Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS®

SECTION 4
OUTILLAGE POUR L'APPRÉCIATION DES RISQUES SSI

Version 2 – 5 février 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)
en collaboration avec le Club EBIOS

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante
(voir formulaire de recueil de commentaires en fin de guide) :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

ebios.dcssi@sgdn.pm.gouv.fr

Historique des modifications

Version	Objet de la modification	Statut
02/1997 (1.1)	Publication du guide d'expression des besoins et d'identification des objectifs de sécurité (EBIOS).	Validé
23/01/2004	Révision globale : - Explications et mise en cohérence avec les normes internationales de sécurité et de gestion des risques - Mise en évidence du référentiel réglementaire par rapport à l'ensemble des contraintes à prendre en compte - Intégration des concepts d'hypothèse et de règles de sécurité (ISO/IEC 15408) - Transfert de la sélection des éléments essentiels dans l'Étude du système-cible - Amélioration de l'élaboration de l'échelle de besoins est améliorée : les valeurs représentant les limites acceptables pour l'organisme par rapport à des impacts personnalisés - Intégration de la détermination des besoins par élément dans l'activité suivante - Intégration de la détermination du mode d'exploitation dans les hypothèses - Adaptation des concepts à l'ISO/IEC 15408 : on étudie l'origine des menaces, c'est-à-dire les méthodes d'attaque et les éléments menaçants, ainsi que leur caractérisation, qui peut inclure un type (naturel, humain, environnemental) une cause (accidentelle, délibérée, en affinant en exposition, ressources disponibles, expertise, motivation), un potentiel d'attaque - Mise en évidence des méthodes d'attaque non retenues - Formalisation des menaces, au sens ISO/IEC 15408 (élément menaçant, attaque et bien sous la forme des entités), avant la confrontation aux besoins de sécurité - Modification de la confrontation des menaces aux besoins, qui permet d'identifier les risques - Mise en évidence des risques non retenus - Intégration de la détermination des objectifs de sécurité minimums dans les activités Formalisation des objectifs de sécurité et Détermination des exigences fonctionnelles - Modification de la détermination des objectifs de sécurité, qui prend en compte les hypothèses, règles de politique de sécurité, contraintes, référentiel réglementaire et risques - Ajout de la détermination des niveaux de sécurité, qui permet de déterminer le niveau des objectifs de sécurité (notamment en fonction des potentiels d'attaque) et de choisir un niveau d'assurance - Ajout de la détermination des exigences de sécurité fonctionnelles, qui permet de déterminer les exigences fonctionnelles couvrant les objectifs de sécurité et de présenter cette couverture - Ajout de la détermination des exigences de sécurité d'assurance, qui permet de déterminer les éventuelles exigences d'assurance Améliorations de forme, ajustements et corrections mineures (grammaire, orthographe, formulations, présentations, cohérence…)	Validé par le Club EBIOS
05/02/2004	Publication de la version 2 du guide EBIOS	Validé

Table des matières

1 Introduction

La méthode EBIOS[1] est composée de cinq sections complémentaires.

- Section 1 – Introduction
  Cette section présente le contexte, l'intérêt et le positionnement de la démarche EBIOS. Elle contient aussi une bibliographie, un glossaire et des acronymes.

- Section 2 – Démarche
  Cette section expose le déroulement des activités de la méthode.

- Section 3 – Techniques
  Cette section propose des moyens de réaliser les activités de la méthode. Il conviendra d'adapter ces techniques aux besoins et pratiques de l'organisme.

- Section 4 – Outillage pour l'appréciation des risques SSI
  Cette section constitue la première partie des bases de connaissances de la méthode EBIOS (types d'entités, méthodes d'attaques, vulnérabilités).

- Section 5 – Outillage pour le traitement des risques SSI
  Cette section constitue la seconde partie des bases de connaissances de la méthode EBIOS (objectifs de sécurité, exigences de sécurité, tableaux de détermination des objectifs et exigences de sécurité fonctionnelles).

