Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°49 du 18 décembre 2009

PARTIE PERMANENTE
Administration Centrale

Texte n°4

DIRECTIVE N° 10/DEF/DGSIC

sur la prévention contre les codes malveillants.

Du *5 novembre 2009*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 10/DEF/DGSIC sur la prévention contre les codes malveillants.

Du 5 novembre 2009

NOR D E F E 0 9 5 2 7 9 7 X

Pièce(s) Jointe(s) :

Deux annexes.

Classement dans l'édition méthodique : BOEM 160.1

Référence de publication : BOC N°49 du 18 décembre 2009, texte 4.

SOMMAIRE

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. Présentation.

1.2. Niveaux de préconisation.

1.3. Modalités d'application.

1.4. Gestion des dérogations pour les projets.

2. CADRE DOCUMENTAIRE.

2.1. Documents applicables.

2.2. Normes et standards applicables.

3. DOMAINE COUVERT ET EMPLOI.

3.1. Service attendus du système.

3.1.1. Protéger le patrimoine applicatif et informationnel du ministère de la défense contre les codes malveillants.

3.1.2. Réduire les coûts et la complexité des solutions de prévention contre les codes malveillants.

3.1.3. Établir une analyse de risque du patrimoine applicatif.

3.1.4. Fournir un système automatique et immédiat de notification en cas d'infection virale.

3.1.5. Disposer de solutions complémentaires de prévention contre les codes malveillants.

3.1.6. Disposer d'équipes d'administration, d'exploitation et de supervision et de spécialistes contre les codes malveillants.

3.1.7. Mettre en œuvre des procédures appropriées de sensibilisation des utilisateurs.

3.1.8. Élaborer des plans appropriés de continuité de l'activité après une attaque par des codes malveillants.

3.1.9. Permettre l'accès aux bases de connaissance des éditeurs de prévention contre les codes malveillants et des organismes certifiés.

3.2. Périmètre et limites.

3.2.1. Périmètre.

3.2.2. Limites.

3.3. Interopérabilité et interfaçage.

3.3.1. Avec les systèmes d'exploitation.

3.3.2. Avec les autres éditeurs de prévention contre les codes malveillants et les standards ouverts.

4. LES RÈGLES.

4.1. Règles techniques.

4.1.1. Administration.

4.1.2. Principe d’installation des mises à jour.

4.1.3. Formation, support.

4.2. Règles organisationnelles.

5. GLOSSAIRE ET ACRONYMES.

ANNEXE(S)

ANNEXE I. CONCEPT DE DÉFENSE EN PROFONDEUR APPLIQUÉ À LA PREVENTION CONTRE LES CODES MALVEILLANTS.

ANNEXE II. DÉFINITION DES CODES MALVEILLANTS.

Nota 1 : les mots marqués d'un astérisque figurent dans le glossaire.

Nota 2 : les mots entre crochets [] figurent dans le cadre documentaire.

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

Les codes malveillants représentent une menace réelle au sein du système d'information du ministère de la défense (SI*). Le résultat d'une infection informatique peut diminuer la productivité, propager à d'autres supports l'infection informatique, causer la perte ou l'altération des données, rendre inopérants des systèmes ou des ordinateurs, porter atteinte à l'image du ministère, à la conduite des opérations, voire à la sûreté nationale ou bien révéler des informations confidentielles à des personnes non autorisées.

La lutte contre les codes malveillants repose sur deux type de processus différents. La prévention contre les codes malveillants (PCM) est le processus amont de cette lutte, et fait l'objet de cette directive. L'effet majeur recherché de la PCM du ministère est de minimiser les impacts des codes malveillants, dans le cadre d'une

analyse de risques globale (1) des SI*. Ce processus est prolongé par des processus opérationnels, dans le cadre plus général de la lutte informatique défensive (LID), qui ne sont pas traités dans cette directive (2).

1.1. **Présentation.**

Cette directive définit les règles du ministère de la défense en matière de PCM. Elle en précise les principes, les objectifs et les moyens généraux pour y parvenir.

