Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Conforme à l'original produit,
Début du texte, page suivante.

BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°7 du 19 février 2010

PARTIE PERMANENTE
Administration Centrale

Texte n°2

DIRECTIVE N° 11/DEF/DGSIC
portant sur la sécurisation des autocommutateurs.

Du *8 janvier 2010*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 11/DEF/DGSIC portant sur la sécurisation des autocommutateurs.

Du 8 janvier 2010

NOR D E F E 1 0 5 0 0 1 2 X

Classement dans l'édition méthodique : BOEM 160.1

Référence de publication : BOC N°7 du 19 février 2010, texte 2.

SOMMAIRE

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. Présentation.

1.2. Niveaux de préconisation.

1.3. Champ et modalités d'application.

1.4. Gestion des dérogations pour les projets.

2. CADRE DOCUMENTAIRE.

2.1. Documents applicables.

2.2. Normes et standards applicables.

2.3. Autres documents et sites de référence.

3. DOMAINE COUVERT ET EMPLOI.

3.1. Principes fondamentaux.

3.2. Services attendus.

3.3. Périmètre et limites.

4. LES RÈGLES.

4.1. Règles techniques.

4.1.1. Lots techniques.

4.1.2. Réseau.

4.1.3. Administration.

4.1.4. Accès.

4.1.5. Sécurité.

4.2. Règles organisationnelles.

4.2.1. Documentation.

4.2.2. Intervenants.

4.2.3. Sécurité.

5. GLOSSAIRE ET ACRONYMES (*).

Nota 1 : les mots marqués d'un astérisque (*) figurent dans le glossaire.
Nota 2 : les mots entre crochets ([]) figurent dans les documents applicables.

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Présentation.**

La présente directive définit la politique à mettre en œuvre par les organismes du ministère de la défense responsables d'un service de téléphonie classique. Elle fournit les critères de décision pour l'acquisition, la réalisation, la mise en œuvre, le maintien en condition et la sortie de service d'un service de téléphonie classique.

La téléphonie classique, étendue fonctionnellement ou non, est un service sensible et critique, voire vital pour certains organismes.

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

Elle tient compte du projet de [RGS] dans sa version V0.98 du 18 décembre 2008.

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. **Champ et modalités d'application.**

Cette directive est applicable aux systèmes d'information et de communication (SIC) non classifiés de défense supports d'un service de téléphonie classique et à tous leurs composants, notamment leurs éléments actifs. Elle

concerne les aspects suivants : organisation, technique, sécurité, exploitation, fonctionnel et maintenance. Elle fait partie de la politique de sécurité du SIC, support d'un service de téléphonie, qui doit être formellement définie suivant les modalités en vigueur.

Les règles de la présente directive définissent la cible et sont applicables à tout nouveau projet ou toute évolution majeure de projet de téléphonie classique. Elles seront prises en compte avec celles liées à la téléphonie sur le protocole internet dans le cas d'un service de téléphonie mixte (classique et protocole internet).

Cette directive sera appliquée dans les meilleurs délais pour les systèmes ayant fait ou faisant actuellement l'objet d'un portage en téléphonie classique et dès la conception pour ceux nécessitant obligatoirement des rénovations.

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

Elles sont présentées et débattues en CMSSI* et font l'objet d'une approbation par le directeur de la DGSIC. Elles concernent :

- les circonstances et justifications du non respect d'une règle recommandée ;

- les circonstances et justifications du non respect d'une règle déconseillée ;

- les justifications des exceptions à toute règle absolue (obligatoire ou interdit). Dans ce dernier cas, l'avis de la DGSIC doit être demandé au préalable et joint au dossier.