Le présent document constitue la quatrième section de la méthode.

Il présente :
- une typologie des types et sous-types d'entités,
- une typologie des méthodes d'attaques décrites selon les éléments menaçants pouvant les exploiter,
- une base de vulnérabilités par méthode d'attaque et sous-type d'entités.

Le tableau suivant présente l'évolution des bases de connaissances fournies dans la section "Outillage" entre la version précédente de la méthode EBIOS et la présente version :

EBIOS v1		**EBIOS v2**	
Objets	**Forme**	**Objets**	**Forme**
Types d'entités	Brève description dans le guide "Techniques"	Types d'entités	Description détaillée et exemples
Sous-types d'entités	Rien dans le guide "Outillage"	Sous-types d'entités	Description détaillée et exemples
Menaces	Liste, regroupement par thèmes, description selon la cause (accidentelle ou délibérée) et l'atteinte	Méthodes d'attaque	Liste, regroupement par thèmes et description selon les éléments menaçants pouvant les exploiter (type, cause, exemples)
Vulnérabilités	Liste de vulnérabilités par menace et type d'entités	Vulnérabilités	Liste de vulnérabilités par méthode d'attaque et sous-type d'entités, avec des exemples

[1] EBIOS est une marque déposée du Secrétariat général de la défense nationale en France.

2 Types et sous-types d'entités

Note
Chaque type et chaque sous-type fait l'objet d'une description. Les exemples figurent en italique.

2.1 MAT : Matériel

Le type matériel est constitué de l'ensemble des éléments physiques d'un système informatique.

2.1.1 MAT_ACT : Support de traitement de données (actif)

Équipement informatique de traitement automatique de données comprenant les organes nécessaires à son fonctionnement autonome.

2.1.1.1 MAT_ACT.1 : Matériel transportable

Matériels informatiques conçus pour être déplacés manuellement et utilisé en des lieux différents.

Micro-ordinateur portable, PDA.

2.1.1.2 MAT_ACT.2 : Matériel fixe

Matériels informatiques appartenant à l'organisme ou utilisés dans les locaux de l'organisme.

Serveur, micro-ordinateur utilisé comme poste de travail.

2.1.1.3 MAT_ACT.3 : Périphérique de traitement

Matériel connecté à un ordinateur par un port de communication (série, parallèle, USB ...) pour la saisie, le transport ou l´émission de données.

Imprimante, lecteur de disques amovible.

2.1.2 MAT_PAS : Support de données (passif)

Il s'agit de supports de stockage d'informations ou de fonctions.

2.1.2.1 MAT_PAS.1 : Support électronique

Support électronique connectable à un ordinateur ou à un réseau informatique pour le stockage de données. Ils sont susceptibles de contenir de grand volume de données tout en restant de petite taille. Ils sont utilisables à partir d'équipement informatique standard.

Disquette, cédérom, cartouche de sauvegarde, disque dur amovible, clé-mémoire, bande.

2.1.2.2 MAT_PAS.2 : Autres supports

Support statique non électronique contenant des données.

Papier, diapositive, transparent, documentation, fax.

2.2 LOG : Logiciel

Le type logiciel est constitué de l'ensemble des programmes participant au fonctionnement d'un ensemble de traitements de l'information.

2.2.1 LOG_OS : Système d'exploitation

Ce libellé comprend l'ensemble des logiciels d'un ordinateur constituant le socle opérationnel sur lequel vont s'exécuter l'ensemble des autres logiciels (services ou applications). Il comprend un noyau et des fonctions ou services de base. Selon les architectures, un système d'exploitation peut être monolithique ou constitué d'un micro-noyau et d'un ensemble de services systèmes. Le système d'exploitation contient principalement tous les services de gestion du matériel (CPU, mémoire, disques, périphériques et interfaces réseaux), ceux de gestions des taches ou processus et ceux de gestion des utilisateurs et de leurs droits.

GCOS, MVS, Solaris, Linux, Windows95, Windows2000, WindowsXP, PalmOS, WCX, MacOS.