Cette directive s'inscrit dans les missions de la direction générale des systèmes d'information et de communication (DGSIC) aux termes du décret n° 2006-497 du 2 mai 2006 portant création de la DGSIC et fixant l'organisation des systèmes d'information et de communication du ministère de la défense.

Elle s'inspire du cadre commun d'interopérabilité [CCI], du projet de [RGI] prévu par l'ordonnance n° 2005-1516 [ORD] relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives. Elle décline la directive n° 1/DEF/DGSIC sur les logiciels [DGSIC001] du ministère de la défense.

Le processus de PCM est ministériel et unique. Chaque projet ou programme du ministère devra en être client (3). Ce processus se décline en différents SI de PCM, dans le cadre de la défense en profondeur, dont le nombre est à minimiser dans un souci d'efficience.

1.2. **Niveaux de préconisation.**

Les règles définies dans ce document ont différents niveaux de préconisation et sont conformes au [RGI] et à la [RFC 2119].

- obligatoire : ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive ;

- recommandé : ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente ;

- déconseillé : ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé ;

- interdit : ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue de la directive.

1.3. **Modalités d'application.**

Ces règles définissent la cible à atteindre et sont applicables à tout nouveau projet mis en œuvre sur le périmètre du SI*. Les politiques de PCM des organismes relevant du ministère de la défense existants à la date de publication de la présente directive seront mises en conformité avec celle-ci dans un délai de 3 ans à compter de cette date.

Une autorité qualifiée (AQ) ne peut poser des conditions complémentaires dans le domaine de la PCM que dans la mesure où celles-ci sont plus protectrices pour le SI que la présente directive.

Cette directive est précisée par une directive technique, des référentiels techniques et méthodologiques au sein de chaque service ou direction. Elle est référencée dans les PSI* des organismes. Les directions et services transposent les exigences de la présente directive dans les cahiers des charges des marchés publics impactés par la politique de PCM.

Les autorités qualifiées, les commissions « métier » (CSIOC, CSIAG et CIST) et les commissions ministérielles spécialisées veillent au respect de l'application de cette directive et à sa prise en compte dans les projets et programmes.

Les formes du contrôle d'application de cette directive tiennent compte :

- des contraintes de calendrier sur les projets et programmes ;

- du code des marchés publics.

1.4. **Gestion des dérogations pour les projets.**

Les dérogations aux règles recommandées ou déconseillées font l'objet d'une saisine de la DGSIC par l'organisme d'appartenance de la maîtrise d'ouvrage concernée. Les cas structurants sont débattus en commission ministérielle spécialisée des SIC (CMSSI, CMTSIC). Les questions d'interopérabilité opérationnelle interalliée sont traitées de façon prioritaire.

2. CADRE DOCUMENTAIRE.

2.1. **Documents applicables.**

Ordonnance n° 2005-1516 du 8 décembre 2005 [ORD].

Instruction n° 4418/DEF/SEC/DIR/SIC du 25 septembre 2000 relative à la mise en œuvre de la sécurité des systèmes d'information au sein du ministère de la défense [IM4418].

Instruction n° 133/DEF/SEC/DIR/SIC du 18 mars 2002 relative à la politique de sécurité des systèmes d'information du ministère de la défense (PSSI) [IM133].

Instruction n° 8192/DEF/SEC/DIR/SIC du 30 juin 2003 relative aux modalités d'accès, de raccordement et d'utilisation des réseaux externes au ministère de la défense [IM8192].

Politique de référencement intersectoriel de sécurité [PRIS].

Recommandations nationales du cadre commun d'interopérabilité [CCI].

Référentiel général d'interopérabilité version 1.0 du 12 mai 2009 [RGI].

Référentiel général de sécurité version provisoire 0.98 du 18 décembre 2008 [RGS].

2.2. **Normes et standards applicables.**

ISO/CEI 27001 : 2005 : Technologies de l'information - Techniques de sécurité - Systèmes de gestion de la sécurité de l'information - Exigences.

ISO/CEI 27002 : 2005 : Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information.

