

(2) à étudier la possibilité de soutenir financièrement cette initiative sur la base des financements prévus pour les activités de formation par la décision du Conseil du 9 décembre 1999 instituant un programme d'action communautaire en faveur de la protection civile <sup>(1)</sup> pour la période allant du 1<sup>er</sup> janvier 2000 au 31 décembre 2004 ou par ladite décision du Conseil instituant un mécanisme communautaire visant à favoriser une coopération renforcée dans le cadre des interventions de secours relevant de la protection civile;

<sup>(1)</sup> JO C 327 du 21.12.1999, p. 53.

(3) à associer les pays candidats à ses travaux;

(4) à considérer, à l'expiration de cette phase pilote et à la lumière des résultats obtenus, toute initiative visant la mise en place d'une coopération à long terme en matière de formation dans le secteur de la protection civile, par exemple, notamment par le biais de la création d'une académie européenne de protection civile qui institutionnaliserait le réseau précité.

## RÉSOLUTION DU CONSEIL

du 28 janvier 2002

relative à une approche commune et à des actions spécifiques dans le domaine de la sécurité des réseaux et de l'information

(2002/C 43/02)

LE CONSEIL DE L'UNION EUROPÉENNE,

EN RÉPONSE:

aux conclusions du Conseil européen de Stockholm des 23 et 24 mars 2001 selon lesquelles le Conseil, en concertation avec la Commission, mettra au point une vaste stratégie en matière de sécurité des réseaux électroniques, prévoyant des mesures de mise en œuvre pratique;

RAPPELANT:

- 1) la résolution du Conseil du 30 mai 2001 (Plan d'action eEurope: sécurité de l'information et des réseaux);
- 2) la communication de la Commission au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions intitulée: «Sécurité des réseaux et de l'information: proposition pour une approche politique européenne»;
- 3) la communication de la Commission au Conseil et au Parlement européen intitulée «eEurope 2002: Impact et priorités»;
- 4) le plan d'action «eEurope 2002» approuvé par le Conseil européen de Santa Maria da Feira des 19 et 20 juin 2000;
- 5) la recommandation 95/144/CE du Conseil du 7 avril 1995 concernant des critères communs d'évaluation de la sécurité des technologies de l'information <sup>(1)</sup>;
- 6) la recommandation du Conseil du 25 juin 2001 concernant les points de contact assurant un service vingt-quatre heures sur vingt-quatre pour lutter contre la criminalité liée à la haute technologie <sup>(2)</sup>;

<sup>(1)</sup> JO L 93 du 26.4.1995, p. 27.

<sup>(2)</sup> JO C 187 du 3.7.2001, p. 5.

7) la communication de la Commission sur la création d'une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité;

8) le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation des ces données <sup>(3)</sup>;

9) la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données <sup>(4)</sup>;

10) la directive 97/33/CE du Parlement européen et du Conseil du 30 juin 1997 relative à l'interconnexion dans le secteur des télécommunications en vue d'assurer un service universel et l'interopérabilité par l'application des principes de fourniture d'un réseau ouvert (ONP) <sup>(5)</sup>;

11) la directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications <sup>(6)</sup>;

12) la directive 98/10/CE du Parlement européen et du Conseil du 26 février 1998 concernant l'application de la fourniture d'un réseau ouvert (ONP) à la téléphonie vocale et l'établissement d'un service universel des télécommunications dans un environnement concurrentiel <sup>(7)</sup>;

<sup>(3)</sup> JO L 8 du 12.1.2001, p. 1.

<sup>(4)</sup> JO L 281 du 23.11.1995, p. 31.

<sup>(5)</sup> JO L 199 du 26.7.1997, p. 32.

<sup>(6)</sup> JO L 24 du 30.1.1998, p. 1.

<sup>(7)</sup> JO L 101 du 1.4.1998, p. 24.

