Distr.
GÉNÉRALE

CES/SEM.47/13 (Summary)
30 janvier 2002

FRANÇAIS
Original: ANGLAIS

COMMISSION DE STATISTIQUE et COMMISSION ÉCONOMIQUE POUR L'EUROPE
CONFÉRENCE DES STATISTICIENS EUROPÉENS

COMMISSION DES COMMUNAUTÉS EUROPÉENNES (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

CHIFFREMENT ET ORDINATEURS PORTABLES

Communication sollicitée

de Statistics Sweden[1]

Résumé

1. Le monde actuel exige une mobilité accrue et l'on recourt de plus en plus aux ordinateurs portables. Il suffit d'une minute pour s'emparer d'un ordinateur portable laissé sans surveillance. Et si le voleur n'est pas intéressé par l'ordinateur lui-même mais par les informations sensibles stockées sur son disque dur, comment protéger ces dernières? L'objet de cette étude est de passer en revue les produits de chiffrement que l'on trouve sur le marché, de choisir un produit susceptible de répondre aux besoins de Statistics Sweden et d'appliquer la solution choisie.

2. Ce sont essentiellement les informations sensibles, qui se trouvent généralement sous la forme de fichiers non protégés sur le disque dur, qui suscitent des préoccupations en termes de sécurité.

[1] Préparée par Behzad Panahi (behzad.panahi@scb.se).

3. Statistics Sweden détient beaucoup de registres et fichiers différents renfermant des données sensibles tels que:

- o des registres couverts par le secret défense;
- o des registres nationaux concernant l'ensemble de la population, des entreprises et du patrimoine immobilier;
- o des données couvertes par le secret d'affaires;
- o des résultats de différentes enquêtes sur la santé, le revenu, la planification familiale);
- o des registres concernant des enfants victimes de mauvais traitements, des toxicomanes et des délinquants.

Par ailleurs, le public fait fond sur les statistiques et les informations SCB.

Les ordinateurs portables sont largement utilisés au sein de Statistics Sweden et la nécessité d'envisager le chiffrement ne fait aucun doute.

4. Le chiffrement est utilisé depuis des milliers d'années pour garder des informations secrètes. Il existe deux types de chiffrement: le chiffrement asymétrique et le chiffrement symétrique. Le chiffrement symétrique consiste à transformer (à chiffrer) un texte en clair (les données originales) en texte chiffré (les données protégées) de façon à ce qu'il soit impossible de réaliser l'opération inverse sans avoir une parfaite connaissance de la fonction qui a permis la transformation. Le chiffrement asymétrique, ou à clef publique, consiste aussi à transformer un texte en clair en texte chiffré à l'aide d'un algorithme et d'une clef. La différence réside dans l'utilisation d'une clef de déchiffrement différente de la clef de chiffrement, d'où le qualificatif «asymétrique».

5. La clef (privée) de déchiffrement est liée à la clef (publique) de chiffrement mais ne peut être reconstituée sur la base de cette dernière. C'est pourquoi, la clef de chiffrement ne doit pas être gardée secrète et peut être divulguée. En revanche, les utilisateurs d'une clef publique doivent pouvoir être sûrs qu'elle appartient bien à tel ou tel propriétaire. Le processus de certification répond à ce besoin. La sécurité réside dans la préservation du secret de la clef privée.

Questions de sécurité au sein de Statistics Sweden

6. Il convient de tenir compte du fait que:

- l'ennemi est un individu et non une puissance étrangère;
- la politique mise en œuvre par l'entreprise se fonde sur l'utilisation des produits Microsoft;
- l'entreprise a également conclu des contrats avec IBM.

7. En raison des incertitudes qui pèsent sur la durée de vie et sur le support futur des produits de sécurité, il a été décidé d'un commun accord de choisir Encryption File System pour Windows 2000, et de le soumettre à une étude approfondie, afin de le mettre en œuvre de façon adéquate sur les ordinateurs portables.

Encryption File System pour Windows 2000

8. Encryption File System pour Windows 2000 résout les problèmes:

- de chiffrement et déchiffrement manuels à chaque utilisation, à savoir que dans la plupart des cas, les fonctions de chiffrement ne sont pas transparentes pour l'utilisateur qui doit donc déchiffrer le fichier avant chaque utilisation et le rechiffrer lorsqu'il a terminé;
- de fuites à partir des fichiers temporaires et des fichiers de pagination, en ce sens que ces fichiers temporaires restent non chiffrés sur le disque, même si le document original est chiffré, ce qui facilite le vol de données;
- de manque de sécurité lié au fait que les clefs sont déterminées à partir de mots de passe ou de formules, une intrusion dans le dictionnaire pouvant aisément déjouer ce type de protection si les mots de passe utilisés sont faciles à retenir;
- d'absence de récupération de données, de nombreux produits ne proposant pas de fonction de récupération de données.

Comment fonctionne le chiffrement avec Encryption File System (EFS)?

9. EFS se fonde sur le chiffrement à clef publique et sur l'utilisation de CryptoAPI. Chaque fichier est chiffré à l'aide d'une clef créée de façon aléatoire, appelée *clef de chiffrement de fichier*, qui est indépendante du couple clef publique/clef privée de l'utilisateur; cette procédure empêche beaucoup de types différents d'attaques de fichiers chiffrés fondées sur l'analyse cryptographique.

10. Si le fichier original est chiffré, EFS chiffre ses copies temporaires lorsque des caractéristiques sont transférées au cours de la création de fichier. EFS se trouve dans la partie résidente de Windows 2000, utilise la zone non paginable pour stocker les clefs de chiffrement de fichier et veille à ce que celles-ci ne soient jamais stockées dans le fichier de pagination.

11. Le chiffrement et le déchiffrement se font fichier par fichier ou par répertoire entier. Le chiffrement des répertoires est mis en œuvre en mode transparent.

12. EFS détecte automatiquement un fichier chiffré et repère le certificat de l'utilisateur ainsi que la clef privée qui y est associée dans les mémoires de certificats d'utilisateur et de clefs.

Conclusions

13. Il a été conclu que Windows 2000 propose un niveau acceptable de chiffrement, adapté aux besoins de Statistics Sweden. Il a été décidé que tous les ordinateurs portables les plus récents qu'il sera possible de faire passer à Windows 2000 bénéficieront de cette nouvelle version, ce qui permettra aux utilisateurs d'employer le système de chiffrement sur ces ordinateurs.