ISO/CEI 27005 : 2008 : Technologies de l'information - Techniques de sécurité - Gestion du risque en sécurité de l'information.

3. DOMAINE COUVERT ET EMPLOI.

Ce paragraphe rappelle les grands principes de la SSI applicables à la PCM, de nature technique ou organisationnelle.

3.1. **Service attendus du système.**

Le présent chapitre décrit les fonctionnalités que doit fournir un système de PCM.

3.1.1. ***Protéger le patrimoine applicatif et informationnel du ministère de la défense contre les codes malveillants.***

Les logiciels et les moyens de traitement de l'information sont vulnérables à l'introduction de codes malveillants comme les virus informatiques (4), les vers, les chevaux de Troie et les bombes logiques. Dès lors, il peut en résulter une perte ou une altération des données, voire un dysfonctionnement du système qui en assure le traitement. Le processus de PCM doit contribuer en tout temps et en tous lieux, à réduire les vulnérabilités résultantes sur les données et les logiciels détenus par le ministère de la défense et à contenir la propagation des effets induits par les codes malveillants. Il doit également permettre de prévenir, détecter, isoler et/ou supprimer les codes malveillants et contrôler l'exécution des codes mobiles (ou autoreproducteurs). Les utilisateurs des SI* doivent être sensibilisés aux dangers de ces codes.

3.1.2. ***Réduire les coûts et la complexité des solutions de prévention contre les codes malveillants.***

Le processus de PCM doit, via la standardisation, déployer et maintenir des solutions de PCM cohérentes et homogènes afin de minimiser le MCO* et les pertes de capacité générées en cas d'infection par des codes malveillants. Pour cela, il doit permettre la distribution et la mise à jour automatique de logiciels de prévention contre les codes malveillants sur la totalité des postes terminaux connectés, en permanence ou occasionnellement, au SI*.

3.1.3. ***Établir une analyse de risque du patrimoine applicatif.***

La protection des informations du ministère de la défense doit être envisagée de manière globale en incluant tous les éléments du SI* potentiellement vulnérables (données, applications, serveurs, postes terminaux, éléments du réseaux ...). Une analyse de risque doit être menée pour chacun des SI* afin d'identifier et de hiérarchiser les principaux risques selon leurs impacts et leurs probabilités d'occurrence. Ces risques devront être acceptés, transférés, éliminés ou réduits par des solutions techniques ou organisationnelles selon les contraintes budgétaires, structurelles ou opérationnelles (5).

3.1.4. ***Fournir un système automatique et immédiat de notification en cas d'infection virale.***

Les équipes de spécialistes de PCM, les responsables fonctionnels de la chaîne SSI et les utilisateurs doivent pouvoir être avertis, automatiquement et sans délais, de la propagation d'un code malveillant au travers du SI*.

3.1.5. ***Disposer de solutions complémentaires de prévention contre les codes malveillants.***

Afin d'appliquer le principe de la défense en profondeur à la PCM, les solutions techniques de PCM doivent être installées de telle manière qu'elles permettent d'analyser, de manière séquentielle, par des technologies différentes et complémentaires, les flux de données qui traversent le SI*, en cohérence avec les performances attendues.

Ainsi, un fichier est analysé consécutivement sur le serveur de fichiers sur lequel il est stocké puis sur le poste terminal depuis lequel il est consulté. Dans le cas d'un courriel, il est successivement analysé par la solution de PCM déployée sur le serveur d'envoi, puis par la solution de PCM de la passerelle de messagerie quand il entre ou sort du SI* et finalement, par la solution de PCM sur le client de messagerie.

Tout flux traversant plusieurs zones techniques* devra être analysé en innocuité au minimum par deux solutions de PCM différentes.

3.1.6. ***Disposer d'équipes d'administration, d'exploitation et de supervision et de spécialistes contre les codes malveillants.***

Il est nécessaire d'entretenir une communication régulière entre tous les acteurs concourant à la PCM. Ce dialogue permanent doit exister à travers les différents organismes en charge de la PCM au sein du ministère de la défense.