2.2.2 LOG_SRV : Logiciel de service, maintenance ou administration

Logiciel qui se caractérise par le fait qu'il complète les services du système d'exploitation et qu'il n'est pas au service direct des utilisateurs ou des applications (même s'il est le plus souvent essentiel ou même indispensable au fonctionnement global du SI).

Logiciel d'administration (Tivoli, Openview…), logiciel d'administration à distance (PC-Anywhere, VNC…).

2.2.3 LOG_STD : Progiciel ou logiciel standard

Les logiciels standards ou progiciels sont de véritables produits commercialisés comme tels (et pas des développements uniques ou spécifiques) avec support, version et maintenance. Ils rendent des services « génériques » aux utilisateurs et applications, mais ne sont pas personnalisés ou spécifiques comme des applications métier.

Logiciel de gestion de base de données, logiciel de messagerie, logiciel de groupware, logiciel d'annuaire, logiciel de type web-serveur…(Oracle, DB2, IIS, Apache, Lotus Notes, Exchange, OpenLDAP…).

2.2.4 LOG_APP : Application métier

2.2.4.1 LOG_APP .1 : Application métier standard

Il s'agit de logiciels du marché dont la finalité est de fournir directement aux utilisateurs les services et fonctions qu'ils attendent de leur système d'information dans le cadre de leur métier. Les domaines sont multiples et par définition sans limite.

Logiciel de comptabilité, logiciel de pilotage de machine outil, logiciel de « customer-care », logiciel de gestion des compétences du personnel, logiciel de téléprocédure administrative…

2.2.4.2 LOG_APP .2 : Application métier spécifique

Il s'agit de développements spécifiques (ce qui impacte notablement les aspects de support, maintenance, évolutions…) dont la finalité est de fournir directement aux utilisateurs les services et fonctions qu'ils attendent de leur système d'information dans le cadre de leur métier. Les domaines sont multiples et par définition sans limite.

Gestion de facturation des clients de l'opérateur télécom, application de suivi temps réel de lancements de fusée.

2.3 RES : Réseau

Le type réseau est constitué de l'ensemble des dispositifs de télécommunication permettant l'interconnexion de plusieurs ordinateurs ou composants d'un système d'information physiquement éloignés.

2.3.1 RES_INF : Médium et supports

Les médiums ou supports de communication et télécommunication se caractérisent principalement par les caractéristiques physiques et techniques du support (point à point, diffusion) et par les protocoles de communication (lien ou réseau – niveau 2 et 3 du modèle OSI à 7 couches).

RTC, Ethernet, GigabitEthernet, câble, fibre, ADSL sur cuivre, WiFi 802.11, BlueTooth, FireWire.

2.3.2 RES_REL : Relais passif ou actif

Ce sous-type comprend tous les dispositifs qui ne sont pas des terminaisons logiques des communications (vision SI) mais des intermédiaires ou relais. Ces relais comportent du matériel mais souvent des logiciels ad-hoc. Ils se caractérisent par les protocoles de communication –réseau– supportés. Ils comportent souvent, en plus du simple relais, des fonctions et services de routage (aiguillage des communications) et/ou de filtrage (filtres dans les routeurs). Ils sont souvent administrables à distance et parfois capables de générer des traces (journaux).

Pont, routeur, hub, switch, autocommutateur.

2.3.3 RES_INT : Interface de communication

Les interfaces de communication des unités de traitement. Elles y sont rattachées, mais se caractérisent par les média et protocoles supportés, par les éventuelles fonctions et capacités de filtrage, de génération de journaux ou d'alerte et par la possibilité et le besoin d'administration à distance.

Adaptateur Wifi, GPRS, Ethernet.

2.4 PER : Personnel

Le type personnel est constitué de l'ensemble des groupes d'individus en relation avec le système d'information.

2.4.1 PER_DEC : Décisionnel

Ce sont les propriétaires des éléments essentiels (informations et fonctions) et les responsables hiérarchiques au sein de l'organisation ou d'un projet spécifique.

