet die Analyse der Anforderungen privater Akteure aus zwei oder drei verschiedenen Sektoren an die Dienste im Bereich der Netz- und Informationssicherheit den Ausgangspunkt der Arbeit. Diese Anforderungen werden im Zusammenhang mit der bereits geleisteten Arbeit der ENISA zur Widerstandsfähigkeit kritischer Informationsinfrastrukturen betrachtet, und die auf die kommerziellen und wirtschaftlichen Bereiche ausgerichtete VM *ergänzt* die eher auf den operativen Bereich und die Technologien bezogene Arbeit im Rahmen des TMP 1 im Arbeitsprogramm 2010. Dabei wird der Schwerpunkt insbesondere auf die nachfrageseitigen Anforderungen an eine Zusammenarbeit von Unternehmen als zwischengeschaltete Organisationen oder Endnutzer von NIS-Diensten zu durchgängigen Lieferketten gelegt. Durch die folgenden Maßnahmen wird eine Beziehung zwischen den allgemeinen und den sektorspezifischen Problemen hergestellt:

1. Ermittlung der allgemeinen Bedrohung, des Geschäftsmodells und der Marktbedingungen, die dazu führen können, dass Akteure auf Nachfrageseite aus verschiedenen Sektoren (sowohl in großen Unternehmen als auch in KMU Nutzer von netzgestützten Diensten) eine stärkere sektorenübergreifende Zusammenarbeit bei grundlegenden Problemen im Bereich der Netz- und Informationssicherheit wünschen;
2. Ermittlung, wie und in welchem Umfang diese Anforderungen die Notwendigkeit bedingen, spezielle Verantwortungen, Verpflichtungen und Belohnungen für die Anbieter von sicheren Infrastrukturen, sicherer Software und sicheren Diensten zu schaffen;
3. Ermittlung jener Instrumente, Dienste und Kooperationsrahmen in Bezug auf bewährte Verfahren, die auf europäischer Ebene gemeinsam von den Akteuren des öffentlichen und des privaten Sektors erarbeitet werden können, um diese Anforderungen zu erfüllen.

Die genannten Maßnahmen werden neben anderen Initiativen auch in Verbindung mit dem bestehenden Auftrag der ENISA zur Verbreitung von Zentren für Finanzinformationen und -analysen (FI-ISAC), der Entwicklung eines Online-Tools für Kleinstunternehmen und dem schwedisch-niederländischen Projekt MIMER (Multipurpose Information Management and Exchange for Robustness, zu dt. etwa: Universelles System für den Austausch und die Verwaltung von Informationen in Bezug auf die Widerstandsfähigkeit) durchgeführt. Weitere Unterstützung besteht in der Einbeziehung der Mitglieder der SGI – darunter sowohl Einzelpersonen als auch weitere Vertreter aus diesen Bereichen – sowie weiterer Netze sektoraler und nationaler Berufsverbände der Abteilung Beziehungen zu den Interessenvertretern (Stakeholder Relations).

Ein Großteil der Arbeit im Rahmen dieser VM erfolgt gemäß der Beschreibung im Arbeitspaket zur VM 2.1. Darüber hinaus wird die Agentur im 1. und 2. Quartal 2010 eine Analyse der wichtigsten Faktoren in Bezug auf die nationalen, EU-weiten und internationalen NIS-Kooperationsstrukturen für Akteure des öffentlichen und privaten Sektors durchführen. Diese Analyse ist eng mit den unter dem TMP 1 beschriebenen Tätigkeiten und Analysen zur Widerstandsfähigkeit von Netzen verbunden sowie mit einem unabhängigen Bericht auf der Grundlage umfassender Befragungen von Vertretern aus wichtigen Mitgliedstaaten und dem privaten Sektor, die an Gemeinschaftsunternehmen beteiligt sind; außerdem nimmt die Analyse Bezug auf die Länderberichte und das Who-is-Who-Verzeichnis im Rahmen des Arbeitspakets 2.3. Ziel dieser Übung ist die eindeutige Ermittlung der Bereiche, in denen die ENISA die Kommission und die Mitgliedstaaten im Rahmen ihres Auftrags am besten bei der Definition der politischen Zielsetzungen unterstützen könnte.

Der Bericht und die Bewertung (VM zum Arbeitspaket 2.1) sollten dann im Rahmen dreier im 2. und 3. Quartal 2010 stattfindenden Workshops erarbeitet und überprüft werden, die von den Mitgliedstaaten oder der ENISA ausgerichtet werden und an denen auf Seite der Lieferkette Vertreter aus zwei bis drei unterschiedlichen Sektoren teilnehmen. Im 4. Quartal 2010 würde die ENISA dann die relevanten Interessenvertreter zu einem abschließenden Workshop versammeln, auf dem die Gesamtergebnisse der geleisteten Arbeit bewertet und über das Jahr 2010 hinausgehende Aktionslinien vorgeschlagen werden.

ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):

SMART-Ziel: Feststellung der Stärken und Schwächen der kommerziellen, wirtschaftlichen und/oder ordnungspolitischen Beschränkungen und Antriebskräfte in Bezug auf die sektorale Zusammenarbeit und der Anreize für die Schaffung von Partnerschaften zwischen dem öffentlichen und dem privaten Sektor bei der Entwicklung verschiedener NIS-Dienste in der Lieferkette	**KPI:** Beteiligung an der Ausarbeitung sektorenübergreifender Initiativen in mindestens drei Lieferketten in mindestens zwei EU-Mitgliedstaaten **KPI:** Ermittlung der Anforderungen für die Beteiligung des öffentlichen Sektors an der Entwicklung von Instrumenten, Diensten und Kooperationsrahmen in Bezug auf bewährte Verfahren durch Akteure auf Nachfrageseite in mindestens zwei Lieferketten
SMART-Ziel: Ermittlung der Möglichkeiten für die Ausarbeitung von Kooperationsinitiativen in mindestens zwei Arbeitsbereichen der ENISA nach 2010	**KPI:** Zahl der ermittelten Instrumente, Dienste und Kooperationsrahmen in Bezug auf bewährte Verfahren, mit denen die ENISA auch nach 2010 befasst sein wird

VORRANGIGE ZIELE, DIE DURCH DAS PROGRAMM UNTERSTÜTZT WERDEN:

- Förderung des Binnenmarkts für elektronische Kommunikation durch die Unterstützung der Institutionen bei der Festlegung geeigneter Gesetzesvorschriften und anderer Maßnahmen
- Intensivierung des Dialogs über die Widerstandsfähigkeit von Netzen, die Sicherheit von Diensten und Software sowie die Privatsphäre und das Nutzervertrauen zwischen den verschiedenen Akteuren in der EU
- Ausweitung der Zusammenarbeit zwischen den Mitgliedstaaten mit dem Ziel, die Unterschiede bei den politischen Initiativen dieser Länder zu verringern
- Stärkung des Vertrauens des öffentlichen und des privaten Sektors in der EU in das „Internet der Zukunft“

AKTEURE UND BEGÜNSTIGTE:

Politische Entscheidungsträger auf Ebene der Mitgliedstaaten und der EU; nationale Regulierungsbehörden (NRA); SGI; Unternehmen in europaweiten Lieferketten; verschiedene „Gemeinschaften des privaten Sektors“ in der Industrie, bei Nutzern/Verbrauchern und in Berufsverbänden

WARUM DIE ENISA?