Les membres de l'OPVAR* (6), le CALID*, la cellule d'expertise (CELEX*) et les représentants de chaque organisme en charge de la PCM constituent les équipes prioritaires de spécialistes du ministère de la défense en charge de la PCM.

Les spécialistes concourant à la PCM échangent dans une certaine mesure avec les experts hors du ministère de la défense (éditeurs, universitaires, industriels).

3.1.7. ***Mettre en œuvre des procédures appropriées de sensibilisation des utilisateurs.***

Il est de la plus haute importance de sensibiliser toutes les catégories de personnes du ministère aux enjeux et aux risques SSI et particulièrement à ceux de la PCM. L'entretien des compétences et la sensibilisation du personnel devront être renforcés par la mise en place de séquences de PCM dans les scénarios d'entraînement à la LID*.

3.1.8. ***Élaborer des plans appropriés de continuité de l'activité après une attaque par des codes malveillants.***

Tous les codes malveillants n'ont pas le même caractère critique, tous les postes terminaux n'ont pas le même impact sur la viabilité du système d'information du ministère. Il convient donc de définir des degrés selon les niveaux de menace et d'y adapter les mesures de sécurité adéquates, en particulier dans les plans de continuité et de reprise d'activité.

3.1.9. ***Permettre l'accès aux bases de connaissance des éditeurs de prévention contre les codes malveillants et des organismes certifiés.***

Les différents aspects de la PCM sont consultables et tenus à jour depuis l'intranet sensible du ministère de la défense. L'état de la menace virale y est prioritairement identifiable.

3.2. **Périmètre et limites.**

3.2.1. ***Périmètre.***

La directive est applicable à l'ensemble du SI* du ministère de la défense, dans toutes ses composantes, y compris les moyens de télécommunications. Elle concerne tous les systèmes (7) quel que soit leur niveau de classification ou leur localisation géographique.

Tout système d'information du ministère de la défense, tout réseau et tout poste de travail ou terminal relèvent du périmètre d'application de la présente directive.

Tous les codes malveillants (virus, vers, logiciels espion « *spyware* » etc.) sont dans le périmètre de la PCM.

3.2.2. ***Limites.***

Les sujets connexes comme les courriers électroniques non sollicités (spams) ou les logiciels espions qui concourent aux mêmes risques que les codes malveillants ne sont que partiellement pris en compte dans ce document.

La SSI* met en œuvre des moyens défensifs spécifiques tels que les systèmes de détection d'intrusion, les systèmes correctifs, d'authentification réseau ou de pare-feu précisés dans une directive ministérielle relative à la protection des postes de travail.

Les aspects de reprise après incidents et de correction des vulnérabilités les plus pertinentes pour la PCM ne sont que très légèrement abordés.

3.3. **Interopérabilité et interfaçage.**

L'interopérabilité traduit, dans le domaine des SIC, la capacité à échanger des informations et à créer les conditions d'un véritable travail en commun dans le respect des conditions de sécurité appropriées (8).

Les règles énoncées dans la présente directive permettent d'envisager une interopérabilité des solutions proposées par les éditeurs de PCM entre elles, ainsi qu'avec les systèmes existants et le monde extérieur (interministériel). L'interopérabilité du système de PCM doit permettre de converger progressivement vers une solution de PCM homogène qui réponde au principe d'administration centralisée pour les actions de gestion et de maintenance. Les bénéfices attendus d'une telle fonction sont une contribution à la réduction du coût global de possession d'une telle solution.

En ce qui concerne les nouveaux systèmes, l'interopérabilité n'est jamais acquise. Elle doit donc être construite, vérifiée et contrôlée obligatoirement lors des étapes contractuelles de pré-test (maquette), de recette (vérification d'aptitude : VA) et de de contrôle (vérification de service régulier : VSR).

3.3.1. ***Avec les systèmes d'exploitation.***

Les solutions de PCM déployées au sein du ministère de la défense devront pouvoir s'interfacer avec l'ensemble des systèmes d'exploitation en production selon les solutions techniques existantes.