Direction générale, Chef de projet.

2.4.2 PER_UTI : Utilisateurs

Ce sont les personnels qui manipulent des éléments sensibles dans le cadre de leur activité et qui ont une responsabilité particulière à cet égard. Ils peuvent disposer de privilèges particuliers d'accès au système d'information pour assurer leurs tâches quotidiennes.

Direction des ressources humaines, Direction financière, gestionnaire de risques.

2.4.3 PER_EXP : Exploitant / Maintenance

Ce sont les personnels en charge de l'exploitation et de la maintenance du système d'information. Ils disposent de privilèges particuliers d'accès au système d'information pour assurer leurs tâches quotidiennes.

Administrateur système, administrateur de données, opérateur de sauvegarde, Help Desk, déploiement d'application, agents de sécurité.

2.4.4 PER_DEV : Développeur

Ce sont les personnels en charge des développements des applications dans l'organisme. Ils accèdent à une partie du système d'information avec des privilèges avancés mais n'agissent pas sur les données de production.

Développeurs d'applications métier.

2.5 PHY : Site

Le type site est constitué de l'ensemble des lieux contenant tout ou une partie du système et les moyens physiques nécessaires à son fonctionnement.

2.5.1 PHY_LIE : Lieu

Périmètres, enceintes physique.

2.5.1.1 PHY_LIE.1 : Externe

Il s'agit de tous les lieux dans lesquels les moyens de sécurité de l'organisme ne peuvent être appliqués.

Domicile des personnels, locaux d'un autre organisme, environnement externe au site (zone urbaine, zone à risque).

2.5.1.2 PHY_LIE.2 : Locaux

Ce lieu est délimité par le périmètre de l'organisme directement en contact avec l'extérieur. Il peut d'agir d'un périmètre de protection physique obtenue en créant des barrières physiques ou des moyens de surveillance autour des bâtiments.

Établissement, bâtiments.

2.5.1.3 PHY_LIE.3 : Zone

Il s'agit d'un périmètre de protection physique offrant un cloisonnement des locaux dans l'organisme. Il est obtenu en créant des barrières physiques autour des infrastructures de traitement de l'information de l'organisme.

Bureaux, zone d'accès réservé, zone sécurisée.

2.5.2 PHY_SRV : Service essentiel

Ensemble de services nécessaires au fonctionnement des matériels dans l'organisme.

2.5.2.1 PHY_SRV.1 : Communication

Services et équipement de télécommunication fournis par un opérateur.

Ligne téléphonique, PABX, réseaux téléphoniques internes.

2.5.2.2 PHY_SRV.2 : Énergie

Services et moyens (sources et câblage) nécessaires à l'alimentation des matériels informatiques et périphériques.

Alimentation basse tension, onduleur, tête de réseau électrique.

2.5.2.3 PHY_SRV.3 : Refroidissement /pollution

Services et moyens (matériel, conduite) de refroidissement et de purification de l'air.

Conduites d'eau glacée, climatiseurs.

2.6 ORG : Organisation

Le type organisation décrit le cadre organisationnel, constitué de l'ensemble des structures de personnels affectés à une tâche et des procédures régissant ces structures.

2.6.1 ORG_DEP : Organisation dont dépend l'organisme

Il s'agit d'organisations dont dépend l'organisme étudié, qu'il y soit juridiquement rattaché ou externe. L'organisme étudié est alors contraint en termes de réglementation, de décisions, d'actions voir de remontée d'informations.

Institution de tutelle, Siège d'un organisme, Cours des comptes.

2.6.2 ORG_GEN : Organisation de l'organisme

Il s'agit des différentes branches de l'organisme rattachées à sa direction, incluant ses activités transversales.

Direction des ressources humaines, direction informatique, direction des achats, directions métiers, service de sécurité des bâtiments, service incendie, Direction de l'audit.

2.6.3 ORG_PRO : Organisation de projet ou d'un système

Il s'agit de l'organisation mise en place pour un projet ou un service particulier.

