Réforme 2007 des télécommunications dans l'UE #6

European Commission
Information Society and Media

Sécuriser les autoroutes européennes de l'information

Les entreprises, les gouvernements et les consommateurs dépendent de plus en plus des télécommunications et des réseaux qui les sous-tendent, internet compris. Ils sont devenus le moteur de notre économie et structurent notre société moderne. Mais nous devons être vigilants. Internet subit constamment les attaques des auteurs de spams et autres cybercriminels. Que se passerait-il si le système s'écroulait ? Les téléphonies fixe et portable dépendent de la disponibilité de l'infrastructure existante. À quel point sommes-nous vulnérables ? L'Europe a besoin de réseaux de communication sûrs et fiables. Elle doit proposer une réponse coordonnée aux menaces d'aujourd'hui et de demain.

Les réseaux de communication sont un élément essentiel de notre économie et de notre société. Ils constituent de plus en plus le principal vecteur pour la fourniture de services vitaux aux entreprises, aux gouvernements et aux citoyens. La sécurisation des réseaux de communication est dès lors devenue aussi essentielle que l'électricité, pour assurer le bon fonctionnement de notre économie et de notre société numérique.

DES MENACES TOUJOURS PLUS GRANDES

Les technologies de l'information et de la communication ont facilité les activités commerciales transfrontalières dans la vie publique comme dans la vie privée. Mais toutes sortes d'activités criminelles et terroristes ont également tiré profit des vertus de ces technologies. Ces menaces constituent un défi considérable pour la société moderne.

Ces dernières années, les menaces auxquelles nous faisons face ont fondamentalement changé. Les agressions d'aujourd'hui sont de plus en plus sophistiquées et organisées. Ce n'est pas tellement la curiosité ou le désir de montrer leur virtuosité technique qui poussent les agresseurs à agir mais plutôt le profit. Les logiciels malveillants (malwares) sont en outre de plus en plus souvent utilisés pour divulguer des données confidentielles, d'où des usurpations d'identité et des pertes financières significatives, en particulier lorsque les informations volées concernent des cartes de crédit ou des données bancaires.

L'Estonie, la France, l'Allemagne et le Royaume-Uni ont récemment fait l'objet de cyberattaques massives. Les citoyens, les entreprises et les gouvernements ont tous été touchés d'une façon ou d'une autre.

Ces développements risquent d'ébranler la confiance du consommateur et de le rendre méfiant à l'égard des promesses de la révolution numérique, une tendance inquiétante pour notre économie toujours plus dépendante d'internet. Même les entreprises prudentes et réputées ont fait état de violations de la sécurité ayant exposé la confidentialité des informations de leurs clients à des risques inconnus.

Les spams (qui, selon les estimations, représentent 40% à 90% du volume total des e-mails) continuent à poser problème. Souvent distribués par de vastes « réseaux » de PC corrompus, les spams ne se contentent plus d'être une simple nuisance et une intrusion dans la sphère privée d'un individu, mais ils véhiculent virus et autres logiciels malveillants. Au niveau mondial, les dommages économiques imputables à ces logiciels sont estimés à €9,2 milliards par an.

Et comme les systèmes et les réseaux continuent à évoluer et sont de plus en plus

complexes, nous pouvons nous attendre à une recrudescence des problèmes de sécurité. Les nouvelles technologies et applications, comme les dispositifs pour les étiquettes radio intelligentes (RFID) et l'informatique ubiquitaire, ouvriront certes de nouvelles opportunités, mais elles présenteront aussi de nouveaux défis en matière de sécurité et de protection de la vie privée.

LA RESPONSABILITÉ DE TOUS !

En matière de sécurité, le principe de la chaîne s'applique: elle est aussi solide que son maillon le plus faible. Toutes les parties prenantes doivent donc être à la hauteur de leurs responsabilités. Sinon, tout point faible sera férocement exploité, offrant un accès aux pirates informatiques et autres criminels. Tout le monde – gouvernement, entreprise et individu – a un rôle à jouer et une responsabilité à remplir.

C'est la raison pour laquelle la sécurité des réseaux et des informations est l'une des priorités de la réforme 2007 des télécoms dans l'UE.

UN RESPONSABLE DE LA SÉCURITÉ DES RÉSEAUX POUR L'EUROPE

L'UE va fortement intensifier la lutte contre les violations de sécurité, sur le plan tant des réseaux que du traitement des données. La future Autorité européenne du marché des télécommunications comptera la sécurité des réseaux et des informations parmi ses tâches essentielles. Elle aura aussi la mission d'assister la Commission dans la mise en œuvre de nouvelles mesures et dans la coordination, à l'échelle européenne, de réponses aux menaces qui pèsent sur la sécurité. La création de cette nouvelle Autorité, dont le besoin se fait fortement sentir, contribuera à stimuler la coordination et la coopération entre les États membres et les institutions de l'UE d'une part, et entre le secteur public et le secteur privé d'autre part. Dirigée par un Responsable de la sécurité des réseaux, elle assumera ainsi les fonctions actuellement remplies par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), qui a déjà fait la preuve de sa plus-value européenne. En sa qualité d'organe unique et intégré, paré des atouts nécessaires pour pouvoir compter sur la meilleure expertise d'Europe, l'Autorité jouera un rôle important dans la mise en place d'une vraie culture de sécurité à travers le continent. Elle contribuera, par la promotion d'approches communes et par l'échange de bonnes pratiques, à la réalisation d'un haut niveau de sécurité, qui protègera la création de services paneuropéens et participera à la prospérité des entreprises dans un environnement européen sécurisé. Un groupe permanent de parties prenantes assurera un contact étroit entre l'Autorité et le secteur privé afin d'améliorer la sécurité des réseaux.

INTENSIFIER LA PROTECTION

La réforme vise à garantir des télécoms sécurisés et de grande qualité. À cet effet, elle renforcera le cadre actuel en matière de protection de la vie privée et de sécurité des réseaux. Les décideurs, par exemple, seront mieux informés du niveau réel de sécurité des réseaux de manière à pouvoir prendre de meilleures décisions. La clarté sera accrue quant aux mesures de sécurité que les opérateurs de télécoms doivent prendre pour s'assurer que les réseaux et services qu'ils fournissent soient sûrs, fiables et inviolables. De plus, les fournisseurs de services victimes de violations devront avertir leurs clients lorsque leurs données personnelles seront compromises, de manière à leur permettre de prendre toutes les précautions nécessaires.

Les nouvelles règles doteront également les opérateurs et les organes compétents de meilleurs instruments pour combattre les spams, logiciels malveillants et autres menaces de sécurité, et pour ainsi protéger les intérêts de leurs clients. Par ailleurs, le nouveau cadre renforcera le pouvoir d'exécution des régulateurs. Enfin, il insistera sur le fait que les règles actuelles de protection de la vie privée s'appliquent aussi aux communications électroniques qui utilisent des étiquettes radio intelligentes (RFID) et des dispositifs similaires.

Pour toute information :

Bureau d'information
Commission européenne – DG Société de l'information et médias
Bureau : BU 25 02/61 B-1049 Bruxelles
E-mail : infso-desk@ec.europa.eu
Tél : +32 2 299 93 99
http://ec.europa.eu/ecomm