3.3.2. ***Avec les autres éditeurs de prévention contre les codes malveillants et les standards ouverts.***

Les solutions mises en œuvre doivent disposer d'une capacité de surveillance centralisée et consolidée de l'activité virale à travers des protocoles documentés.

4. LES RÈGLES.

La directive est déclinée sous 2 angles : technique (RT) et organisationnel (RO). Les règles sont numérotées séquentiellement par catégorie.

4.1. **Règles techniques.**

4.1.1. ***Administration.***

RT 1 : il est obligatoire que tous les postes terminaux, les serveurs et les équipements actifs (9) disposent d'une solution de protection antivirale correctement installée, configurée, activée et disposant de la dernière version valide de mécanismes de détection avant de pouvoir être exploités sur le SI*.

RT 2 : il est recommandé que chaque solution de PCM bénéficie du certificat de sécurité du premier niveau (CSPN*) pour les fonctionnalités de lutte contre les virus informatiques.

RT 3 : il est recommandé que le processus de PCM repose sur une architecture centralisée et redondée, répartie au minimum sur deux centres de production physiquement distincts.

RT 4 : il est obligatoire de disposer d'un outil d'administration centralisé qui permette de télé-administrer les mises à jour des signatures et des moteurs de tous les postes terminaux, serveurs et équipements actifs (9) en réseau. Cet outil doit permettre d'effectuer une consolidation à l'échelon central des notifications d'infections virales.

RT 5 : il est recommandé de disposer d'un outil d'administration centralisé qui permette de déployer automatiquement la solution de PCM sur tous les postes terminaux, les serveurs et les équipements actifs (9).

RT 6 : il est obligatoire de disposer de moteurs de détection de virus en temps réel, de technologies (10) et d'éditeurs de solution de PCM différents entre les postes terminaux et les équipements d'application* ou de connexion*.

RT 7 : il est recommandé que les sas de sécurité (sous réserve de la nécessité d'emploi (11)) soient protégées par une solution de PCM différente de celle utilisée sur les postes de travail.

RT 8 : il est obligatoire que les solutions de PCM disposent de la capacité de nettoyer ou mettre en quarantaine des fichiers infectés, et d'éradiquer les codes malveillants actifs.

RT 9 : il est recommandé que tous les fichiers exécutables et fichiers systèmes puissent être protégés par des mécanismes de contrôle d'intégrité.

RT 10 : s'agissant d'un courriel, il est interdit de mettre en place un système de PCM qui, en l'absence de code malveillant modifierait, lors de son analyse en innocuité, le corps ou l'objet du message (12).

RT 11 : il est recommandé de prendre en compte la mise en œuvre des services additionnels (13) de protection de tous les postes terminaux, les serveurs et les équipements actifs (9).

RT 12 : il est recommandé de prendre en compte les mécanismes de type NAC* pour l'authentification et pour le contrôle de conformité afin de s'assurer que la posture de protection d'un poste terminal de type 2 (14) est conforme à la PSI* (15) au moment de sa demande de connexion au SI*.

4.1.2. ***Principe d'installation des mises à jour.***

RT 13 : il est obligatoire que le système de PCM dispose d'une connexion permanente sécurisée et dédiée avec le prestataire de service de la solution PCM afin de garantir le maintien à jour des mécanismes de détection implémentés dans les ressources du SI*.

RT 14 : il est obligatoire que cette connexion soit physiquement déconnectée du SI* du ministère.

RT 15 : il est obligatoire pour les équipements connectés en permanence, que les mises à jour des bases de signature soient systématiquement installées dans les huit heures suivant leur publication par l'éditeur de la solution de PCM.

RT 16 : il est recommandé que les mises à jour des moteurs de détection soient installées dans les huit heures suivant leur publication par l'éditeur de la solution de PCM.

RT 17 : il est recommandé que les passerelles applicatives, d'interconnexion et les serveurs ne fassent pas l'objet de mises à jour simultanées avec les postes terminaux.

Les mécanismes de mise à jour peuvent varier : scripts au démarrage de la machine, programmation quotidienne, envoi (*push*) ou téléchargement (*pull*). Le point important à retenir ici est qu'il faut s'assurer que la mise à jour a bien été réalisée dans les 8 heures et qu'elle est opérationnelle.