13) la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques <sup>(1)</sup>;

CONSIDÉRANT CE QUI SUIT:

- (1) Les réseaux et les systèmes de communications sont devenus un facteur clé du développement économique et social. En outre, leur existence et leur intégrité sont vitales pour des infrastructures essentielles, de même que pour la plupart des services publics et privés et pour l'économie dans son ensemble.
- (2) Étant donné le rôle de plus en plus important joué par les services électroniques dans l'économie, la sécurité des réseaux et des systèmes d'information est de plus en plus une question d'intérêt public.
- (3) La sécurité des transactions et des données est désormais essentielle pour la fourniture des services électroniques, notamment les opérations commerciales et les services publics en ligne, et le manque de confiance dans la sécurité risquerait de ralentir l'introduction à grande échelle de ces services.
- (4) Il est nécessaire que les particuliers, les entreprises, les administrations et les autres organisations protègent leurs propres systèmes d'information, de stockage des données et de communication en utilisant, lorsqu'il y a lieu, des technologies de sécurité efficaces.
- (5) Le secteur privé, agissant dans un environnement de marché concurrentiel et grâce à sa capacité d'innovation, apporte un éventail de solutions adaptées aux besoins réels du marché.
- (6) La nature complexe de la sécurité des réseaux et de l'information oblige les autorités publiques, lorsqu'elles élaborent des mesures dans ce domaine, à tenir compte de divers aspects politiques, économiques, organisationnels et techniques, et à garder à l'esprit le caractère décentralisé et mondial des réseaux de communication.
- (7) Les mesures politiques peuvent être plus efficaces si elles s'inscrivent dans une approche européenne, respectent le fonctionnement efficace du marché intérieur, s'appuient sur une coopération accrue entre les États membres et au niveau international et soutiennent l'innovation, ainsi que la capacité des entreprises européennes d'être concurrentielles au niveau mondial.
- (8) Il existe déjà une abondante législation sur la sécurité des réseaux et de l'information qui fait notamment partie du cadre juridique de l'Union relatif aux télécommunications, au commerce électronique et aux signatures électroniques.

(9) Il existe des dispositions légales qui imposent aux fournisseurs de services de télécommunications de prendre des mesures appropriées au niveau technique et organisationnel pour garantir la sécurité de leurs services, ces mesures assurant un niveau de sécurité approprié eu égard au risque connu.

- (10) La norme internationale ISO-15408 (Critères communs) est désormais un système reconnu pour définir les exigences de sécurité des produits d'ordinateurs et de réseaux et évaluer si un produit donné satisfait à ces exigences.
- (11) La norme internationale ISO-17799 («Technologies de l'information — Code de pratique pour la gestion des sécurité de l'information») et d'autres dispositions nationales similaires sont aujourd'hui des références reconnues pour la gestion des problèmes de sécurité dans les organismes privés et publics.
- (12) L'infrastructure de l'Internet devrait permettre un niveau élevé d'accès aux réseaux et services et être gérée et exploitée d'une manière solide et sûre, par exemple par l'adoption de normes ouvertes et de protocoles de sécurité concernant l'Internet;

CONSIDÉRANT, conformément à la résolution du Conseil du 30 mai 2001 intitulée «Plan d'action «Europe: sécurité de l'information et des réseaux», que la sécurité des réseaux et de l'information a pour finalité:

- d'assurer la disponibilité des services et des données,
- de prévenir la perturbation et l'interception non autorisée des communications,
- de confirmer que les données qui ont été envoyées, reçues ou stockées sont complètes et n'ont pas subi de modification,
- d'assurer la confidentialité des données,
- de protéger les systèmes d'information contre l'accès non autorisé,
- de protéger les réseaux contre les attaques utilisant des logiciels malveillants,
- de permettre une authentification fiable;

PAR CONSÉQUENT, INVITE LES ÉTATS MEMBRES

- 1) d'ici la fin de 2002, à lancer des campagnes d'information et d'éducation afin d'attirer l'attention sur le problème de la sécurité des réseaux et de l'information, ou à renforcer les campagnes en cours; à cibler particulièrement, à travers ces actions, les entreprises, les particuliers et les administrations publiques; à élaborer ces actions de sensibilisation en étroite coopération avec le secteur privé, notamment les fournisseurs de services Internet, et à encourager les initiatives menées par le secteur privé;

<sup>(1)</sup> JO L 13 du 19.1.2000, p. 12.