Durch die Beteiligung vieler verschiedener Interessenvertreter in der SGI, die vorhandenen Netze von Unternehmen und Berufsverbänden (auf nationaler und auf EU-Ebene) und die bereits geleistete Arbeit im Zusammenhang mit der Sicherheit der IKT-Infrastrukturen und -Dienste kann die ENISA in besonderer Weise dazu beitragen, bei den Akteuren des öffentlichen und des privaten Sektors ein hohes

Maß an Vertrauen hinsichtlich der Entwicklung eines Rahmens für die europaweite Zusammenarbeit im Bereich der NIS zu schaffen. Die ENISA ist die einzige offizielle Agentur, die Probleme im Zusammenhang mit europaweiten Lieferketten lösen und die auf dieser Ebene bestehenden Lücken in den Kooperationsmodellen schließen kann; darüber hinaus ist die Agentur eng mit den internationalen Organisationen verbunden, die mit den relevanten Aspekten befasst sind (OECD, ICANN, ITU und Drittländer).
RESSOURCEN FÜR 2010 (Personenmonate und Haushaltsmittel):
• 105 000 EUR • 10 Personenmonate

2.5.1 *VM: Arbeitspaket 2.1 – Anreize und Anforderungen im Zusammenhang mit der NIS-Rahmenstruktur für die Zusammenarbeit mehrerer Interessenvertreter in Gemeinschaften von IKT-Anbietern und –Nutzern*

Bezeichnung des TMP:	
Antriebskräfte und Rahmenstrukturen für die EU-weite sektorale Zusammenarbeit auf dem Gebiet der NIS	
BEZEICHNUNG DES ARBEITSPAKETS:	
VM: Arbeitspaket 2.1 – Anreize und Anforderungen im Zusammenhang mit der Zusammenarbeit mehrerer Interessenvertreter im Bereich der NIS in Gemeinschaften von IKT-Anbietern und -Nutzern	
ANGESTREBTE ERGEBNISSE (KPI für SMART-Ziele):	
SMART-Ziel: Ermittlung der Gefahren, die private Akteure dazu veranlassen, Kooperationsrahmen für eine europaweite gemeinsame Verantwortung für NIS mit Akteuren des öffentlichen Sektors zu erarbeiten	**KPI:** Gemeinsame Entwicklung eines EU-weiten Rahmens durch den öffentlichen Sektor und private Akteure aus mindestens zwei Sektoren in mindestens zwei EU-Mitgliedstaaten
SMART-Ziel: Ermittlung der kommerziellen und der Marktbedingungen, die für Unternehmen auf Nachfrageseite (große Unternehmen und KMU) die Schaffung eines öffentlich-privaten Rahmens für eine sektorenübergreifende Zusammenarbeit im Bereich der NIS erforderlich machen	**KPI:** Marktversagen bei der sektorenübergreifenden Bereitstellung von NIS-Diensten für mindestens zwei Sektoren auf Nachfrageseite in Märkten der großen Unternehmen und/oder KMU-Märkten in mindestens zwei EU-Mitgliedstaaten
SMART-Ziel: Ermittlung relevanter Instrumente oder Dienste für bewährte Verfahren, die zur Unterstützung der Funktionsweise solcher Kooperationsrahmen zu erarbeiten sind	**KPI:** Zahl der ermittelten Instrumente und/oder Dienste für bewährte Verfahren zur Unterstützung der Kooperationsrahmen für große oder kleine Unternehmen in mindestens zwei Sektoren
BESCHREIBUNG DER AUFGABEN:	

Eine erste Aufgabe im Rahmen dieser VM besteht darin, die Stärken und Schwächen der Beschränkungen und Antriebskräfte in Bezug auf die sektorenübergreifende Zusammenarbeit im Bereich der NIS aufzuzeigen und festzustellen, in welchen Bereichen kurz- oder mittelfristig größere Chancen auf Erfolge bestehen und wo in diesem Zusammenhang mehr oder weniger Bedarf an Partnerschaften des öffentlichen und des privaten Sektors besteht. Im Rahmen dieses Arbeitspakets sollen daher die Anforderungen der verschiedenen Gruppen und Akteure des privaten Sektors an die NIS sowie die Anreize untersucht werden, die für ihre Beteiligung an Rahmenstrukturen für die Zusammenarbeit mehrerer Interessenvertreter geschaffen werden.

Im Rahmen dieser VM soll insbesondere untersucht werden, wie die Anforderungen der geschäftlichen Nutzer von netzgestützten Diensten an die NIS sich gegebenenfalls auf die Zusammenarbeit von Software- und Diensteanbietern und Netzbetreibern bei der Entwicklung und Bereitstellung von NIS-Diensten auswirken. In mindestens einer Lieferkette möchte die ENISA bezüglich der erfolgreichen Bereitstellung von Diensten und der angebotsseitigen Zusammenarbeit eine Unterscheidung von Nutzern aus großen Unternehmen und Nutzern aus KMU vornehmen. In Bezug auf KMU-Nutzer soll zudem geklärt werden, ob durch die Beteiligung von Multiplikator-Organisationen bei der Definition der Anforderungen von KMU (anstelle der Zusammenarbeit mit NIS-Diensteanbietern in Einzelfällen) Änderungen vorangetrieben werden können.

Schließlich soll in dieser VM auch ermittelt werden, ob in Fällen, in denen die Anforderungen der Nutzer nicht erfüllt werden, eine Einbindung von Akteuren des öffentlichen Sektors in die Entwicklung von Instrumenten und Diensten für bewährte Verfahren die von den Nutzern geforderte sektorenübergreifende Zusammenarbeit unterstützen kann.

Im 1. und 2. Quartal 2010 führt die Agentur zwei Studien zu den Anforderungen geschäftlicher Nutzer an die NIS durch, wobei in mindestens einer dieser Studien auch Bezug auf KMU der Hochtechnologiebranche genommen wird. Beide Studien decken diese Sektoren in mindestens zwei Mitgliedstaaten ab.

Die Entwürfe dieser Studien, einschließlich erster Ergebnisse, fließen auch in die beiden im 2. und 3. Quartal 2010 stattfindenden Workshops ein, die unter dem allgemeinen Teil der VM 2 von Mitgliedstaaten oder der ENISA organisiert werden. Im 4. Quartal 2010 würde die ENISA dann die relevanten Interessenvertreter zu einem abschließenden Workshop versammeln, auf dem die Gesamtergebnisse der geleisteten Arbeit bewertet und über das Jahr 2010 hinausgehende Aktionslinien vorgeschlagen werden.
ERGEBNISSE UND TERMINE:
• Sektorstudien aus Sicht der Nachfrageseite (Q1, Q2); • Beratungsbericht (Q4); • Workshops (Q2, Q3, Q4)
FOLGENDE INTERESSENVERTRETER SOLLTEN DAS ARBEITSPAKET AKTIV UNTERSTÜTZEN:
Mitgliedstaaten: Verwaltungsrat, nationale Verbindungspersonen, SGI, Netzwerke verschiedener „Themengemeinschaften im privaten Sektor“ (z. B. Industrie, Nutzer/Verbraucher und Hochschulen), einzelne Unternehmen
RESSOURCEN FÜR 2010 (Personenmonate und Haushaltsmittel):
• 105 000 EUR • 10 Personenmonate
VORSCHLAG FÜR DAS ARBEITSPAKET:
ENISA
RECHTSGRUNDLAGE:
ENISA-Verordnung, Artikel 3 Buchstaben c und d

Übersicht über die thematischen Mehrjahresprogramme und Arbeitspakete

TMP 1:	**Verbesserung der Widerstandsfähigkeit der europäischen elektronischen Kommunikationsnetze**	**Haushalts-linie**	**Haushalts mittel**	**Personen-monate**	**Neue Maß-nahme**
AP 1.1	Unterstützung der Anstrengungen der Interessenvertreter bezüglich der Umsetzung der Leitfäden zu bewährten Verfahren für den Informationsaustausch und das Berichtswesen für Sicherheitsvorfälle	3510	100 000	11,5	überarbeitet
AP 1.2	Unterstützung der Anbieter bei der Verbesserung der Widerstandsfähigkeit ihrer Netze	3510	150 000	13,5	überarbeitet
AP 1.3	Untersuchung innovativer Maßnahmen	3520	195 000	17,5	NEIN
AP 1.4	Unterstützung der Interessenvertreter bei der ersten europaweiten Übung	3520	100 000	13,5	überarbeitet
	INSGESAMT		**545 000**	**56**	
TMP 2	**Entwicklung und Fortführung von Kooperationsmodellen**	**Haushalts-linie**	**Haushalts mittel**	**Personen-monate**	**Neue Maß-nahme**
AP 2.1	Plattform für die Zusammenarbeit bei der Sensibilisierung	3310	60 000	24	NEIN
AP 2.2	Sicherheitskompetenzkreis und Austausch bewährter Verfahren für die CERT-Gemeinschaft	3300	135 000	24	NEIN
AP 2.3	Institutionalisierte Verbreitung europäischer bewährter Verfahren im Bereich der NIS	3320	120 000	7	NEIN
	INSGESAMT		**315 000**	**55**	
TMP 3	**Ermittlung aufkommender Risiken zum Zwecke der Vertrauensbildung**	**Haushalts-linie**	**Haushalts mittel**	**Personen-monate**	**Neue Maß-nahme**
AP 3.1	Konzept für die Bewertung und Diskussion aufkommender Risiken – Analyse konkreter Szenarien	3500	120 000	16	NEIN
AP 3.2	Weiterführung der Rahmenstruktur für aufkommende Risiken	3500	35 000	3	NEIN
AP 3.3	Förderung der nationalen Vorsorgemaßnahmen im Rahmen des Risikomanagements	3500	80 000	11	JA
	INSGESAMT		**235 000**	**30**	
VM 1	**„Internet der Zukunft“: Identität, Rechenschaftspflicht und Nutzervertrauen**	**Haushalts-linie**	**Haushalts mittel**	**Personen-monate**	**Neue Maß-nahme**
VM: AP 1.1	Überwachung und Bewertung der Risiken und Bedrohungen für die Widerstandsfähigkeit, den Schutz der Privatsphäre und das Vertrauen, die sich aus der Einführung neuer Technologien ergeben	3520	0	9	JA
VM: AP 1.2	Erarbeitung politischer Strategien mit dem Ziel, ein Gleichgewicht von Transparenz, Rechenschaftspflicht, Einverständnis und Überwachung zu erreichen	3520	0	9	JA
	INSGESAMT		**0**	**18**	