RT 18 : il est recommandé que les mécanismes de mises à jour de PCM soient incrémentiels et quotidiens.

4.1.3. ***Formation, support.***

RT 19 : il est obligatoire que l'ensemble du personnel du ministère de la défense ayant accès au SI* ait reçu une sensibilisation à la PCM conforme à la PSI*.

RT 20 : il est obligatoire que les administrateurs du système reçoivent en plus d'une formation initiale à la SSI*, une formation spécifique à la PCM. Les administrateurs mettant en œuvre des solutions de sécurité doivent recevoir une formation adéquate sur les produits déployés et leurs technologies. Cette formation doit être permanente tout au long du cycle de vie des solutions déployées.

RT 21 : il est obligatoire de souscrire au profit du CALID un support technique de l'ensemble des solutions de PCM utilisées au sein du ministère.

4.2. **Règles organisationnelles.**

RO 1 : il est obligatoire d'adopter une organisation de PCM conforme aux concepts de la défense en profondeur (cf. annexe I).

RO 2 : il est obligatoire qu'un poste terminal ou un équipement contaminé par un code malveillant soit immédiatement déconnecté ou mis en quarantaine du SI* du ministère.

RO 3 : il est recommandé que tous les types de fichiers échangés fassent l'objet d'un contrôle antiviral.

RO 4 : il est recommandé que la protection de PCM soit active en toutes circonstances.

RO 5 : il est obligatoire de disposer au sein de chaque organisme de plans d'urgence qui couvrent les principaux types de menaces.

RO 6 : il est obligatoire de rendre compte ou d'informer le cas échéant, selon les procédures décrites, les représentants de l'autorité qualifiée, le FSSI*, les parties prenantes à la PCM (le CPCO/J6/LI*, le CALID*, l'OPVAR*, la CELEX*) et d'informer les entités extérieures au ministère concourant à la PCM (CERTA*), dès le déclenchement d'un plan d'urgence consécutif à une attaque virale d'envergure.

RO 7 : dans le cadre de l'analyse de risques globale préliminaire à la conception d'un SI*, il est obligatoire de mener une analyse des risques en distinguant les menaces « classiques », pour lesquelles les outils commerciaux apporteront des solutions intéressantes, des menaces étatiques ou terroristes pour lesquelles les mesures de sécurité ne pourront pas reposer sur ces seuls outils. Parallèlement, une analyse d'impact devra déterminer les conséquences directes et indirectes d'une attaque par des codes malveillants sur le SI*.

RO 8 : il est obligatoire que les risques identifiés et non couverts soient pris en compte par les AQ dans l'acceptation des risques encourus (16).

RO 9 : il est obligatoire que des mesures organisationnelles complètent les moyens techniques des solutions de PCM.

RO 10 : il est obligatoire de préciser les conditions dans lesquelles le chiffrement des données est obligatoire ou recommandé. Ces conditions doivent intégrer le risque généré par le fait qu'un document chiffré ne permet pas d'effectuer une analyse en innocuité. Elles doivent être intégrées dans la PSI de l'organisme.

RO 11 : il est recommandé d'utiliser un système de signature des courriels à base de certificats électroniques. Les fonctions de signature électronique permettent de s'assurer de l'authentification de l'émetteur et de l'imputabilité du message tout en autorisant une analyse en innocuité.

RO 12 : il est obligatoire que l'efficacité de la solution de PCM soit mesurée. Cette mesure est centralisée. L'architecture mise en place doit permettre, en minimisant les flux, de centraliser à chaque niveau de commandement l'ensemble des données de PCM relevant de son périmètre.

RO 13 : il est recommandé de tracer les actions de PCM réalisées par les administrateurs.

RO 14 : il est obligatoire de prendre en compte les solutions de PCM dans la politique de gestion des correctifs et le MCS.

5. GLOSSAIRE ET ACRONYMES.

AQ : autorité qualifiée.