2. CADRE DOCUMENTAIRE.

2.1. **Documents applicables.**

[R&TTE] Directive 1999/5/CE du Parlement européen et du Conseil, du 9 mars 1999 (1), concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, JO L 091 du 7.4.1999. p. 0010 - 0028.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0005:fr:HTML

[CPP] Code de procédure pénale.
(1).http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=DF3AD0911B2E51F6D5D122B48EFD4D0E.tpdjo0

[CPCE] Code des postes et des communications électroniques (1).
http://www.legifrance.gouv.fr/affichCode.do?dateTexte=20091210&cidTexte=LEGITEXT000006070987&fastReqId=

[CNIL] Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, version consolidée au 14 mai 2009.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20091003

[RGI] Référentiel général d'interopérabilité (1).
http://www.references.modernisation.gouv.fr/rgi-interoperabilite
http://www.references.modernisation.gouv.fr/sites/default/files/RGI_Version1%200_0.pdf

[RGS] Référentiel général de sécurité (1).
http://www.references.modernisation.gouv.fr/rgs-securite
http://www.references.modernisation.gouv.fr/sites/default/files/rgs0.98.pdf

[IGI 1300] Instruction générale interministérielle n° 1300/SGDN/PSE/SSD du 25 août 2003 (1) relative à la protection du secret de la défense nationale.
http://www.ssi.gouv.fr/IMG/pdf/igi1300.pdf

[PSSI] IM 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.

[DGSIC001] BOC/PP 6 mars 2007 - Nº 5 texte 8.
Directive n° 1/DEF/DGSIC du 17 octobre 2006 portant sur les logiciels du ministère de la défense . NOR DEFM0652897.
http://www.boc.sga.defense.gouv.fr/visu/boc_visu4.php?nor=M0652897X&id=8994

[PRIS] Politique de référencement intersectoriel de sécurité v2.0 du 1er juin 2005 (1) (ADAE et DCSSI).
http://web.archive.org/web/20061126013510/synergies.modernisation.gouv.fr/article.php3?id_article=123

[RFC 2119] Mots clés à utiliser dans les RFC (Request For Command) pour indiquer un niveau d'exigence (03/1997).

[R 901] Recommandation 901/DISSI/SCSSI (1) pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense du 2 mars 1994.
http://www.ssi.gouv.fr/IMG/pdf/1994_03_02_901_protection_systemes_d_information.pdf

[DGSIC259] Note n° 259/DEF/DGSIC du 15 juin 2006 (1) relative aux spécifications de sécurisation et régime dérogatoire pour les nouvelles technologies.

2.2. **Normes et standards applicables.**

[CNIL ns47] Norme simplifiée n° 47 : délibération n° 2005-019 du 3 février 2005 (1) portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de l'utilisation de services de téléphonie fixe et mobile sur les lieux de travail et portant abrogation de la norme simplifiée n° 40.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000238073&dateTexte=

2.3. **Autres documents et sites de référence.**

[Site DGSIC] Site DGSIC à l'adresse Intradef www.dgsic.defense.gouv.fr
[Sites SSI] Site SSI à l'adresse Intradef www.ssi.defense.gouv.fr
Site SSI à l'adresse Internet www.ssi.gouv.fr

3. DOMAINE COUVERT ET EMPLOI.

La directive vise à définir des mécanismes permettant la sécurisation d'un autocommutateur téléphonique, ainsi que des liaisons à des services connexes (gestion, administration et contrôle). Elle comprend aussi l'organisation humaine nécessaire au bon fonctionnement de ce système d'information téléphonique.

3.1. **Principes fondamentaux.**

Le principe de défense dans la profondeur, en multipliant les protections à tous les niveaux où il est possible d'agir, doit être appliqué à tous les stades de la sécurisation. Ces règles doivent s'inscrire en amont de toute autre action, dont l'objectif est de garantir l'accès physique, l'intégrité et la disponibilité du système et de ses données.

3.2. **Services attendus.**

La téléphonie doit permettre la communication synchrone ou temps réel* entre plusieurs personnes internes ou externes au ministère de la défense, en intégrant différentes fonctionnalités.

3.3. **Périmètre et limites.**

Le périmètre de la présente directive concerne les règles, architectures et mécanismes qui permettent la protection (sécurisation) des communications entre personnes ainsi que certains des éléments de la politique de sécurité. Le domaine couvert concerne la téléphonie dite administrative*.

