

Protection contre les logiciels malveillants

REG 1

Un outil de protection contre les logiciels malveillants doit être installé sur tous les serveurs, les ordinateurs fixes et les terminaux mobiles.

REG 3

Il faut installer et mettre à jour régulièrement les logiciels de détection et de réparation pour analyser les ordinateurs et les supports. Ces opérations doivent inclure notamment l'analyse des fichiers reçus ou téléchargés, ainsi que celles des pièces jointes, attachées aux courriers électroniques, et l'analyse des pages web pour s'assurer de l'absence de logiciels malveillants.

REG 5

Les courriers électroniques suspects, avec ou sans pièces jointes, ne doivent pas être ouverts.

REG 7

Des filtres de contenus doivent être installés pour empêcher l'utilisation de sites web malveillants ou suspectés en tant que tels.

REG 9

Les utilisateurs doivent veiller à se protéger de l'introduction de logiciels malveillants qui peuvent contourner les mesures de protection habituelles, lors des opérations de maintenance et de dépannage.

REG 2

L'utilisateur, ou à défaut, l'administrateur doit prendre toutes les mesures et effectuer les paramétrages nécessaires pour la mise à jour de l'outil (cf. REG 1) en vue de son fonctionnement efficient.

REG 4

En cas de détection de logiciels malveillants, une alerte doit être diffusée dans l'ensemble de l'entité.

REG 6

Des anti-spams doivent être installés sur les serveurs de messagerie. Des listes noires en temps réel doivent être utilisées pour bloquer les spams.

REG 8

Etablir des procédures de continuité d'activités de l'organisme, après une attaque par logiciels malveillants, comprenant les sauvegardes de tous les logiciels et données nécessaires ainsi que les dispositions de sauvegarde.

REG 10

Il faut s'assurer que les bulletins d'alerte concernant les logiciels malveillants sont exacts et informatifs, et proviennent de sources qualifiées pour distinguer les canulars des menaces réelles. Tous les utilisateurs doivent être informés de l'existence de canulars et de la démarche à suivre