Projet de développement d'une nouvelle application, projet de migration du système d'information.

2.6.4 ORG_EXT : Sous-traitant/Fournisseurs/Industriels

Organisation fournissant un service ou des ressources à l'organisme et liée avec lui par contrat.

Société d'infogérance, société d'externalisation, société de conseil.

2.7 SYS : Système

Le type système est constitué de l'ensemble des installations spécifiques liées aux technologies de l'information, avec un objectif particulier et environnement opérationnel. Il est composé de diverses entités appartenant aux autres types décrits ci-avant.

2.7.1 SYS_INT : Dispositif d'accès Internet

Dispositif composant l'interconnexion entre le réseau de l'organisme et le réseau Internet et offrant les services d'accès depuis ou vers l'Internet.

Dispositif de filtrage, DMZ, passerelles.

2.7.2 SYS_MES : Messagerie

Dispositif permettant aux utilisateurs habilités la saisie, la consultation différée et la transmission, sur des ordinateurs connectés en réseau, de documents informatisés ou messages électroniques.

Messagerie interne, messagerie web.

2.7.3 SYS_ITR : Intranet

Données et services informatiques partagées et privé, qui utilise les protocoles de communication et les technologies fédératrices (technologie d'Internet par exemple).

Service d'information interne.

2.7.4 SYS_ANU : Annuaire d'entreprise

Dispositif de gestion et d'accès à une base de données décrivant des personnels de l'entreprise et leurs caractéristiques.

Gestion des droits applicatifs.

2.7.5 SYS_WEB : Portail externe

Un portail externe est un point d'accès qu'un utilisateur trouvera ou utilisera lorsqu'il cherche de l'information ou un service de l'organisme. Les portails fournissent un grand éventail de ressources et de services.

Portail d'information, portail de téléprocédure, site de commerces électroniques.

3 Méthodes d'attaque et éléments menaçants génériques

Le tableau suivant présente les méthodes d'attaque avec leurs principales atteintes sur les critères de sécurité. Les méthodes d'attaque sont classées selon un thème représentatif (elles pourraient néanmoins être placées dans plusieurs thèmes).

Méthodes d'attaque	D	I	C
Thème 1 – Sinistres physiques			
1- INCENDIE	X	X	
2- DÉGÂTS DES EAUX	X	X	
3- POLLUTION	X	X	
4- SINISTRE MAJEUR	X	X	
5- DESTRUCTION DE MATÉRIELS OU DE SUPPORTS	X	X	
Thème 2 – Événements naturels			
6- PHÉNOMÈNE CLIMATIQUE	X	X	
7- PHÉNOMÈNE SISMIQUE	X	X	
8- PHÉNOMÈNE VOLCANIQUE	X	X	
9- PHÉNOMÈNE MÉTÉOROLOGIQUE	X	X	
10- CRUE	X	X	
Thème 3 – Perte de services essentiels			
11- DÉFAILLANCE DE LA CLIMATISATION	X		
12- PERTE D'ALIMENTATION ÉNERGÉTIQUE	X		
13- PERTE DES MOYENS DE TÉLÉCOMMUNICATIONS	X		
Thème 4 – Perturbations dues aux rayonnements			
14- RAYONNEMENTS ÉLECTROMAGNÉTIQUES	X	X	
15- RAYONNEMENTS THERMIQUES	X	X	
16- IMPULSIONS ÉLECTROMAGNÉTIQUES (IEM)	X	X	
Thème 5 – Compromission des informations			
17- INTERCEPTION DE SIGNAUX PARASITES COMPROMETTANTS			X
18- ESPIONNAGE À DISTANCE			X
19- ÉCOUTE PASSIVE			X
20- VOL DE SUPPORTS OU DE DOCUMENTS			X
21- VOL DE MATÉRIELS	X		X
22- RÉCUPÉRATION DE SUPPORTS RECYCLÉS OU MIS AU REBUS			X
23- DIVULGATION			X
24- INFORMATIONS SANS GARANTIE DE L'ORIGINE	X	X	
25- PIÉGEAGE DU MATÉRIEL		X	X
26- PIÉGEAGE DU LOGICIEL	X	X	X
27- GÉOLOCALISATION			X
Thème 6 – Défaillances techniques			
28- PANNE MATÉRIELLE	X	X	
29- DYSFONCTIONNEMENT DU MATÉRIEL	X	X	
30- SATURATION DU SYSTÈME INFORMATIQUE	X		
31- DYSFONCTIONNEMENT LOGICIEL	X	X	
32- ATTEINTE À LA MAINTENABILITÉ DU SYSTÈME D'INFORMATION	X		
Thème 7 – Actions illicites			
33- UTILISATION ILLICITE DES MATÉRIELS	X	X	X
34- COPIE FRAUDULEUSE DE LOGICIELS			X
35- UTILISATION DE LOGICIELS CONTREFAITS OU COPIÉS	X		
36- ALTÉRATION DES DONNÉES		X	X
37-TRAITEMENT ILLICITE DES DONNÉES			X
Thème 8 – Compromission des fonctions			
38- ERREUR D'UTILISATION	X	X	X
39- ABUS DE DROIT	X	X	X
40- USURPATION DE DROIT	X	X	X
41- RENIEMENT D'ACTIONS		X	
42- ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL	X		

