Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
nationale

*Direction centrale de la sécurité
des systèmes d'information*

Paris, le 9 août 2005
N° 2328 /SGDN/DCSSI

Recommandations de sécurité pour l'application SKYPE

1. Présentation de l'application de téléphonie sur l'internet SKYPE

L'application SKYPE est une application de téléphonie sur l'internet (téléchargeable gratuitement http://www.skype.com) qui fonctionne sur plusieurs types de micro-ordinateurs (PC Windows, MacOSX, Linux sur X86, IPAQ et certains PDA sous WIFI). Pour accéder au service gratuit de téléphonie, il faut s'enregistrer dans un annuaire protégé par un mot de passe. Des services de transferts de fichiers à bas débit et de messagerie instantanée font partie du service de base gratuit. L'accès depuis (SkypeIN) et vers (SkypeOut) le réseau téléphonique classique se fait moyennant un abonnement prépayé en ligne qui constitue le seul revenu de l'entreprise.

L'application SKYPE contourne les protections périmétriques (pare-feu) et n'obéit pas aux normes de la voix sur IP (elle n'utilise ni SIP ni H323, les normes de signalisation). Elle est dangereuse comme toute application qui fait sortir des données chiffrées d'un périmètre protégé sans qu'il soit possible d'exercer un contrôle par inspection au départ ou par inspection après déchiffrement à la sortie (car l'utilisateur ou l'administrateur ne dispose pas des clés de chiffrement). De plus le poste de travail peut devenir nœud de transit à l'insu de son utilisateur : l'utilisateur l'accepte en téléchargeant le logiciel (voir la licence utilisateur *End User License Agreement*). Il est clair que le service peut être intecepté en particulier depuis l'étranger, devenant ainsi un outil d'intelligence économique voire pour des services d'investigation étrangers.

2. Recommandations

Pour ces raisons, SKYPE ne doit jamais être placé sur un poste relié à un intranet sensible ouvert sur l'internet ; il est recommandé de le placer sur une machine sacrifiée, sur un réseau sacrifié isolé hors intranet (bibliothèque, services communs, etc.), avec une connexion internet spécifique.

Dans ce cas il est nécessaire d'observer absolument les règles suivantes :

- nettoyer l'ordinateur à intervalles réguliers en reconstruisant toute la configuration logicielle,
- arrêter l'ordinateur en l'absence de besoins, suivant le mode d'utilisation : soit après chaque appel, soit à la fin de la période où les appels sont acceptés, pour limiter les interactions en l'absence d'usagers présents,
- placer l'ordinateur derrière un garde barrière spécifiquement configuré et dont les journaux sont exploités régulièrement (hebdomadairement) pour éviter qu'il ne devienne un nœud de transit,
- authentifier de manière forte chaque utilisateur sur un compte différent,
- expliciter et contrôler l'interdiction de la présence de SKYPE sur les micro-ordinateurs des réseaux intranet reliés à l'internet.