VM 2	Ermittlung von Antriebskräften und Rahmenstrukturen für die EU-weite sektorale Zusammenarbeit auf dem Gebiet der NIS	Haushalts-linie	Haushalts mittel	Personen-monate	Neue Maß-nahme
VM: AP 2.1	Anreize und Anforderungen im Zusammenhang mit der NIS-Rahmenstruktur für die Zusammenarbeit mehrerer Interessenvertreter in Gemeinschaften von IKT-Anbietern und -Nutzern	3520	105 000	10	JA
	INSGESAMT		**105 000**	**10**	
	INSGESAMT (Alle TMP)		**1 200 000**	**169**	

3 HORIZONTALE MASSNAHMEN

Die Agentur wird neben den thematischen Mehrjahresprogrammen eine Reihe von Maßnahmen durchführen, die für die Wahrnehmung ihrer Aufgaben erforderlich sind. Dazu gehören Aktivitäten in den Bereichen der Entwicklung der Strategie und der Verwaltung der öffentlichen Angelegenheiten der ENISA, die Verwaltung von Instanzen und Arbeitsgruppen der ENISA, die Verwaltung der Beziehungen zu externen Interessenvertretern, die Bewertung der Nutzung der Leistungen der ENISA, die Verwaltung der internen Kapazitäten der Agentur, die interne Kommunikation und die Erstellung des Arbeitsprogramms.

3.1. Entwicklung der Strategie und der Verwaltung der öffentlichen Angelegenheiten der ENISA

Die Agentur wird für den Zeitraum bis 2012 und darüber hinaus eine Strategie entwickeln. Die strategischen Anforderungen für die jährlichen Arbeitsprogramme werden im Rahmen des Entwicklungsprozesses des Arbeitsprogramms erarbeitet.

Zur Unterstützung ihrer Arbeit wird die ENISA in den Bereichen Kommunikation und Einbindung verschiedene Aktivitäten durchführen. Im Jahr 2010 wird die Agentur ihre Kommunikationskanäle nutzen und NIS-Experten einbeziehen. Die Aktivitäten zur Unternehmenskommunikation wurden unter den folgenden Haushaltslinien neu strukturiert: Kommunikationstätigkeiten (44 000 EUR), Website der ENISA (20 000 EUR), Gesamtbericht über die Tätigkeiten der ENISA sowie weitere Veröffentlichungen (40 000 EUR). Die Einbindung von NIS-Experten soll durch den vierteljährlich erscheinenden Newsletter „ENISA QUARTERLY“ (40 000 EUR), gemeinsame Veranstaltungen (30 000 EUR) und die Referententätigkeit von ENISA-Experten bei Konferenzen und Veranstaltungen (keine zusätzlichen Haushaltsmittel erforderlich) erreicht werden.

Rechtsgrundlage: ENISA-Verordnung, Artikel 2 Absatz 3 und Artikel 3 Buchstaben a, e, f und k sowie Artikel 7 Absatz 5 Buchstabe a.

3.2. Verwaltung von Instanzen und Arbeitsgruppen der ENISA

Die Agentur wird Sitzungen des Verwaltungsrats (110 000 EUR) und der Ständigen Gruppe der Interessenvertreter durchführen (100 000 EUR, einschließlich einer informellen Sitzung von Verwaltungsrat/SGI). Die Koordinierung der Aktivitäten der Arbeitsgruppen und die Verwaltung des Netzes nationaler Verbindungspersonen wurden in die TMP-Maßnahmen eingebunden.

Rechtsgrundlage: ENISA-Verordnung, Artikel 5, Artikel 6, Artikel 7 Absatz 4 Buchstaben g, h und i sowie Artikel 7 Absatz 8.

3.3. Verwaltung der Beziehungen zu externen Interessenvertretern

Die Agentur wird in enger Zusammenarbeit mit den Dienststellen der Kommission den Aufbau und die Pflege von Beziehungen zu EU-Institutionen, Industrie, Hochschulen und

Verbrauchervertretern, zu Drittländern und internationalen Institutionen (z. B. ITU, IETF und OECD) fortsetzen und die Möglichkeit der Unterstützung öffentlich-privater Partnerschaften, die die verschiedenen Akteure zusammenbringen, erörtern. Darüber hinaus wird die ENISA Bereiche von gemeinsamem Interesse ermitteln und bewerten, in welchem Umfang eine Zusammenarbeit mit diesen Akteuren bei spezifischen Maßnahmen der Agentur realisierbar ist (z. B. Förderung des Dialogs über die Entwicklung von sicherer Software zwischen der Industrie und der Kommission als Gesetzgeber). Diese Tätigkeiten erfordern Finanzmittel in Höhe von 410 000 EUR für Dienstreisen der Mitarbeiter, 5 000 EUR für Repräsentationskosten, 3 000 EUR für Sitzungen des Büros des Direktors und 10 000 EUR für sonstige Sitzungen.

Rechtsgrundlage: ENISA-Verordnung, Artikel 3 Buchstaben c und j sowie Artikel 7 Absatz 4 Buchstaben g und h.

3.4. Verwaltung der internen Kapazitäten

Die Agentur wird ihre Who-is-Who-Datenbank für die Kontakte zum öffentlichen und privaten Sektor auch künftig pflegen und erweitern (0 EUR). Mit der Schaffung einer internen Auditstelle setzt die Agentur ihre Aktivitäten zum internen Risikomanagement und zur Informationssicherheit fort (25 000 EUR). Darüber hinaus behält die Agentur die Übersetzung (20 000 EUR) von offiziellen Finanzdokumenten bei.

Rechtsgrundlage: ENISA-Verordnung, Artikel 7 Absatz 4 Buchstabe d.

3.5. Verwaltung der internen Kommunikation der ENISA

Die Agentur legt großen Wert auf den Informationsaustausch und die Zusammenarbeit zwischen Mitarbeitern und Führungskräften sowie allgemein innerhalb des gesamten Personals. Zu diesem Zweck hat die Agentur verschiedene interne Kommunikationskanäle eingerichtet. Sie wird in regelmäßigen Abständen ein internes Mitteilungsblatt herausgeben, einmal in der Woche interne Mitarbeiterbesprechungen durchführen und den Informationsaustausch über das eigene Intranet fördern.

Rechtsgrundlage: ENISA-Verordnung, Artikel 7 Absatz 4 Buchstaben d und f.

3.6. Erstellung des Arbeitsprogramms

Die Agentur erstellt jedes Jahr ihr jährliches Arbeitsprogramm. Das Programm wird nach der Anhörung der Ständigen Gruppe der Interessenvertreter vom Verwaltungsrat genehmigt. Grundsätzlich sind für diese Tätigkeit keine Haushaltsmittel erforderlich.

Rechtsgrundlage: ENISA-Verordnung, Artikel 7 Absatz 5 Buchstabe b, Artikel 7 Absatz 6 sowie Artikel 9.