Les méthodes d'attaque sont décrites en fonction des éléments menaçants pouvant les exploiter.

Thème 1 – Sinistres physiques

1- INCENDIE

Type	Naturel / Humain / Environnemental.
Cause accidentelle	Concentration de matières inflammables ou explosives dans un environnement confiné, enflammée par un évènement extérieur ou un accident interne.
Exemples	*Foudre, feu de corbeille à papier, court-circuit.*
Cause délibérée	Terroristes, vandales accédant aux biens pour provoquer la mise à feu directement ou indirectement (bombes incendiaires, altération des dispositifs de ventilation …) de matières inflammables ou explosives.
Exemples	*Gréviste accédant à un accès aux locaux (par exemple à travers les fenêtres de la salle informatique) pour y déposer un engin incendiaire.*
Type de conséquences	Destruction du bien. Atteinte à la sécurité des personnes. Pertes financières. Perturbation de fonctionnement interne
Critères de sécurité	Disponibilité / Intégrité.

2- DÉGÂTS DES EAUX

Type	Naturel / Humain / Environnemental.
Cause accidentelle	Inondation due à une fuite ou une rupture de canalisation.
Exemples	*Fuite des équipements de climatisation, fuite provenant d'une salle d'eau située à l'étage supérieur, lance à incendie ouverte.*
Cause délibérée	Terroristes, vandales accédant au bien pour provoquer l'inondation des locaux.
Exemples	*Rupture délibérée de canalisation, déclenchement de systèmes d'extinction ou simplement, arrosage des matériels.*
Type de conséquences	Destruction ou indisponibilité temporaire d'un bien. Pertes financières. Perturbation de fonctionnement interne.
Critères de sécurité	Disponibilité / Intégrité.

3- POLLUTION

Type	Naturel / Humain / Environnemental.
Cause accidentelle	Présence de poussières, de vapeurs, de gaz corrosifs ou toxiques, dans l'air ambiant.
Exemples	*Gaz d'échappement dans une zone de circulation dense.*
Cause délibérée	Pollution volontaire de l'air ambiant en altérant les dispositifs de climatisation ou en déposant une source de pollution dans les locaux.
Exemples	*Accès malveillant et dépose dans les gaines d'aération, de chauffage ou de climatisation de polluant.*
Type de conséquences	Destruction d'un bien. Atteinte à la sécurité des personnes. Disponibilité de personnels opérationnels.
Critères de sécurité	Disponibilité / Intégrité.