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. **Lots techniques.***

Énergie électrique :

- RT 01 : il est recommandé d'implanter le local accueillant le poste de transformation MT/BT (moyenne tension/basse tension) sur le site, tout en laissant un accès, sous contrôle, au fournisseur. (Idem pour la dernière chambre de tirage avant transformation) ;

- RT 02 : il est recommandé, dans le cas où une seconde arrivée serait mise en place (secours), de négocier avec le fournisseur un tirage de câble, pour ce qui est hors site, empruntant un chemin physique différent et venant d'une sous-station différente ;

- RO 03 : il est obligatoire de rester conforme à la réglementation pour tout ce qui a trait à l'alimentation électrique : terres, masses, ensembles électriques primaires, TGBT (tableau général basse tension), revêtements de sols ou muraux, locaux renfermant des batteries, parafoudres, parasurtenseurs, ...

Secours énergie électrique :

- RT 04 : il est obligatoire, concernant l'ensemble des matériels formant le SI (serveurs, terminaux, imprimantes, consoles d'administration, ...), qu'un raccordement sur un circuit ondulé soit réalisé avec une disponibilité de secours d'un minimum de 15 minutes, afin de permettre une extinction propre des systèmes, c'est-à-dire avec sauvegarde des données ;

- RT 05 : il est obligatoire, concernant les autocommutateurs*, que le maintien des batteries en tampon soit de l'ordre de 8 heures minimum ;

- RT 06 : il est recommandé, selon l'importance du site, de mettre en place un secours par groupe électrogène, spécifique ou partagé, en portant une attention particulière à sa localisation.

Climatisations et ventilations :

- RT 07 : il est obligatoire d'asservir en arrêt sur une détection confirmée d'incendie l'ensemble climatisation/ventilation ;

- RT 08 : il est recommandé de mettre en place une redondance dans ce domaine afin d'assurer une forte disponibilité.

Incendie :

- RT 09 : il est obligatoire d'avoir à disposition des procédures et des consignes relatives à l'incendie, tant en prévention qu'en action.

Dégât des eaux :

- RT 10 : il est obligatoire de protéger contre le dégât des eaux les locaux revêtant un caractère sensible au regard du système d'information ou contribuant à sa disponibilité.

Contrôle des accès et dispositifs anti-intrusion :

- RT 11 : il est obligatoire de compléter les alarmes, contrôles d'accès et les dispositifs anti-intrusion, ainsi que leurs renvois intégrés ou non dans une unité de gestion centralisée, par des consignes et des procédures ;

- RT 12 : il est recommandé de ne pas confier la gestion des alarmes techniques et celles concernant les contrôles d'accès/anti-intrusion aux mêmes personnes et qu'elles ne soient pas techniquement regroupées.

4.1.2. ***Réseau.***

Informatique :

- RT 13 : il est recommandé de ne pas interconnecter l'ensemble du système téléphonique* à un réseau informatique, sauf si ce dernier est spécifique à son administration et son exploitation.

Distribution des lignes téléphoniques :

- RT 14 : il est obligatoire de placer sous clé l'ensemble des éléments de distribution d'une installation téléphonique ;

- RT 15 : il est obligatoire de réaliser et de maintenir un plan détaillé du schéma de câblage, qui pourra également servir de base à des inspections régulières.

4.1.3. ***Administration.***

Relevé de configuration :

- RT 16 : il est recommandé d'établir et de tenir à jour, aussi souvent que nécessaire, un relevé de configuration des autocommutateurs, en distinguant les différents types de serveur et leur localisation dans l'architecture globale du système d'information ;

- RT 17 : il est obligatoire d'identifier le relevé de configuration papier comme Diffusion Restreinte et de le stocker dans un endroit protégé.

Mots de passe :

- RT 18 : il est obligatoire d'activer la fonction d'authentification et de mettre en place une authentification forte (mot de passe à usage unique au minimum et différent du mot de passe constructeur) pour l'accès à l'exploitation du système. Si cette fonction n'existe pas, il est nécessaire de fortement renforcer la sécurité physique du commutateur pour en interdire l'accès à toute personne non autorisée ;

- RT 19 : il est obligatoire, de sensibiliser les utilisateurs et les administrateurs aux risques liés à l'utilisation dangereuse des mots de passe réutilisables ou des codes d'accès triviaux, partagés entre plusieurs utilisateurs ou identiques sur plusieurs systèmes, puis de les former à des comportements plus sûrs ;

- RT 20 : il est recommandé de recenser l'ensemble des comptes et d'en modifier ou d'en faire modifier les mots de passe par défaut (en forçant leur changement) et de supprimer les comptes inutilisés.

