Directive sur la cybersécurité : TI 8.05	Diffusée : 04/2019
Chapitre : Sécurité physique et sécurité des systèmes	Dernière révision : 06/2024
Objet : **CONTRÔLES contre les VIRUS, les VERS et les LOGICIELS MALVEILLANTS**	

1 DIRECTIVE

1.01 Le réseau du GNB sera protégé par un pare-feu contre les intrusions non désirées de l'Internet public et contre les communications non autorisées depuis l'intérieur du pare-feu vers l'Internet public.

1.02 Tous les systèmes informatiques seront protégés des infections par logiciel malveillant grâce à l'antivirus choisi par le GNB.

1.03 Tous les systèmes doivent être régulièrement mis à jour avec la plus récente protection antivirus en fonction du calendrier de mise à jour du fournisseur de l'antivirus.

1.04 Tous les programmes, fichiers et documents introduits dans un système informatique d'une source externe doivent être scannés par l'antivirus avant d'être utilisés pour détecter toute infection par logiciel malveillant.

1.05 Les utilisateurs du réseau du GNB doivent supprimer immédiatement tout courriel provenant d'un expéditeur non reconnu.

1.06 Toutes les pièces jointes de courriel doivent être scannées par l'antivirus avant d'être consultées ou exécutées afin de détecter toute infection par logiciel malveillant.

2 OBJET

2.01 La présente directive vise à réduire au minimum les risques auxquels sont exposés les systèmes informatiques du GNB en raison d'infections par logiciel malveillant.

3 PORTÉE

3.01 La présente directive s'applique à tous les employés.

4 RESPONSABILITÉ

4.01 Tous les employés sont responsables de surveiller les symptômes d'infection par logiciel malveillant sur les systèmes informatiques qu'ils utilisent.

5 DÉFINITIONS

5.01 Les termes suivants décrivent différents types de logiciels malveillants :

5.02 Un **logiciel de publicité** est un logiciel qui surveille la navigation sur le Web d'une personne et qui l'interrompt en affichant des publicités dans des fenêtres contextuelles.

5.03 Une **trappe** est un logiciel installé clandestinement sur un système informatique et qui permet à un utilisateur malveillant d'obtenir un accès non autorisé au système à des fins illicites.

5.04 Un **appeleur automatique** est un programme qui profite de la capacité de composition d'un ordinateur par l'intermédiaire d'un modem et d'une ligne téléphonique. Il peut remplacer un numéro de téléphone stocké dans l'accès par ligne commutée du modem par un numéro de téléphone interurbain ou un numéro payé à l'appel afin de faire grimper la facture de téléphone. Il peut aussi composer de nuit pour envoyer les données d'un enregistreur de frappe ou d'autres renseignements à un pirate informatique.

5.05 Un **enregistreur de frappe** est un logiciel qui copie dans un fichier les éléments saisis au clavier par un utilisateur. Souvent, ce logiciel est programmé pour être activé seulement lorsque l'utilisateur est connecté sur un type précis de site Web, comme celui d'une institution financière, pour saisir les numéros de compte et les codes d'accès avant qu'ils soient cryptés et transmis à l'institution financière. Le fichier peut être transmis ultérieurement au pirate qui a créé le logiciel d'enregistreur de frappe.

5.06 Un **logiciel malveillant** est un programme conçu à toute fin contraire aux intérêts de la personne qui l'exécute.

5.07 Un **pourriel** est un courriel indésirable envoyé en grand volume. Il impose habituellement une charge injustifiée ou indésirable sur les systèmes de courriel, contient souvent d'autres types de logiciels malveillants, et comprend des renseignements frauduleux.

5.08 Un **logiciel espion** est un logiciel qui recueille clandestinement des renseignements permettant d'identifier une personne ou une organisation, comme le nom, les identifiants de connexion, les numéros de carte de crédit, les mots de passe, les adresses électroniques, la liste de contacts et les numéros de téléphone. Il enregistrera ces renseignements ou les enverra à

des tiers lorsque la personne sera connectée à Internet. Un autre exemple de logiciel espion est un programme qui parcourt le modem d'une personne pour modifier les numéros de composition automatique.

5.09 Un **cheval de Troie** est un logiciel qui semble utile, mais qui causera intentionnellement des dommages une fois qu'il sera installé ou exécuté sur un ordinateur. Certains chevaux de Troie ne visent pas à causer des dommages directs, mais plutôt à installer une trappe sur l'ordinateur.

5.10 Un **virus** est un programme malveillant qui s'auto-réplique et qui se propage en joignant des copies de lui-même, parfois modifiées, à d'autres codes ou documents exécutables, infectant ainsi les codes ou les documents en question. Le virus se propage lorsque les fichiers infectés sont copiés dans des systèmes non infectés par l'intermédiaire de supports amovibles ou de pièces jointes de courriel, puis exécutés et ouverts dans ces systèmes.

5.11 Un **wabbit** est un type de logiciel malveillant qui cause des dommages à un système informatique en se répliquant rapidement; il peut causer des effets secondaires malveillants visant précisément une attaque par déni de service.

5.12 Un **ver** est un logiciel malveillant qui se propage en profitant des fonctionnalités de transport de fichier ou de réseau d'un système informatique, qui lui permettent de se propager par lui-même.

6 DIRECTIVES CONNEXES

DCS TI 10.02 – Protection pare-feu

DCS TI 10.03 – Accès à distance