CALID : centre d'analyse de lutte informatique défensive.

CELEX : cellule d'expertise.

CERTA : centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques, rattaché à l'ANSSI.

CMSSI : commission ministérielle de la sécurité des systèmes d'information.

CMTSIC : commission ministérielle technique des systèmes d'information et de communication .

Code malveillant : programme simple ou autoreproducteur s'installant dans un système d'information, à l'insu du ou des utilisateurs, en vue de porter atteinte à la confidentialité, l'intégrité ou la disponibilité de ce système (cette définition évoque des programmes, indépendamment de toute plateforme particulière).

CSPN : certification de sécurité de premier niveau. Cette certification s'appuie sur des critères, une méthodologie et un processus élaborés par la ANSSI.

CPCO/J6/LI : centre de préparation et de conduite opérationnelle/bureau J6/lutte informatique.

Équipement d'applications : plateforme matérielle supportant un système d'exploitation et fournissant des services ou des applications à toutes les composantes du SI (serveur).

Équipement actif de réseau : équipement matériel de niveau 3 selon l'ISO.

FSSI : fonctionnaire de la sécurité des systèmes d'information.

IGI : instruction générale interministérielle.

PCM : prévention contre les codes malveillants.

LID : lutte informatique défensive.

MCO : maintien en conditions opérationnelles.

NAC : n*etwork access control* (contrôleur d 'accès au réseau).

OPVAR : organisation permanente veille alerte réponse.

PSI : politique de sécurité informatique.

SI : système d'information du ministère de la défense.

SIC : système d'information et de communication.

SMSI : système de management de la sécurité de l'information.

SSI : sécurité des systèmes d'information.

Zones techniques : couches de différents niveaux de criticité (barrières, coupures, niveaux de protection différents).

Pour le ministre de la défense et par délégation :

L'amiral,
directeur général des systèmes d'information et de communication,

Christian PÉNILLARD.

(1) En particulier, la confidentialité ou la disponibilité des SI du ministère doivent être prises en compte dans les critères de choix d'implémentation.

(2) Toutefois, certains aspects opérationnels sont parfois abordés.

(3) Une directive technique précisera les exigences demandées aux clients (protocoles, ports, ...).

(4) Cf Annexe II.

(5) Le cas des systèmes embarqués et/ou temps réel illustre concrètement l'éventualité de prise de risque pour une contrainte opérationnelle. Néanmoins, ce cas ne dispense pas d'un processus réfléchi de prise de décision incluant a minima une analyse de risques.

(6) Cf : Instruction ministérielle n° 2001/DEF/DGSIC du 20 novembre 2007.

(7) Les systèmes d'armes temps réel doivent faire l'objet d'une analyse de risques adaptée.

(8) Définition adaptée de celle du PIA 06.301.

(9) Pouvant techniquement supporter une solution de PCM.

(10) Reconnaissance de signature, comportemental, heuristique ou bayésien...

(11) Cas des OPEX, par exemple.

(12) Une telle modification rendrait inopérant tout système de signature des courriels.

(13) Tels que les pare-feu personnel, antispam, antispyware etc.

(14) Selon la typologie de la directive DGSIC n° 8 définissant les règles à appliquer au système de postes terminaux.

(15) Principalement en matière de mise à jour des correctifs de sécurité, des bases de signature PCM et des moteurs de détection antivirus.

(16) exemple : le choix de ne plus mettre à jour des composants d'un SIOC afin de conserver leur homologation.

ANNEXE I.

CONCEPT DE DÉFENSE EN PROFONDEUR APPLIQUÉ À LA PREVENTION CONTRE LES CODES MALVEILLANTS.

La défense en profondeur, terme emprunté à une technique militaire destinée à retarder l'ennemi, consiste à exploiter plusieurs techniques de sécurité afin de réduire le risque lorsqu'un composant particulier de sécurité est compromis ou défaillant.

Typiquement, des logiciels antivirus peuvent être présents à plusieurs niveaux pour renforcer la sécurité et pallier le non-fonctionnement d'un antivirus à un moment donné : les pare-feu, les serveurs et les postes clients. L'organisation des SI* et le rôle de l'utilisateur constituent également un des composants de la défense en profondeur.