Übersicht über die horizontalen Maßnahmen

HM 1	Beratung und Unterstützung	Haushalts-linie	Haushalts mittel	Personen-monate	Neue Maß-nahme
HM 1.1	Koordinierung und Bearbeitung von Anfragen	3320	0	0,5	NEIN
HM 1.2	Beantwortung von Anfragen	3320	0	0,5	NEIN
	INSGESAMT		**0**	**1,0**	
HM 2	**Kommunikation mit den Akteuren im Bereich der NIS und deren Einbindung**	**Haushalts-linie**	**Haushalts mittel**	**Personen-monate**	**Neue Maß-nahme**
HM 2.1	Strategieentwicklung	p.m.	0	2,0	überarbeitet
HM 2.2	Verwaltung der öffentlichen Angelegenheiten	p.m.	0	10,5	überarbeitet
HM 2.3	Kommunikationstätigkeiten	3210	44 000	5,5	überarbeitet
HM 2.4	Website der ENISA	3220	20 000	21	NEIN
HM 2.5	Gesamtbericht über die Tätigkeiten der ENISA und Veröffentlichungen	3210	40 000	6	NEIN
HM 2.6	Newsletter „ENISA QUARTERLY“	3240	40 000	4	NEIN
HM 2.7	Gemeinsame Veranstaltungen	3200	30 000	4	NEIN
HM 2.8	Referententätigkeit	Entfällt	0	11	NEIN
	INSGESAMT		**174 000**	**64**	
HM 3	**Verwaltung von Instanzen und Arbeitsgruppen der ENISA**	**Haushalts-linie**	**Haushalts mittel**	**Personen-monate**	**Neue Maß-nahme**
HM 3.1	Verwaltungsrat	3003	110 000	4	NEIN
HM 3.2	Ständige Gruppe der Interessenvertreter	3000	100 000	4	NEIN
HM 3.3	Koordinierung der Arbeitsgruppen	Entfällt	0	2	NEIN
HM 3.4	Netz nationaler Verbindungspersonen	Entfällt	0	2	NEIN
	INSGESAMT		**210 000**	**12**	

HM 4	Verwaltung der Beziehungen zu externen Interessenvertretern	Haushalts-linie	Haushalts mittel	Personen-monate	Neue Maß-nahme
HM 4.1	Aufbau von Beziehungen zu Industrie, Hochschulen, Verbrauchervertretern, internationalen Einrichtungen und Drittländern	3330	0	4,5	NEIN
HM 4.2	Verwaltung der Beziehungen zu EU-Einrichtungen	3320	0	3,5	NEIN
HM 4.3	Dienstreisen des Büros des Direktors	3015	35 000	0	NEIN
HM 4.5	Dienstreisen der operativen Abteilungen	3013	345 000	0	NEIN
HM 4.6	Dienstreisen der Verwaltungsabteilung	3014	30 000	0	NEIN
HM 4.7	Repräsentationskosten	3011	5000	0	NEIN
HM 4.8	Sitzungen des Büros des Direktors	3005	3000	0	NEIN
HM 4.9	Sonstige Sitzungen	3021	10 000	0	NEIN
	INSGESAMT		**428 000**	**8**	
HM 5	**Verwaltung der internen Kapazitäten der ENISA**	**Haushalts-linie**	**Haushalts mittel**	**Personen-monate**	**Neue Maß-nahme**
HM 5.1	Who-is-Who-Datenbank	3320	0	0	NEIN
HM 5.2	Interne Auditstelle der ENISA	3400	25 000	1	NEIN
HM 5.3	Übersetzungen	3230	20 000	0	NEIN
	INSGESAMT		**45 000**	**1**	
HM 6	**Verwaltung der internen Kommunikation der ENISA**	**Haushalts-linie**	**Haushalts mittel**	**Personen-monate**	**Neue Maß-nahme**
HM 6.1	Internes Mitteilungsblatt, Mitarbeiterbesprechungen, Informationsaustausch über das Intranet	Entfällt	0	4	NEIN
	INSGESAMT		**0**	**4**	
HM 7	**Erstellung des Arbeitsprogramms**	**Haushalts-linie**	**Haushalts mittel**	**Personen-monate**	**Neue Maß-nahme**
HM 7.1	Erstellung des Arbeitsprogramms 2011	Entfällt	0	10	NEIN
	INSGESAMT		**0**	**10**	
	INSGESAMT (Horizontale Maßnahmen)		**857 000**	**100**	

4 BERATUNG UND UNTERSTÜTZUNG

Die Agentur hat seit 2006 Ersuchen der Mitgliedstaaten (8), der Europäischen Kommission (6) und anderer europäischer Einrichtungen (2) erhalten (siehe Übersicht unten). Für 2010 wird mit dem Eingang weiterer Ersuchen gerechnet. Damit erfüllt die Agentur die in den Artikeln 2, 3 und 10 der Gründungsverordnung vorgesehene Rolle.

Das Verfahren für die Bearbeitung von Ersuchen ist in Artikel 6 der internen Verfahrensvorschriften festgelegt. Die Agentur legt anhand von Kriterien wie der Verfügbarkeit von Ressourcen, der Weiterführung langfristiger Maßnahmen, bestehender Verpflichtungen und des erwarteten zusätzlichen Nutzens sowie der Auswirkungen, die die Beantwortung des Ersuchens auf EU-Ebene hat, die Priorität der Bearbeitung fest.

Grundsätzlich werden an die Agentur gerichtete Ersuchen in der Reihenfolge ihres Eingangs bearbeitet. Falls erforderlich, konsultiert der Direktor umgehend den Verwaltungsrat, bevor eine Entscheidung über die Rangfolge der Bearbeitung getroffen wird.

Übersicht: Im Zeitraum Dezember 2005 bis Juni 2009 bearbeitete Ersuchen

Ersuchende Stelle	Thema	Haushaltsmittel [EUR]	ENISA-Personal [Personenmonate]
1) EDSB	Unterstützung bei der Prüfung des EURODAC-Systems	3400	1,6
2) Kommission	Bewertung der Sicherheitsmaßnahmen der Anbieter elektronischer Kommunikationsdienste	0	2,2
3) NRA Litauen	Unterstützung bei der Einrichtung von CERT mit der Durchführung einer CERT-Schulung in Litauen	6745	0,8
4) Kommission	Stellungnahme zur Folgenabschätzung der geplanten Mitteilung	0	1,3
5) Kommission	Beratung zur Halbzeitüberprüfung der Richtlinie über elektronische Signaturen	850	0,5
6) Kommission	Beratung zum elektronischen ID-Management in Kommissionsdienststellen	850	1,1
7) Tschechische Republik	Bewertung der Sicherheitsanforderungen für Informationssysteme der öffentlichen Verwaltung	0	0,6
8a) Kommission	Prüfung der Realisierbarkeit eines Rahmens zur Erhebung von Daten	50 000	6,0
8b) Kommission	Prüfung der Realisierbarkeit eines europäischen Informationsaustausch- und Warnsystems	25 000	4,0
9) Griechenland	Beratung zur Verschlüsselung im Bereich der Telefonie	0	0,1
10) Österreich	Zusammenarbeit zwischen SBA und ENISA	0	0,1
11) Österreich	Fragebogen zu Risikomanagement und -analyse	0	1,0
12) Bulgarien	Förderung der Zusammenarbeit zwischen Ungarn und Bulgarien bei der Einrichtung des CERT der bulgarischen Regierung	0	1,0
13) Griechenland	Aufbau eines CSIRT bei FORTH-ICS	0	0,1
14) Österreich	Unterstützung bei der Einrichtung von CERT mit der Durchführung einer CERT-Schulung	6745	0,8
15) Europ. Parlament	Beratung zu Fragen der Internetsicherheit	0	0,5
16) Zypern	Unterstützung bei der Einrichtung eines CERT der Regierung	0	0,5

5 VERWALTUNGSTÄTIGKEITEN

Die Verwaltungsabteilung der ENISA sorgt für die Einhaltung der Vorschriften und setzt sich für eine weitere Verbesserung der Funktionsfähigkeit der Verwaltungsverfahren der Agentur ein, um verlässliche Dienstleistungen erbringen zu können. Zu den Arbeitsschwerpunkten der Verwaltungsabteilung für 2010 gehören die Optimierung des Umfangs und der Qualität der verfügbaren Dienste im Einklang mit den Zielsetzungen, für die die Ergebnisse der internen Kontrollstandards und Audits Beispiele enthalten. In diesem Zusammenhang werden elektronische Arbeitsabläufe auch in neuen Tätigkeitsbereichen eingeführt, und um die Geschäftskontinuität zu gewährleisten, werden die Risiken weiter verringert. Für das Jahr 2010 hat sich die Verwaltungsabteilung Folgendes zum Ziel gesetzt:

- Optimierung des Umfangs und der Qualität der verfügbaren Dienste
- Verringerung der mit Verstößen verbundenen Risiken
- Gewährleistung der Geschäftskontinuität

Im Jahr 2010 wird die Verwaltungsabteilung sich weiter mit den horizontal ausgerichteten Aufgabenbereichen der Agentur, wie Rechnungsführung und interne Kontrolle, austauschen. Im Arbeitsprogramm für 2010 werden die Schwerpunkttätigkeiten dieser beiden Aufgabenbereiche, die eng mit den Tätigkeiten der Verwaltungsabteilung verzahnt sind, erneut aufgeführt.