Administration locale :

- RT 21 : il est obligatoire de protéger efficacement le terminal local d'administration (accès, subtilisation), en mettant en œuvre les mêmes mécanismes de sécurité que pour l'autocommutateur lui-même ;

- RT 22 : il est recommandé d'administrer le serveur à partir de sa console d'administration, en renforçant sa sécurité et en évitant de la déporter dans un bureau annexe ; la protection doit inclure en particulier l'utilisation ponctuelle d'un compte spécifique avec les privilèges adéquats.

Administration distante :

- RT 23 : il est obligatoire, dans le cas où une administration distante est requise, de limiter cette dernière aux seuls postes des administrateurs, en particulier au niveau de leur adresse IP, avec un degré de protection au moins équivalent à celui du serveur (sécurité physique et logique).

Protection des données :

- RT 24 : il est recommandé, afin de protéger les données circulant sur le réseau, d'utiliser des mécanismes cryptographiques conformes aux exigences, portant a minima sur la protection des identifications/authentifications et d'intégrer cette partie du système d'information dans l'homologation.

SNMP :

- RT 25 : il est recommandé, dans le cas où la couche réseau SNMP est activée et en prenant en compte les limitations liées à l'implémentation du protocole, que les noms de communauté utilisés répondent aux mêmes contraintes de complexité que les mots de passe, voire que le trafic SNMP soit véhiculé dans des tunnels de niveau adéquat (voir RT24).

Télémaintenance :

- RT 26 : il est obligatoire de ne pas activer en permanence la liaison de télémaintenance du serveur et de débrancher physiquement le modem d'accès à cette fonctionnalité en fonctionnement normal ;

- RT 27 : il est interdit, pour l'administration à distance des autocommutateurs, d'utiliser un modem simple sans authentification ;

- RT 28 : il est obligatoire, concernant le modem donnant accès à la liaison de télémaintenance, d'utiliser au minimum deux des trois mécanismes de sécurisation suivants :

  - modem acceptant exclusivement des méthodes d'authentification fortes ;

  - modem assurant un rappel automatique d'un numéro prédéfini (call-back), lui-même protégé par la RT37 ;

  - modem utilisant un chiffrement adéquat (voir RT24) ;

- RT 29 : il est recommandé, concernant le modem donnant accès à la liaison de télémaintenance, d'utiliser conjointement les trois mécanismes de sécurisation suivants :

  - modem acceptant exclusivement des méthodes d'authentification fortes ;

  - modem assurant un rappel automatique d'un numéro prédéfini (call-back), lui-même protégé par la RT37 ;

- modem utilisant un chiffrement adéquat (voir RT24) ;

- RT 30 : il est obligatoire, dans le cas où toute ou partie de la télémaintenance est réalisée par des prestataires externes, d'imposer, même si cela peut être lourd, des règles très strictes de gestion des moyens d'identification/authentification et de contrôle du personnel en charge de la prestation ; ces règles doivent inclure l'accès nominatif des comptes d'administration, la mise en place de traçabilité spécifique, la tenue d'un carnet de bord des actions d'administration réalisées.

Protection des communications :

- RT 31 : il est obligatoire d'assurer la protection de toutes les communications risquant d'être interceptées hors du cadre légal (conformément à la loi n° 91-646 [SECCOR] et/ou au code de procédure pénale) ;

- RT 32 : il est recommandé, dans le cas de communications destinées à échanger des informations très sensibles, d'utiliser des moyens de communication (réseaux homologués) assurant un chiffrement adéquat des communications.

Journalisation, imputabilité et accès concurrentiels :

- RT 33 : il est obligatoire de mettre en œuvre, lorsque cela est possible, la journalisation protégée de manière adéquate des actions opérées par les administrateurs.

Sauvegardes :

- RT 34 : il est obligatoire d'assurer l'intégrité et une sauvegarde régulière des éléments de configuration de l'ensemble du système téléphonique*, en respectant les principes élémentaires (vérification, lieu de conservation, qualité, ...) ;

- RT 35 : il est recommandé de mettre en place des exercices périodique visant à tester les procédures de restauration des éléments sauvegardés.