Le premier niveau de défense se situe aux frontières du SI* ministériel. La première couche de défense consiste en un moyen de protection sur :

- les passerelles de connexion : passerelles SMTP, HTTP(S)-FTP (*Firewall*, *Proxy*...) et leurs composants ;

- composants itinérants navigateur, disques durs et client de messagerie sur les terminaux mobiles ;

- médias amovibles : disque dur externe, clé USB etc.

La seconde couche de défense est assurée par une protection sur les serveurs, en particulier et au minimum les serveurs de fichiers et les serveurs de messagerie.

La troisième couche de défense est assurée sur les postes terminaux de l'utilisateur final à l'aide de l'antivirus couplé avec le navigateur et le client de messagerie.

Les solutions techniques déployées sur ces trois couches sont différentes.

ANNEXE II.

DÉFINITION DES CODES MALVEILLANTS.

Code malveillant, logiciel malveillant *(Malicious software, malware)* : tout programme développé dans le but de nuire à un SIC ou au moyen d'un SIC.

Remarques : les virus ou les vers sont deux types de codes malveillants connus.

1. LES PROGRAMMES SIMPLES.

Le mode propre de ces programmes comme leur nom l'indique, est de simplement s'installer dans le système. L'installation se fait en général :

- en mode furtif : l'utilisateur ne doit pas se rendre compte qu'un tel programme est présent dans son système ;

- en mode résident : le programme est actif en mémoire afin de pouvoir agir en permanence dès que l'ordinateur est allumé ;

- en mode persistant : en cas d'effacement ou de désinstallation, le programme est capable par différentes techniques de se réinstaller dans la machine indépendamment.

Les programmes simples infectants appartiennent essentiellement à trois classes :

- la bombe logique est un logiciel malveillant conçu pour causer des dommages à un système informatique et qui est déclenché lorsque certaines conditions sont réunies (*Logic Bomb* en anglais).

Remarque : certains virus contiennent une fonction de bombe logique : déclenchement à date fixe, déclen−chement quand une adresse réticulaire (URL) particulière est renseignée dans le navigateur, etc.

- le cheval de Troie (1) est un logiciel apparemment inoffensif, installé ou téléchargé. Il dissimule un programme malveillant qui peut par exemple permettre la collecte frauduleuse, la falsification ou la destruction de données (*Trojan horse* en anglais) ;

- le logiciel espion, ou mouchard, est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et de transférer des informations (*spyware* en anglais).

2. LES PROGRAMMES AUTOREPRODUCTEURS.

Les virus définissent avec les vers, la catégorie des programmes autoreproducteurs.

2.1. **Les virus.**

Un virus est un programme ou morceau de programme malveillant dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, etc.) et, bien souvent, d'en atteindre ou d'en parasiter les ressources (données, mémoire, réseau). Le mode de survie peut prendre plusieurs formes : réplication, implantation au sein de programmes légitimes, persistance en mémoire, etc.

Pour sa propagation, un virus utilise tous les moyens disponibles : messagerie, partage de fichiers, portes dérobées, page internet frauduleuse, clés USB.

Les virus peuvent être classés selon plusieurs critères. On a choisi ici de les classer selon la nature de la cible.

Le virus d'exécutable est un code malveillant qui s'attaque à un programme exécutable.

Le virus de document, est un code malveillant s'attaquant aux fichiers produits par les suites bureautiques.

2.2. **Les vers.**

Un ver (ou *worm*) est un logiciel malveillant indépendant, cherchant à propager son code au plus grand nombre de cibles, généralement sans limite puis de l'exécuter sur ces mêmes cibles générant le plus souvent des attaques par indisponibilité (saturation de la mémoire ou de la bande passante).

---

(1) Les bots et les botnets combinent les technologies de type ver (la machine infectée devient base de départ de nouvelles attaques) et cheval de Troie (pour la prise de contrôle à distante de machine corrompues, dites « zombies »).