5.1. Allgemeine Verwaltung

Zu den Aufgaben der Verwaltungsabteilung gehören die Wahrnehmung allgemeiner Verwaltungstätigkeiten und die Messung der Leistung der Verwaltungsabteilung. Wichtige Aufgabenbereiche sind unter anderem die Planung, Beratung, Vertretungsaufgaben, Berichterstattung und Überwachung der Tätigkeiten der einzelnen Fachbereiche sowie der Abteilung als Ganzes. Zu den wichtigsten Aufgaben der allgemeinen Verwaltung für 2010 gehören:

- Mehrjahresplanung der Tätigkeiten
- Überwachung der jährlichen Ausführung des Haushaltsplans
- Planung elektronischer Arbeitsabläufe
- Verringerung der mit Verstößen verbundenen Risiken
- Gewährleistung der Geschäftskontinuität

Die wichtigsten für 2010 geplanten Tätigkeiten umfassen:

Nr.	Beschreibung	Leistungen	Leistungsindikatoren	Termine	Haushaltsmittel
1.1	Planung der Verwaltungs-tätigkeiten Vertretung der Verwaltung	Planung von Tätigkeiten, Beratung und Management; Festlegung von Zielen und Prioritäten; Abstimmung mit den Abteilungen und Fach-bereichen der Agentur; Zusammenarbeit mit wichtigen Mitarbeitern, um die Ziele zu erreichen; Personalführung	Planung der Tätigkeiten nach Fachbereichen; Hilfestellung für die Erreichung der Ziele; Jahresarbeitsplan; Koordination der Zielvorgaben für das Verwaltungspersonal; Kommunikation	laufend	0

1.2	Beratung und Unterstützung des Direktors und der Abteilungsleiter in allen verwaltungsbezogenen Fragen einschließlich Verwaltungsstrukturen, wirtschaftliche Haushaltsführung, maßnahmenbezogenes Management, Ausfallplanung, Geschäftskontinuität, Rechtsdienste und Vermögenswerte	Erstellung von Berichten für den Direktor und Zusammenarbeit mit den Abteilungsleitern und gegebenenfalls mit wichtigen Mitarbeitern	Kontinuierliche Unterstützung des Direktors und der Abteilungsleiter; termingerechte Bearbeitung aller Unterstützungsanfragen; Unterstützung bei der Durchführung interner Kontrollen; Unterstützung der Systeme zur Überwachung der Vermögenswerte	wöchentlich	0
1.3	Sicherstellen, dass jederzeit eine ordnungsgemäße Berichterstattung über die Verwendung der Ressourcen der Agentur gewährleistet ist; Auswirkungen auf Finanzdaten und Berichtslinien der Verwaltung	Nach Bedarf	Regelmäßige Bewertung der internen und externen Berichterstattungsanforderungen	vierteljährlich	0
			Berichterstattung und Überwachung		
1.4	Überwachung von Audit-Ergebnissen, Arbeitspraktiken und -verfahren im Einklang mit der Haushaltsordnung, den Durchführungsbestimmungen und dem Statut; Abstimmung mit den Bereichen Koordination der internen Kontrolle und Rechnungsführung; Geschäftskontinuitätsplanung; MwSt-Erstattung	Aktualisierung von Dokumenten und Berichterstattung über Tätigkeiten; Koordination mit internen (Koordination der internen Kontrolle, Rechnungsführung, Risikomanagement) und externen Akteuren (ECA, IAS usw.)	Umsetzung von Audit-Empfehlungen; Kontinuierliche Verbesserung der Leistung; Risikomanagement	vierteljährlich	0
1.5	Allgemeine organisatorische Aufgaben	Archivierung, Berichterstattung, Unterstützung von Bereichen der Verwaltungsabteilung nach Bedarf, Durchführung von Finanztransaktionen nach Bedarf	Umfang der Tätigkeiten; termingerechte Durchführung	laufend	0
1.6	Bürodienste	Verwaltung horizontaler Aufgaben einschließlich Übersetzung, Büromaterial, Logistik, Büroverwaltung, Sicherheit, Postdienste, Fuhrpark	Umfang der Tätigkeiten; termingerechte Durchführung	laufend	384 000
1.7	Beziehungen zu den griechischen Behörden	Regelmäßiger Kontakt zum Direktor und Beratung hinsichtlich der Beziehungen zu den Mitgliedstaaten	Zahl der bearbeiteten Fälle; Schnelligkeit der Reaktion	laufend	0
1.8	Bearbeitung von Ersuchen des Personals bezüglich der Vereinbarung über den Sitz der Agentur (besondere Ausweisdokumente, Zulassung der Fahrzeuge, Befreiung von der MwSt usw.)[12]	Regelmäßige Bearbeitung von Ersuchen bezüglich der MwSt-Befreiung für das Personal der Agentur	Zahl der bearbeiteten Fälle; Schnelligkeit der Reaktion	laufend	0

[12] *Vgl.* Tätigkeiten der Direktion im Zusammenhang mit den Beziehungen zu den griechischen Behörden.

5.2. Finanzen

Zu den Aufgaben der Abteilung Finanzen gehören Planung und Verwaltung des Haushalts sowie Finanzkontrolle, aber auch Teile der Lohnverwaltung und die Koordination und Sicherstellung von Dienstreisen. Die Abteilung Finanzen verfolgt das Ziel, die Glaubwürdigkeit der Finanzabläufe und der Haushaltsplanung sicherzustellen. Durch die enge Überwachung der Haushaltsplanung und -ausführung kann die Agentur die Verwendungsquote bezüglich ihrer Haushaltsmittel zugunsten ihrer Betriebsabläufe optimieren und Haushaltsengpässen entgegenwirken. Im Jahr 2010 hat die Abteilung Finanzen folgende Arbeitsschwerpunkte:

- Haushaltsplanung einschließlich tätigkeitsbezogene Budgetierung
- Überwachung und Planung der Haushaltsausführung
- Funktionelle Unterstützung in Bezug auf elektronische Arbeitsabläufe (ABAC, Dienstreisen-Management)

Die wichtigsten für 2010 geplanten Tätigkeiten umfassen:

Nr.	Beschreibung	Leistungen	Leistungsindikatoren	Termine	Haushalts-mittel
2.1	Aufstellung und Abschluss des Jahreshaushalts und Erstellung der Haushalts-erklärungen	Ausführung des genehmigten Haus-haltsplans; ordnungs-gemäße Mittelzuweisung	Abruf von Mitteln aus den Haushaltslinien des Jahreshaushalts ab Ende der dritten Woche des Geschäftsjahrs; Übersicht über das wirtschaftliche Ergebnis; termingerechte Ausführung unterstützender Maßnahmen	bis Ende Januar und bis Ende der dritten Dezember-woche; Vorlage bis 10. Dezember	0
2.2	Durchführung und Konsolidierung interner Verfahren und Kontrollen für alle Finanzabläufe einschließlich Dienstreisen.	Jährliche Überprüfung der internen Verfahren und Kontrollen; regelmäßige Durch-führung von Kontrollen für alle Finanz-transaktionen	Überprüfung von Leitlinien und Checklisten; jährliche Risikobewertung; entsprechende Aktualisierung der Kontrollen; Durchführung von Schulungen zur Sensibilisierung für die Verfahren und Kontrollen; Durchführung von Kontrollen	vierteljährlich	0
2.3	Berichterstattung über die Ausführung des jährlichen Haushaltsplans	monatlich	Berichterstattung über den aktuellen Stand der Durchführung des Haus-haltsplans für alle Bereiche, Titel und Abteilungen, soweit erforderlich, einschließlich der Analyse der wichtigsten Aspekte	monatlich (für den Vormonat)	0
2.4	Durchführung von Mittelübertragungen	Unterstützung der Abteilungen bei der Durchführung von Mittelübertragungen	Kommunikation, Zeit und Kontrolle	jährlich bis zum Ende der zwei-ten Kalender-woche	0
2.5	Lohnverwaltung	Finanzielle Aspekte der Lohnverwaltung in Zusammenarbeit mit der Abteilung Human-ressourcen; Planung und Kontrolle	Termingerechte Auszahlung der Löhne und Gehälter und gegebenenfalls Abstimmung mit dem Amt für die Feststellung und Abwicklung individueller Ansprüche	monatlich	0

5.3. Humanressourcen

Zu den Aufgaben der Abteilung Humanressourcen gehören wiederkehrende Aufgaben und allgemeine Tätigkeiten, insbesondere im Zusammenhang mit Personalbeschaffung, Leistungsbewertung, Weiterbildungsmaßnahmen, Gesundheit und Sicherheit am Arbeitsplatz, Urlaubsmanagement, Verwaltung individueller Ansprüche und Lohnverwaltung. Die Abteilung Humanressourcen möchte im Einklang mit dem Personalstatut Strategien für die rechtzeitige Personalbeschaffung und die Personalbindung schaffen.

Im Jahr 2010 befasst sich die Abteilung Humanressourcen mit der Konsolidierung der 2009 erfolgten organisatorischen Änderungen, die bei der Ausführung der operativen Ziele im Rahmen der TMP eine stärkere hierarchische Kontrolle der Agentur bedeuten. Im Jahr 2010 hat die Abteilung Humanressourcen folgende Arbeitsschwerpunkte:

- erneute Ressourcenplanung (Personalentwicklungsplan)
- messbare Maßnahmen zur Personalbindung (Personalabgangsquote, Ziele, Kosten der Personalfluktuation, Weiterbildungsmaßnahmen, Beförderungen usw.)
- Bereitstellung von Diensten über elektronische Arbeitsabläufe

Die wichtigsten für 2010 geplanten Tätigkeiten umfassen:

Nr.	Beschreibung	Leistungen	Leistungsindikatoren	Termine	Haushaltsmittel
3.1	Personal-entwicklungsplan und Durchführungs-bestimmungen	Ausarbeitung, Aktualisierung und Weiterverfolgung aller Änderungen im Statut und den dazugehörigen Durchführungsbe-stimmungen sowie gegebenenfalls in anderen Personal-vorschriften; Erstellung, Aktualisierung und Überwachung des Personalentwicklungs-plans	Aktualisierte Durchführungsbe-stimmungen, Unterrichtung des Personals; Zusammenarbeit mit der Personalvertretung und der Kommission in Bezug auf die Durchführungsbestimmungen und den Personalentwicklungsplan	laufend	0
3.2	Titel 1, Lohnverwaltung und individuelle Ansprüche; Ausschuss für Personaleinstufung (Einstufungsausschuss); Verwaltungskosten der Kommission	Termingerechte Ausführung der monatlichen Lohn- und Gehaltszahlungen; individuelle Ansprüche; Einstufungsausschuss; Verwaltungskosten der Kommission	Wahrnehmung aller Aufgaben in Verbindung mit Titel 1, Lohnverwaltung; Überprüfung der Kontenbuchungen; Abstimmung der korrekten Buchungen mit der Buchhaltung und dem Amt für die Feststellung und Abwicklung individueller Ansprüche; Ex-post-Kontrolle der Zahlungsbelege; Verwaltungskosten der Kommission für Leistungen im Bereich der Lohnbuchhaltung	monatlich; Einstufung sausschuss (2-3 Sitzungen pro Jahr)	4 520 000
3.3	Bewertung der Personalleistung	Jährliche Leistungs-bewertung und Probezeitbewertungen; Vorgabe und Ab-stimmung von Zeit-plänen; Unterstützung bei Beschwerden; Überwachung der Stellen- und Aufgaben-beschreibungen	Anzahl der Bewertungen; Planung; rechtzeitiger Abschluss von Vorgängen	einmal jährlich, bei Probezeit be-wertunge n nach Bedarf	0
3.4	Jährliches Weiterbildungs-programm	Weiterbildungsprogramm (intern, extern, auf Eigeninitiative); Konzeption, Umsetzung und Bewertung von Weiterbildungsmaß-nahmen	Planung der Weiter-bildungsmaßnahmen; Vorlage und Genehmigung der Unterlagen; Weiter-bildungsangebote in den Kernleistungsbereichen	jährlich	100 000
3.5	Einstellungsplan	Umsetzung des Ein-stellungsplans der Agentur im Einklang mit dem Stellenplan; Veröffent-lichung von Stellen-ausschreibungen; Bildung von Auswahlausschüssen; Kommunikation mit den Bewerbern; Einarbeitung neuer Mitarbeiter	Anzahl der Neueinstellungen bzw. Neubesetzungen; benötigte Zeit für Einstellungen; Planung von Leitlinien für den Wieder-einstieg von Mitarbeitern	laufend	474 200
3.6	Gesundheit und Sicherheit am Arbeitsplatz	Jahresprogramm für Gesundheitsschutz und Sicherheit	Verwaltung des Jahresprogramms für Gesundheitsschutz und Sicherheit (ärztliche Untersuchungen, Gesundheitsattests für die Einstellung, Arbeitsbedingungen, erste Hilfe, Gesundheitsberater, Gesundheitszentrum)	jährlich	44 000
3.7	Dienste von Dritten	Aushilfs-leistungen und Beratung	Aushilfsleistungen, um kurzfristige Verpflichtungen, Aufgaben und saisonale Unterstützung abzudecken; Berater im Bereich T1, z. B. für die Rechtsberatung	jährlich	159 000

5.4. IKT

Das IKT-Team betreut die internen IKT-Systeme und -Netze der Agentur. Das Team als Wertschöpfungseinheit ist mit der Bearbeitung von Kundenanforderungen befasst und für die Planung und das jederzeit reibungslose Funktionieren aller verfügbaren IT-Systeme verantwortlich, insbesondere der Server, Datenbanken, Endgeräte (z. B. PCs, Laptops, Handys), Netze, Telekommunikation usw. Ein Teil seiner Arbeit, insbesondere Arbeiten im Zusammenhang mit Internetzugang, Finanzverwaltungssystemen usw., wird an Dritte untervergeben, das Team übernimmt dabei eine Vermittlerrolle und bietet Unterstützung. Das IKT-Team ist in Bezug auf Nutzeranforderungen, Ausfallplanung und Geschäftskontinuität alleinige Anlaufstelle für alle verfügbaren IT-Ressourcen. Im Jahr 2010 hat das IKT-Team folgende Arbeitsschwerpunkte:

- Aktualisierungen von Hardware und Software am Ende ihres Lebenszyklus
- Leistungsniveaus für bestehende elektronische Arbeitsabläufe
- Risikomanagement im Hinblick auf die Geschäftskontinuität

Die wichtigsten für 2010 geplanten Tätigkeiten umfassen:

Nr.	Beschreibung	Leistungen	Leistungsindikatoren	Termine	Haushalts-mittel
4.1	Planung von IKT-Systemen in Bezug auf Hardware, Software und Netze	Pflege der durch die ENISA oder Dritte errichteten IKT-Netze und -Systeme; Verwaltung der Software-Lizenzen; Nutzeranforderungen	Verfügbarkeit und Integrität der Systeme; Ausfallzeiten; Ausfallplanung	laufend	105 000
4.2	IKT-Dienste und ABAC-Kosten	Verfügbarkeit der Dienste festlegen und sicherstellen	Nach festgelegten Standards erbrachte Dienstleistungen	laufend	85 000
4.3	Interner IKT-Support	ABAC-Administration und -Support; Support für die allgemeinen Systeme und Netze und den Helpdesk; Wartung; Tests	Support-Anfragen; Ergebnisse eines Prüfplans; Wartungsplan	laufend	0
4.4	Risikomanagement und Sicherheitsplan für die Ressourcen der Agentur; Geschäftskontinuität	Sicherstellung der Vertraulichkeit und Integrität der Systeme; Zusammenarbeit mit ITMAC, dem Risikomanagement-Team und der Technologiegruppe	Planung und Durchführung von Maßnahmen zur Risikominderung; Bearbeitung von Sicherheitsverletzungen	vierteljährlich	0