4.1.4. ***Accès.***

Consoles opératrices/postes opérateurs :

- RT 36 : il est recommandé de ne pas déployer de console opératrice ou poste opérateur au sein d'une organisation si les fonctions de base des postes téléphoniques sont suffisantes et dans le cas contraire, de limiter les interactions entre ces postes et le système d'information téléphonique dans le respect du « moindre privilège » et en définissant des consignes strictes.

Réseau téléphonique public :

- RT 37 : il est recommandé, pour l'administration à distance des autocommutateurs à travers un réseau public, de faire attribuer par l'opérateur un numéro de téléphone SDA* ne faisant pas partie de la ou des principales plages de numéros SDA gérés par l'autocommutateur, de le faire inscrire sur « liste rouge » et de veiller à ce qu'il ne soit référencé dans aucun document public ;

- RT 38 : il est obligatoire de définir, en respectant le principe du « moindre privilège », les utilisateurs ayant accès à la messagerie vocale, d'identifier ceux qui bénéficient aussi d'un accès externe à cette messagerie et de consigner le tout dans un document d'exploitation.

4.1.5. ***Sécurité.***

Substitution :

- RT 39 : il est recommandé, sauf besoin motivé, de désactiver les fonctions de substitution et de groupes d'interception.

Entrée en tiers :

- RT 40 : il est obligatoire, sauf besoin motivé, de désactiver la fonction permettant de s'insérer dans une conversation sans y avoir été invité.

Renvoi sur numéro externe :

- RT 41 : il est obligatoire de limiter les possibilités de renvois des postes téléphoniques (intégrant la consultation à distance de la messagerie utilisateur) aux seuls renvois vers des numéros internes à l'entité ou des numéros externes prédéfinis, tout en sensibilisant les utilisateurs ;

- RT 42 : il est recommandé d'exercer un suivi strict de la taxation relative aux renvois.

DISA* :

- RT 43 : il est obligatoire, sauf si le besoin de la fonction DISA est motivé, de désactiver la fonction permettant à un abonné d'accéder depuis l'extérieur aux fonctions d'usager interne légitime (boîte vocale par exemple) ;

- RT 44 : il est recommandé, si la fonction DISA est nécessaire, de veiller à limiter soigneusement les services de l'autocommutateur et les personnes susceptibles d'y accéder, tout en sécurisant cet accès (authentification forte, journalisation).

Poste fictif :

- RT 45 : il est obligatoire de répertorier explicitement les postes fictifs créés et de vérifier régulièrement l'état du parc par rapport à l'ensemble des postes affectés à des prises valides.

Justification :

- RT 46 : il est obligatoire de désactiver la fonctionnalité permettant de masquer certains postes dans la facturation éditée par l'autocommutateur et de réaliser régulièrement un audit de l'ensemble des postes recensant d'éventuels postes non justifiés.

Cadenas ou verrouillage des postes :

- RT 47 : il est recommandé d'activer les fonctions qui permettent à un utilisateur de verrouiller et de déverrouiller son poste ;

- RT 48 : il est recommandé, si l'autocommutateur le permet, d'automatiser le verrouillage et déverrouillage des postes (horaires prédéfinis).

Accès au réseau public :

- RT 49 : il est obligatoire de définir, conformément au principe de « moindre privilège », à quel type de réseau un poste peut accéder : interne, local (urbain), national (interurbain), international, mobile, numéros surtaxés, numéros de fournisseurs d'accès à Internet ;

- RT 50 : il est recommandé de définir et d'utiliser des catégories d'accès jour/nuit.

Aboutement de réseau :

- RT 51 : il est obligatoire, sauf besoin motivé, de désactiver la fonction permettant de mettre en relation directe et autonome deux numéros appelés.