4- SINISTRE MAJEUR

Type	Naturel / Environnemental.
Cause accidentelle	Évènement extérieur ou sinistre lié à l'environnement naturel ou industriel proche des biens et pouvant les affecter physiquement de manière très importante.
Exemples	*Explosion de sites industriels situés à proximité, éboulements de terrain, raz-de-marée, chutes d'aéronefs, mobile endommagé ou détruit suite à une collision…*
Cause délibérée	Évènement extérieur ou sinistre lié à une action de vandalisme ou de terrorisme proche des biens et pouvant les affecter physiquement de manière très importante.
Exemples	*Explosion de sites industriels situés à proximité, éboulements de terrain, chutes d'aéronefs, mobile endommagé ou détruit suite à une collision…*
Type de conséquences	Destruction d'un bien. Atteinte à la sécurité des personnes. Pertes financières. Arrêt de fonctionnement.
Critères de sécurité	Disponibilité / Intégrité.

5- DESTRUCTION DE MATÉRIELS OU DE SUPPORTS

Type	Humain.
Cause accidentelle	Négligence ou évènement accidentel provoquant la destruction d'un matériel ou d'un support.
Exemples	*Négligence commise lors du transport du matériel.* *Stockage des supports d'archive dans de mauvaises conditions environnementales.* *Dégâts causés par un animal.* *Renversement de nourriture ou de boisson sur un matériel.*
Cause délibérée	Personne accédant au matériel et provoquant sa destruction.
Exemples	*Destruction d'une machine et de ses sauvegarde (cartouche).*
Type de conséquences	Perte de données. Pertes financières liées à la valeur de l'équipement détruit. Indisponibilité de l'équipement.
Critères de sécurité	Disponibilité / Intégrité.

Thème 2 – Événements naturels

6- PHÉNOMÈNE CLIMATIQUE

Type Naturel.

Cause accidentelle Conditions climatiques particulières (à la limite des caractéristiques de fonctionnement des matériels).

Exemples *Site placé dans une zone géographiquement sensible à une extrême chaleur, de froid, d'humidité, de vent et la sécheresse.*

Type de conséquences Destruction ou arrêt temporaire d'un bien.

Critères de sécurité Disponibilité / Intégrité.

7- PHÉNOMÈNE SISMIQUE

Type Naturel.

Cause accidentelle Secousse ou tremblement de terre provoquant des vibrations extrêmes ou le déclenchement d'un évènement catastrophique (raz de marée).

Exemples *Site abritant le système d'information situé dans une zone géographique dans laquelle des rescousses sont fréquemment ressenties.*

Type de conséquences Destruction d'un bien.
Atteinte à la sécurité des personnes.

Critères de sécurité Disponibilité / Intégrité.

8- PHÉNOMÈNE VOLCANIQUE

Type Naturel.

Cause accidentelle Éruption volcanique provoquant des vibrations ou le déclenchement d'un autre évènement catastrophique (raz de marée).

Exemples *Site abritant le système d'information situé dans une zone géographique réputée volcanique (phénomène intermittent, les phases d'émission alternant avec les phases de sommeil qui peuvent être très longue).*

Type de conséquences Destruction d'un bien.
Atteinte à la sécurité des personnes.

Critères de sécurité Disponibilité / Intégrité.

9- PHÉNOMÈNE MÉTÉOROLOGIQUE

Type Naturel / Humain.

Cause accidentelle Perturbation atmosphérique ponctuelle entraînant des conditions climatiques extrêmes.

Exemples *Tempêtes, ouragans, cyclones, pluie de grêle, foudre, avalanche.*

Cause délibérée Un saboteur accède aux dispositifs de protection contre la foudre.

Exemples *Déconnexion de la mise à la terre, mis en court-circuit des éclateurs, déplacement les dispositifs.*

Type de conséquences Destruction d'un bien.
Atteinte à la sécurité des personnes.

Critères de sécurité Disponibilité / Intégrité.