5.5. Rechtsfragen

Die Abteilung für Rechtsfragen ist für Aufgaben im Zusammenhang mit der Ausführung und Kontrolle des Haushaltsplans zuständig, zu denen die allgemeine Vertragsverwaltung und das öffentliche Beschaffungswesen der Agentur gehören. Sie übernimmt eine Doppelrolle, um einerseits die Einhaltung der vorherrschenden Rechtsvorschriften und Verordnungen durch die Agentur sicherzustellen und andererseits der Verwaltung und dem Personal der ENISA bei Bedarf geeignete Dienste bereitzustellen, damit die Zielsetzungen bezüglich der Einhaltung von Vorschriften erfüllt werden können. Die Abteilung unterstützt die Agentur durch Rechtsberatung und Rechtsdienste und bietet Beratungs- und Dienstleistungen für den Bereich des Beschaffungswesens an. Darüber hinaus kann sie auch operative Ad-hoc-Unterstützung leisten, wenn dies für bestimmte Maßnahmen erforderlich und mit den operativen Abteilungen abgestimmt ist. Für 2010 hat die Abteilung für Rechtsfragen folgende Arbeitsschwerpunkte geplant:

- Organisation der internen Infrastruktur in Bezug auf einen elektronischen Arbeitsablauf für das Beschaffungswesen
- effiziente Beschaffungsplanung
- Vertragsverwaltungsplanung

Die wichtigsten für 2010 geplanten Tätigkeiten umfassen:

Nr.	Beschreibung	Leistungen	Leistungsindikatoren	Termine	Haushalts-mittel
5.1	Rechtsberatung auf Ersuchen des Direktors und der Abteilungen; Koordinierung des Datenschutzes	Erstellen von Rechtsgutachten auf Anforderung; Vertretung der Agentur in allen maßgeblichen Instanzen; Beteiligung an internen und externen Veranstaltungen und Tätigkeiten; Aufgaben des Datenschutz-beauftragten und Bericht-erstattung an EDSB	Anzahl der behandelten internen Fälle (Rechtsgutachten, Beschwerden, Rechtsfälle, Berichte, in denen zentrale Elemente zusammengefasst und relevante Informationen weitergegeben werden); Koordinierung des Datenschutzes	laufend	0
5.2	Öffentliches Beschaffungswesen	Regelmäßige Durchführung von Verfahren zur Vergabe öffentlicher Aufträge und geeignete Unterstützung aller Abteilungen; Beschaffungsplanung	Beschaffungspläne, verfügbare Laufzettel und Formulare; Anzahl und Art der durchgeführten Vergabeverfahren; erstellte Dokumentation; Lieferaufträge; Lieferantendatenbank; bearbeitete Anfragen; Beschaffungsplanung und Bündelung der Beschaffungsmaßnahmen	laufend	0
5.3	Vertragsverwaltung	Allgemeine Unterstützung bei der Vertragsverwaltung	Anzahl der aufgesetzten und von der Agentur unterzeichneten Verträge; Anzahl der Unter-stützungsanfragen der Abteilungen; Anzahl der diesen Bereich betreffenden Beschwerden; Laufzettel	laufend	0
5.4	Operative Unterstützung	Beratung zu rechtlichen Aspekten der operativen Tätigkeit der ENISA auf Anforderung und nach Vereinbarung	Zeitaufwand für die Bearbeitung der Vorgänge und die entsprechende Berichterstattung	*ad hoc*; auf Anforderung und nach Vereinbarung	0
5.5	Vertretung	Vertretung bei offiziellen Veranstaltungen und bei Verwaltungs- und Haushaltsbehörden sowie bei Gericht nach Zustimmung des Direktors	Anzahl der bearbeiteten Fälle	laufend	0

5.6. Rechnungsführung[13]

Die Rechnungsführung der ENISA ist ein gesonderter Funktionsbereich, der gemäß der Haushaltsordnung folgende Aufgaben erfüllt:

- Jahresrechnungsabschluss der Agentur
- Führung der Bücher mit Buchführungsjournal, Hauptbuch und Bestandsverzeichnis
- Bestandsverzeichnisse über die Anlagewerte
- Zahlungen usw.

Nr.	Beschreibung	Leistungen	Leistungsindikatoren	Termine	Haushalts-mittel
6.1	Zahlungen und Rechnungslegung	Anweisung von Zahlungen; Berichterstattung; Jahresabschluss	Genauigkeit; Schnelligkeit der Bearbeitung; Einhaltung förmlicher Termine	laufend	0
6.2	Koordinierung von Audits	Stellungnahmen des Rechnungsführers; Beratung der Leitung und des Personals in Fragen der Rechnungs-führung; ggf. Abstimmung mit externen Akteuren, insbesondere dem Rechnungshof	Zahl der unterstützten Fälle; Schnelligkeit der Reaktion	laufend	0

[13] Infolge der kürzlich durchgeführten Neuausrichtung der Organisation der ENISA erstattet die Rechnungsführung nun der Verwaltungsabteilung Bericht.

Übersicht über die Verwaltungstätigkeiten

VT 1	Allgemeine Verwaltung	Haushaltslinie	Haushalts-mittel	Personen-monate14	Neue Maßnahme
VT 1.1	Planung der Verwaltungstätigkeiten; Vertretung	Entfällt	Entfällt	1,6	NEIN
VT 1.2	Beratung und Unterstützung	Entfällt	Entfällt	3	NEIN
VT 1.3	Berichterstattung über die Verwendung der Ressourcen der Agentur	Entfällt	Entfällt	2	NEIN
VT 1.4	Follow-up von Audits	Entfällt	Entfällt	2	NEIN
VT 1.5	Allgemeine organisatorische Aufgaben	Entfällt	Entfällt	13,4	NEIN
VT 1.6	Bürodienste	Titel 2 ausgenommen Kapitel 23 IKT	384 000	10	NEIN
VT 1.7	Kontakt zu und Beratung bezüglich der griechischen Behörden[15]	Entfällt	Entfällt	3,2	NEIN
VT 1.8	Bearbeitung von Ersuchen des Personals bezüglich der Vereinbarung über den Sitz der Agentur (besondere Ausweisdokumente, Zulassung der Fahrzeuge, Befreiung von der MwSt usw.)	Entfällt	Entfällt	3,2	NEIN
	INSGESAMT		**384 000**	**38,4**	
VT 2	**Finanzen**	**Haushaltslinie**	**Haushalts-mittel**	**Personen-monate**	**Neue Maßnahme**
VT 2.1	Aufstellung und Abschluss des Jahreshaushaltsplans	Entfällt	Entfällt	3	NEIN
VT 2.2	Durchführung und Konsolidierung interner Kontrollen	Entfällt	Entfällt	19,2	NEIN
VT 2.3	Berichterstattung über die Ausführung des jährlichen Haushaltsplans	Entfällt	Entfällt	2,6	NEIN
VT 2.4	Durchführung von Mittelübertragungen	Entfällt	Entfällt	2	NEIN
VT 2.5	Lohnverwaltung	Entfällt	Entfällt	2	NEIN
	INSGESAMT			**28,8**	
VT 3	**Humanressourcen**	**Haushaltslinie**	**Haushalts-mittel**	**Personen-monate**	**Neue Maßnahme**
VT 3.1	Personalentwicklungsplan	Entfällt	Entfällt	2	NEIN
VT 3.2	Lohnverwaltung, individuelle Ansprüche und Einstufung	Kapitel 11	4 520 000	9,6	NEIN
VT 3.3	Leistungsbewertung	Entfällt	Entfällt	4,0	NEIN
VT 3.4	Jährliches Weiterbildungsprogramm	1320	100 000	4	NEIN
VT 3.5	Einstellungsplan	Kapitel 12	474 200	14,6	NEIN
VT 3.6	Gesundheit und Sicherheit am Arbeitsplatz	1310	44 000	1	NEIN
VT 3.7	Dienste von Dritten	Kapitel 14	159 000	0	NEIN
	INSGESAMT		**5 297 200**	**38,4**	

[14] Ein Jahr wird auf der Grundlage von 9,6 Monaten pro Mitarbeiter im Organigramm berechnet.