4.2. **Règles organisationnelles.**

4.2.1. ***Documentation.***

- RO 01 : il est obligatoire que, au sein d'un organisme mettant en œuvre un autocommutateur, il existe une politique de sécurité du système d'information, à jour, qui détaille les règles relatives à la protection (mise en sécurité) de l'autocommutateur, incluant les mises à jours de sécurité et, pour les sites d'administration, une procédure de dévolution ;

- RO 02 : il est obligatoire, dans le cas d'une architecture basée sur une télémaintenance avec accès par le réseau téléphonique public, de mettre en place une procédure, avec le concours des acteurs autorisés à accéder au local de l'autocommutateur, pour éviter d'offrir un accès permanent aux acteurs malveillants ;

- RO 03 : il est recommandé de définir, maintenir à jour et tester périodiquement (exercices) des fiches réflexes pour gérer les alertes et préciser, pour chaque incident possible, les tâches devant être réalisées ;

- RO 04 : il est recommandé de définir et d'inclure dans la politique de sécurité une politique de gestion des codes d'accès lorsque le verrouillage des postes est mis en place ;

- RO 05 : il est obligatoire de définir et d'inclure dans la politique de sécurité une politique de gestion des moyens d'authentification forts concernant les comptes d'administration des équipements de téléphonie ;

- RO 06 : il est recommandé de mettre à jour et de regrouper dans un même document l'ensemble des documents techniques (architecture des équipements de téléphonie, procédures de configurations des postes téléphoniques, plans de câblages, schémas divers,...).

4.2.2. ***Intervenants.***

- RO 07 : il est obligatoire d'identifier les différents acteurs qui interviennent ou interagissent, directement ou indirectement, sur un autocommutateur ;

- RO 08 : il est recommandé de préciser le rôle de chacun des intervenants identifiés dans la RO 07 ;

- RO 09 : il est recommandé de séparer les rôles et les responsabilités dans l'exploitation du système de téléphonie (celui qui définit la politique de sécurité ne configure pas; celui qui exploite les traces dans les journaux et la comptabilité ne les configure pas) ;

- RO 10 : il est recommandé, pour garantir une disponibilité adéquate, de veiller à ce que le personnel chargé de l'administration soit en nombre suffisant et soit formé aux dernières évolutions.

4.2.3. ***Sécurité.***

Homologation/audit :

- RO 11 : il est obligatoire d'homologuer le système suivant un processus d'homologation conforme à l'article 47 de l'IGI 1300, comprenant une gestion globale et continue des risques grâce à des inspections périodique du système et des audits périodique de configuration ;

- RO 12 : il est obligatoire d'effectuer périodiquement et selon les besoins spécifiques des inspections et audits de l'écart entre la politique de sécurité adéquate, choisie formellement, et la situation réelle ;

- RO 13 : il est recommandé d'effectuer périodiquement une revue de la configuration et de l'attribution des catégories d'accès, de l'allocation de catégories d'exploitation et de la définition ou

non de postes fictifs ou injustifiés.

Gestion des correctifs :

- RO 14 : il est recommandé de rechercher la solution la plus stable et sécurisée lorsqu'il s'agit de mise en place de correctifs de sécurité (derniers correctifs sur dernière version logicielle, dernière version stable connue, ...).

Serveur de secours :

- RO 15 : il est recommandé, en fonction du besoin en disponibilité, de disposer d'un serveur/système de secours, évoluant de la même manière que le composant qu'il est chargé de remplacer et qui doit être testé périodiquement.

Outils de contrôle :

- RO 16 : il est recommandé de mettre en place des solutions de protection (sécurisation) tout en établissant une corrélation avec une configuration de base maintenue et intègre ; ces solutions doivent permettre de détecter, d'analyser et bloquer les flux de téléphonie suspects et malveillants (facilitant entre autre la détection d'équipements illicites).

Révocation :

- RO 17 : il est recommandé de révoquer le plus rapidement possible les capacités d'authentification des utilisateurs ayant quitté l'organisme.

5. GLOSSAIRE ET ACRONYMES (*).

ACL (Access Control List) : liste de permissions (lecture, écriture, exécution) sur un fichier, un répertoire ou une arborescence ajoutée aux permissions classiques. Ces permissions concernent des utilisateurs et/ou des groupes définis.

Authentification : concept ayant pour but de garantir l'identité et les droits associés d'un correspondant dans une transaction à distance. En télécommunication, les procédures correspondantes font généralement appel à des procédés de cryptographie par clé publique ou privée. L'authentification est dite forte si elle permet d'empêcher le rejeu d'un échange intercepté.

