Distr.
GÉNÉRALE

CES/SEM.47/11 (Summary)
9 janvier 2002

FRANÇAIS
Original: ANGLAIS

COMMISSION DE STATISTIQUE et COMMISSION ÉCONOMIQUE POUR L'EUROPE

COMMISSION DES COMMUNAUTÉS EUROPÉENNES

CONFÉRENCE DES STATISTICIENS EUROPÉENS

EUROSTAT

Séminaire commun CEE−Eurostat sur les systèmes intégrés d'information statistique et les questions connexes (ISIS 2002)
(Genève, Suisse, 17-19 avril 2002)

Thème II: Sécurité des communications et confidentialité des données

LA PRATIQUE DE L'INFORMATIQUE SÛRE

Communication sollicitée

Établie et présentée par Eduardo Gelbstein[1]

Résumé

1. La sécurité informatique est désormais un thème de première importance, compte tenu de la diffusion considérable des virus informatiques et de la banalisation de phénomènes tels que l'utilisation abusive des informations figurant sur les cartes de crédit. Toutefois, la nécessité de protéger l'information remonte aux débuts de l'écriture, il y a environ 5 000 ans.

2. Ce document se compose de deux parties. La première décrit les «acteurs» et les «infractions». Les *acteurs* sont les nombreuses parties intervenant dans le domaine de la sécurité de l'information; parmi eux figurent, du côté des «mauvais garçons», tant les apprentis pirates (habituellement de jeunes passionnés d'informatique qui acquièrent les outils utilisés par des pirates plus avertis) que les espions industriels, le crime organisé et les services secrets «d'autres pays» et, du côté des «gentils», des professionnels de la sécurité, de l'audit, etc.

[1] Consultant indépendant sur la gestion des systèmes et des technologies informatiques (ed.gelbstein@wanadoo.fr).

GE.02-30064 (F) 250202 250202

Les *infractions* sont les actes qui ont des conséquences en termes de disponibilité, de confidentialité et d'intégrité de l'information stockée sous forme numérique. Ces infractions vont bien au-delà de la diffusion de virus et comprennent la fraude et le sabotage, le vol d'information et de logiciels protégés, l'utilisation de codes nuisibles, les dénis de service et autres attaques, manœuvres qui sont toutes décrites en détail dans le document.

3. La deuxième partie du document est un guide pratique de l'*informatique sûre*. S'il est vrai que les entreprises se sont dotées (ou devraient se doter) de politiques, de directives, d'outils et de technologies destinés à assurer un niveau adéquat de sécurité de l'information, on constate une tendance croissante à l'utilisation de l'informatique mobile et sans fil, à domicile, c'est-à-dire en dehors du périmètre de sécurité installé au sein des entreprises.

4. Pour pratiquer l'informatique sûre, il est nécessaire de réunir les différents éléments suivants:

- Des outils, par exemple des logiciels de détection des virus et des pare-feu personnels;

- Certaines procédures systématiques, telles que sauvegardes régulières et mises à jour périodiques des définitions de virus;

- Du «bon sens», par exemple dans des domaines comme la non-divulgation, la façon de traiter les courriers électroniques suspects et la sensibilisation aux attaques possibles.

Cette partie du document examine ces trois éléments de façon suffisamment détaillée pour que le lecteur puisse appliquer les conseils prodigués.