- 2) à encourager l'adoption, notamment dans les petites et moyennes entreprises, de pratiques éprouvées dans la gestion de l'information, fondées, s'il y a lieu, sur des normes reconnues au niveau international;
  - 3) d'ici la fin de 2002, à renforcer ou promouvoir, dans l'enseignement de l'informatique ou dans la formation dans ce domaine, l'importance des notions de sécurité;
  - 4) d'ici le milieu 2002, à évaluer l'efficacité des dispositifs nationaux d'intervention en cas d'urgence informatique, au nombre desquels pourraient figurer les systèmes d'alerte aux virus, afin de renforcer, au besoin, leur capacité au niveau national et international, à être efficaces sur le plan de la prévention, de la détection et de la réaction en cas de perturbations et d'attaques de systèmes de réseaux et d'information;
  - 5) à promouvoir l'utilisation de la norme relative aux critères communs (ISO-15408) et à faciliter la reconnaissance mutuelle des certificats qui s'y rapportent;
  - 6) d'ici la fin 2002, à prendre des mesures significatives visant l'adoption de solutions efficaces et interopérables en matière de sécurité, fondées si possible sur des normes reconnues — au nombre desquelles pourraient figurer des logiciels libres — dans leurs activités d'administration en ligne et de passation de marchés par voie électronique, ainsi que l'introduction de signatures électroniques pour permettre aux services publics nécessitant une authentification solide d'être également accessibles en ligne;
  - 7) lorsqu'ils optent pour l'introduction de systèmes d'identification électronique et biométrique destinés à un usage public ou officiel, à coopérer, s'il y a lieu, à l'évolution technologique et à examiner toutes les exigences d'interopérabilité qui pourraient se présenter;
  - 8) en vue de faciliter la coopération au sein de la Communauté et au niveau international, à échanger des informations entre eux et avec la Commission sur les organismes compétents au premier chef pour les questions de sécurité des réseaux et de l'information sur leur territoire;
- en plus grande à l'égard des réseaux de communications électroniques, et, dans ce contexte, de proposer d'ici la fin de 2002 une stratégie permettant un fonctionnement plus stable et plus sûr de l'infrastructure de l'Internet;
- 3) d'ici la fin de 2002, de proposer des mesures appropriées destinées à promouvoir la norme ISO 15408 (critères communs), à faciliter la reconnaissance mutuelle des certificats et à améliorer le processus d'évaluation des produits, par exemple en définissant des profils de protection appropriés;
  - 4) d'ici la fin de 2002, d'élaborer un rapport sur les technologies et les applications de l'authentification électronique et biométrique de l'identité, en vue d'améliorer l'efficacité de ces systèmes, notamment par l'interopérabilité;
  - 5) d'ici la fin de 2002, de faire des propositions — en consultation avec les États membres et le secteur privé — en vue de la mise en place d'un groupe de travail sur la cybersécurité afin de tirer profit des efforts entrepris au niveau national pour améliorer la sécurité des réseaux et de l'information et la capacité des États membres à faire face, isolément et collectivement, à de graves problèmes de sécurité des réseaux et de l'information;
  - 6) d'ici la fin de 2002, d'étudier, en collaboration avec les États membres, les différentes formules possibles pour la mise en place de mécanismes permettant aux États membres et à la Commission d'échanger des informations et des expériences concernant la réalisation des objectifs de la présente résolution, en tenant compte du fait que la sécurité des réseaux et de l'information concerne plusieurs piliers, et d'étudier les meilleurs moyens d'associer le secteur privé à cet échange d'informations et d'expériences;

SE FÉLICITE que les activités de recherche européenne accordent une place de plus en plus grande aux questions de sécurité;

SOULIGNE la nécessité d'entreprendre davantage de recherches, notamment sur les mécanismes de sécurité et leur interopérabilité, sur la fiabilité et la protection des réseaux, sur la cryptographie de pointe, sur les technologies servant à renforcer la confidentialité et sur la sécurité des communications sans fil;

ENGAGE:

SE FÉLICITE DE L'INTENTION DE LA COMMISSION

- 1) de faciliter l'échange de pratiques éprouvées concernant les actions de sensibilisation et de dresser un premier inventaire des différentes campagnes d'information nationales en 2002;
- 2) de faire en 2002 des propositions pour renforcer le dialogue et la coopération de la Communauté avec les organisations et les partenaires internationaux sur la sécurité des réseaux, et notamment sur les implications de la dépendance de plus

— les fournisseurs et les prestataires des services à renforcer la sécurité en tant qu'elle fait partie intégrante de leurs produits et services et en constitue un élément essentiel,

— les fournisseurs et les prestataires de services européens du secteur privé et leurs associations représentatives à participer plus activement aux travaux internationaux dans le domaine de la normalisation et à se regrouper dans des enceintes appropriées pour contribuer à la réalisation des objectifs de la présente résolution.