Autocommutateur : équipement capable d'établir des connexions temporaires entre des lignes entrantes et sortantes pour acheminer des communications. Commutateur d'abonné (ou commutateur privé) : commutateur téléphonique qui appartient à une installation terminale chez l'abonné et qui est raccordé au réseau général du téléphone. Voir aussi les anglicismes PABX, PBX, IPBX.

CDR (Call Detail Record) : enregistrement de données contenant les informations relatives aux appels téléphoniques telles que l'adresse de l'appelant et celle du destinataire, l'heure d'appel et celle de terminaison d'appel, la durée de l'appel et les taxes ajoutées sur le réseau ou la taxation des opérateurs de service.

Chiffrement : moyen par lequel un message est rendu inintelligible en l'absence d'un moyen approprié appelé convention secrète (par exemple clé de chiffrement). Les clefs sont basées sur des algorithmes mathématiques.

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

CNIL : Commission nationale de l'informatique et des libertés.

Commutateur : équipement électronique auquel sont raccordés les abonnés et qui permet leur interconnexion.

Commutation : établissement de connexion à la demande et seulement pendant la durée d'une conversation entre des lignes téléphoniques d'abonnés ou, plus généralement, entre des circuits et/ou lignes de transmission.

Commutation de circuits : système dans lequel chaque voie de communication dispose de supports physiques de transmission qui lui sont affectés pendant toute la durée de la communication, même pendant les silences.

DECT (Digital Enhanced Cordless Telephone) : norme de téléphonie sans fil, fonctionnant dans la bande des 1800 MHz, définie à la fin des années 80 par l'ETSI. Le DECT permet d'offrir des services de téléphonie de proximité autour d'un autocommutateur d'entreprise ou d'un poste résidentiel. Les postes portatifs peuvent dialoguer entre eux et prendre une liaison externe.

DISA (Direct Inward System Access) : fonction qui permet d'obtenir d'une destination externe des fonctions internes (boîte vocale, annuaire, appel vers une destination externe). Cette fonction peut être utilisée pour effectuer de chez soi un renvoi de poste de bureau vers une destination interne ou externe (distinct de la SDA (Sélection Directe à l'Arrivée)).

DTMF (Dual Tone Multi-Frequency - en français : signalisation multifréquences) : une des signalisations utilisées en téléphonie. Elle consiste à combiner deux fréquences prises parmi cinq (700, 900, 1100, 1300 et 1500 Hz). Cette signalisation est utilisée notamment lorsque l'on effectue la numérotation de son correspondant.

E.164 : recommandation de l'UIT, actuellement utilisée pour la numérotation téléphonique au plan mondial.

Équipement légitime : équipement autorisé par la politique de sécurité.

Facilités téléphoniques : ensemble de fonctionnalités, permettant d'enrichir la fonction de base de téléphonie, telles que le transfert d'appel, le filtrage patron - secrétaire, la mise en attente, etc.

Flux légitime : flux entre deux équipements conforme à la politique de sécurité.

ITU (International Telecommunication Union) : voir UIT.

Messagerie vocale : système d'enregistrement, de stockage, d'écoute, voire de réexpédition, de messages vocaux, fonctionnant comme un répondeur téléphonique partagé par plusieurs utilisateurs.

PABX : Private Automatic Branch eXchange ; autocommutateur téléphonique privé. Il sert à relier les postes téléphoniques d'un établissement (lignes internes) avec le réseau téléphonique public (lignes externes). Il permet la mise en œuvre d'un certain nombre de fonctions, notamment :

- relier plus de lignes internes qu'il n'y a de lignes externes ;
- permettre des appels entre postes internes sans passer par le réseau public ;
- programmer des droits d'accès au réseau public pour chaque poste interne ;
- proposer un ensemble de services téléphoniques (conférences, transferts d'appel, renvois, messagerie, appel par nom, ...) ;
- gérer la sélection directe à l'arrivée ;
- gérer la ventilation par service de la facture téléphonique globale (taxation) ;
- apporter des services de couplage téléphonie-informatique.

PCA (plan de continuité d'activité) : ensemble de mesures visant à assurer, selon divers scénarios de crise, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé,

des prestations de services essentielles de l'entreprise puis la reprise planifiée de l'activité. C'est donc un mode planifié et formalisé de réaction à un sinistre en vue de diminuer ses impacts adverses sur l'activité de l'entreprise. C'est plus qu'un plan de secours informatique, plus qu'un plan de gestion de crise, plus qu'un plan de reprise d'activité, plus qu'un plan de continuité opérationnel, plus que des procédures de fonctionnement dégradé : on pourrait dire que c'est tout cela, coordonné.