[15] Mit dieser Aufgabe ist der Personalvorstand betraut.

VT 4	IKT	Haushaltslinie	Haushalts-mittel	Personen-monate	Neue Maßnahme
VT 4.1	IKT-Systemplanung	2300	105 000	4,8	NEIN
VT 4.2	IKT-Dienste	2301+2302	85 000	4,8	NEIN
VT 4.3	Interner IKT-Support	Entfällt	0	14,4	NEIN
VT 4.4	IT-Risikomanagement und Geschäftskontinuität	Entfällt	0	4,8	NEIN
	INSGESAMT		**190,00**	**28,8**	
VT 5	**Rechtsfragen und Beschaffungswesen**	**Haushaltslinie**	**Haushalts-mittel**	**Personen-monate**	**Neue Maßnahme**
VT 5.1	Rechtsberatung und -vertretung	Entfällt	Entfällt	6	NEIN
VT 5.2	Öffentliches Beschaffungswesen	Entfällt	Entfällt	9,6	NEIN
VT 5.3	Vertragsverwaltung	Entfällt	Entfällt	2	NEIN
VT 5.4	Operative Unterstützung	Entfällt	Entfällt	0,6	NEIN
VT 5.5	Vertretung	Entfällt	Entfällt	1	NEIN
	INSGESAMT		**0**	**19,2**	
VT 6	**Rechnungsführung**	**Haushaltslinie**	**Haushalts-mittel**	**Personen-monate**	**Neue Maßnahme**
VT 6.1	Zahlungen und Erstellung der Jahresabschlüsse	Entfällt	Entfällt	25,6	NEIN
VT 6.2	Koordinierung von Audits	Entfällt	Entfällt	Noch festzulegen	NEIN
	INSGESAMT		**0**	**25,6**	
	GESAMTSUMME		**5 871 200**	**179,2**	

6 TÄTIGKEITEN DER DIREKTION

In der Direktion der ENISA stellen die Berichtslinien die horizontalen Aufgaben der Rechnungsführung sicher.

6.1 Beziehungen zu den griechischen Behörden

Die Beziehungen zu den griechischen Behörden stehen in engem Zusammenhang mit der Verpflichtung der beteiligten Parteien im Rahmen der zwischen Griechenland und der ENISA geschlossenen Vereinbarung über den Sitz der Agentur. Die Hauptaufgaben im Rahmen dieser Tätigkeiten betreffen die regelmäßige Zusammenarbeit und den regelmäßigen Dialog mit:

- dem Ministerium für Transport und Telekommunikation als dem zuständigen Ministerium für den Bereich Informationssicherheit und dem führenden Ministerium in allen Angelegenheiten der ENISA;
- den zuständigen Stellen für Politik und öffentliche Verwaltung in Griechenland;
- dem interministeriellen Ausschuss, der von Griechenland eingerichtet wurde, um aufkommende Probleme der ENISA schnell und wirksam zu lösen;
- den lokalen Behörden (Präfektur, Stadtverwaltung, Polizei), um so das reibungslose Funktionieren der Agentur und den Schutz der Rechte der Mitarbeiter sicherzustellen;
- *dem Außenministerium, um Fragen im Zusammenhang mit den der Agentur als konsularische* Vertretung sowie ihren Mitarbeitern verliehenen Rechten (spezielle Ausweisdokumente, CD-Kennzeichen, MwSt-Befreiung usw.) zu klären.

Nr.	Beschreibung	Leistungen	Leistungsindikatoren	Termine	Haushaltsmittel
6.1.1	Kontakte zu den griechischen Behörden	Kontaktaufnahme, Berichterstattung und Folgemaßnahmen zu den verschiedenen Aktivitäten in Bezug auf die griechischen Behörden	Termingerechte Abwicklung der Fälle; Einhaltung von Fristen	laufend	0

Übersicht über die Tätigkeiten der Direktion

DIR		Haushalts-linie	Haushalts mittel	Personen-monate16	Neue Maßnahme
DIR 1.1	Kontakt zu und Beratung bezüglich der griechischen Behörden und Bearbeitung der Ersuchen an die Agentur im Zusammenhang mit der Vereinbarung über den Sitz der Agentur	Entfällt	Entfällt	3,2	NEIN
	INSGESAMT		**0**	**3,2**	
	GESAMTSUMME		**0**	**3,2**	

[16] Ein Jahr wird auf der Grundlage von 9,6 Monaten pro Mitarbeiter im Organigramm berechnet.

7 ANHANG 1 – OPERATIVE AKTIVITÄTEN IM ZUSAMMENHANG MIT DEM ARBEITSPROGRAMM 2010

OPERATIVE AKTIVITÄTEN IM ZUSAMMENHANG MIT DEM ARBEITS-PROGRAMM 2010		Operative HR (Hinweis 1)	Lohnkosten Operative HR (Hinweis 2)	Operative Aufwendungen (Hinweis 3)	Gemeinkosten (Hinweis 4)	Gesamtkosten (Tätigkeiten)
TMP 1:	Verbesserung der Widerstandsfähigkeit der europäischen elektronischen Kommunikationsnetze	6,2	620 814	545 000	268 936	1 434 210
TMP 2:	Entwicklung und Fortführung von Kooperationsmodellen	6,3	625 707	315 000	270 512	1 211 218
TMP 3:	Ermittlung aufkommender Risiken zum Zwecke der Vertrauensbildung	3,9	387 813	235 000	167 663	790 476
VM 1:	„Internet der Zukunft“: Identität, Rechenschaftspflicht und Nutzervertrauen	1,9	187 400	0	81 018	268 418
VM 2:	Ermittlung von Antriebskräften und Rahmenstrukturen für die EU-weite sektorale Zusammen-arbeit auf dem Gebiet der NIS	1,0	101 508	105 000	43 885	250 393
HM 1:	Beratung und Unterstützung	0,0	0	0	0	0
HM 2:	Kommunikation und Einbindung	7,6	759 385	174 000	328 305	1 261 690
HM 3:	Verwaltung von Instanzen und Arbeits-gruppen der ENISA	1,6	156 166	210 000	67 515	433 682
HM 4:	Verwaltung der Beziehungen zu externen Interessen-vertretern	0,3	27 069	428 000	11 703	466 772
HM 5:	Verwaltung der internen Kapazitäten der ENISA	0,0	0	45 000	0	45 000
HM 6:	Verwaltung der internen Kommuni-kation der ENISA	0,3	26 028	0	11 253	37 280
HM 7:	Erstellung des Arbeitsprogramms	0,9	92 659	0	40 059	132 718
Verwaltungstätigkeiten Abteilungen		4,2	421 129	0	182 066	603 195
Verwaltungstätigkeiten Abteilungsleiter		0,9	93 700	0	40 509	134 209
Tätigkeiten des Sekretariats		6,0	599 679	0	259 259	858 938
Insgesamt		41,0	4 099 056	2 057 000	1 772 144	7 928 200

Hinweis 1: Die operative HR (Human Resources) setzt sich aus Mitarbeitern der ENISA und den abgeordneten nationalen Sachverständigen zusammen, die direkt an den operativen Tätigkeiten beteiligt sind.

Hinweis 2: Die Lohnkosten der operativen HR setzen sich aus den Kosten für das Personal und die abgeordneten nationalen Sachverständigen zusammen, die direkt an den operativen Tätigkeiten beteiligt sind.

Hinweis 3: Bei den operativen Aufwendungen handelt es sich um die direkten Kosten jeder Aktivität im Rahmen des Arbeitsprogramms und des Ausgabenplans für 2010.

Hinweis 4: Die Gemeinkosten beinhalten alle nicht operativen Kosten wie die Gehälter von nicht im operativen Bereich tätigem Personal, Betriebskosten (z. B. für die Lieferung von Büromaterial) usw.