PRA (plan de reprise d'activité) : plan permettant de répondre au besoin du redémarrage rapide de l'activité suite à un sinistre occasionnant la perte partielle ou totale du site informatique de production. Il se traduit par :

- une infrastructure matérielle/logicielle et des procédures de transfert de données assurant une copie sécurisée des applications et données vitales pour l'entreprise ;

- des procédures d'accès au système ainsi que les processus humains permettant le redémarrage des services.

QoS (Quality of Service - en français : qualité de service) : recouvre des ensembles de plus en plus souvent formalisés de critères permettant d'évaluer le service rendu.

Les critères varient selon le type de service, mais on retrouve souvent, au-delà de la qualité des réseaux (débit annoncé...), des critères liés à l'accueil client, au service après-vente, à la disponibilité, à la réactivité, avec des engagements contractualisés. Voir aussi SLA.

QSIG : protocole de signalisation compatible avec le système de signalisation par canal sémaphore n° 7 (SS7) permettant l'interconnexion d'autocommutateurs privés (PABX) hétérogènes.

Réseau maîtrisé : réseau sur lequel on peut faire appliquer une PSSI, des mesures de détection, de coercition ou blocage.

RTC (réseau téléphonique commuté - en anglais : PSTN ou Public Switched Telecommunication Network) : réseau permettant l'établissement de communications point à point par commutation de circuits. Ce réseau offre un débit numérique ou une bande passante garantie qui peut être utilisée pour transmettre des données informatiques, des télécopies, etc. par utilisation d'un modem.

SDA : sélection directe à l'arrivée.

Signalisation téléphonique : ensemble des ordres ou informations échangés entre autocommutateurs ou entre un autocommutateur et un poste, afin d'établir, maintenir ou terminer une communication.

- Signalisation téléphonique par canal sémaphore (SS7) :
technique de signalisation dans laquelle les informations de signalisation relatives à un circuit ne sont pas transmises sur ce circuit mais sur des canaux sémaphores indépendants ne transmettant que des données. Le système le plus répandu est le code CCITT n° 7.

- Signalisation téléphonique RON-TRON :

méthode de signalisation, hors bande ou dans la bande par laquelle l'information de signalisation est restituée aux extrémités sur les équipements de commutation et de transmission au moyen de fils conducteurs spécialisés, appelés RON (réception par l'autocommutateur) et TRON (transmission par l'autocommutateur).

SNMP (Simple Network Management Protocol) : protocole de communication de la famille TCP-IP (internet) qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et des matériels à distance.

Système téléphonique : ensemble constitué par l'autocommutateur et les organes informatiques dédiés à son administration.

Téléphonie : application synchrone qui « travaille » avec des flux isochrones. La diffusion vidéo ou sonore n'est pas synchrone, seuls les flux sont qualifiés d'isochrones.

Téléphonie administrative : téléphonie standard par opposition à la téléphonie opérationnelle.

Temps réel : propriété des applications dont les données manipulées ont une durée de validité prédéterminée. Ce sont des applications dites aussi à temps borné.

Exemple : la transmission de l'heure avec une précision d'une seconde demande à ce que le temps de réponse du système soit inférieur à la seconde, sinon l'information reçue est erronée.

Dans le cas d'une application interactive, la notion de temps réel recouvre celle du fonctionnement correct de l'application. Pour assurer une communication téléphonique correcte, le temps de bouche à oreille (appelé aussi temps bo) doit être inférieur à 150 ms (ITU-T G.114).

UIT : l'union internationale des télécommunications est la plus ancienne organisation internationale technique de coordination (ex CCITT). Elle est chargée de la réglementation et de la planification des télécommunications dans le monde, elle établit les normes de ce secteur et diffuse toutes les informations techniques nécessaires pour permettre l'exploitation des services mondiaux des télécommunications.

Pour le ministre de la défense et par délégation :

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

Christian PENILLARD.

---

(1) n.i. BO.