10- CRUE

Type	Naturel.
Cause accidentelle	Rivière, cours d'eau ou nappe souterraine provoquant une inondation des terrains proches de manière périodique ou exceptionnelle.
Exemples	*Le site peut être situé en zone inondable et subir une inondation d'une rivière proche, ou être plus éloigné mais subir les conséquences de cette inondation (glissement de terrain).*
Type de conséquences	Destruction d'un bien. Atteinte à la sécurité des personnes. Pertes financières.
Critères de sécurité	Disponibilité / Intégrité.

Thème 3 – Perte de services essentiels

11- DÉFAILLANCE DE LA CLIMATISATION

Type Humain / Environnemental.

Cause accidentelle Panne, arrêt ou insuffisance du service de climatisation peut entraîner, pour les biens nécessitant un refroidissement et une ventilation, leur arrêt, des dysfonctionnements voire des pannes.

Exemples *Absence d'entretien de l'équipement de climatisation, mauvais dimensionnement du matériel de climatisation, interruption de l'alimentation en eau par le fournisseur…*

Cause délibérée Une personne peut saboter les éléments nécessaires au fonctionnement du dispositif de climatisation (arrêt de l'alimentation en eau ou en énergie, destruction du dispositif).

Exemples *Arrêt de la climatisation, arrêt de l'alimentation en eau…*

Type de conséquences Altération de biens.
Critères de sécurité Disponibilité.

12- PERTE D'ALIMENTATION ÉNERGÉTIQUE

Type Humain / Environnemental.

Cause accidentelle Panne, arrêt ou mauvais dimensionnement de l'alimentation énergétique des biens provenant soit du service fourni par le fournisseur, soit des dispositifs internes de distribution.

Exemples *Interruption du service EDF pour grèves, dérangements, travaux.*
Défaut ou mauvais dimensionnement de la centrale électrique interne ou du réseau électrique secouru, dans la mesure ou ces installations existent.
Connexion d'équipements de grandes puissances non prévus au réseau secouru, entraînant une insuffisance des équipements de secours.
Défaut de maintenance ou vieillissement des batteries de l'onduleur.
Coupure accidentelle de câbles internes ou externes.
Arrêt de l'alimentation en eau (défaut du fournisseur, anomalie interne telle qu'une négligence).

Cause délibérée Sabotage ou perturbation de l'installation électrique par une personne accédant aux dispositifs (tête de ligne, TGBT, onduleur…).

Exemples *Coupure volontaire des câbles de l'installation EDF, arrêt volontaire de l'alimentation en eau.*

Type de conséquences Interruption temporaire de service électrique, de service de climatisation.
Critères de sécurité Disponibilité.

13- PERTE DES MOYENS DE TÉLÉCOMMUNICATION

Type Humain / Environnemental.

Cause accidentelle Perturbation, arrêt ou mauvais dimensionnement des services de télécommunication (téléphone, accès Internet, réseau Internet).

Exemples *Grèves, évènement extérieur exceptionnel provoquant la saturation des communications.*

Cause délibérée Sabotage ou perturbation de l'installation Télécom par une personne accédant aux dispositifs de télécommunication (tête de ligne, PABX, Répartiteur, câbles extérieurs…).

Exemples *Coupure volontaire des câbles Télécom, destruction d'un central Télécom extérieur, saturation volontaire de la bande passante Télécom.*

Type de conséquences Interruption faible ou longue des services Télécom.
Pertes financières.

Critères de sécurité Disponibilité.

Thème 4 – Perturbations dues aux rayonnements

14- RAYONNEMENTS ÉLECTROMAGNÉTIQUES

Type Humain / Environnemental.

Cause accidentelle Perturbations électromagnétiques liées à un équipement interne ou externe.

Exemples *Radar, antenne radio, centrale électrique, machine d'usinage.*

Cause délibérée Personne utilisant des rayonnements parasites pour brouiller ou saturer les communications, ou perturber le fonctionnement d'appareillage.

Exemples *Brouillage de communication WIFI.*

Type de conséquences Altération d'affichage des écrans cathodiques, brouillage de communication.
Altération, perturbation de fonctionnement.

Critères de sécurité Disponibilité / Intégrité.

15- RAYONNEMENTS THERMIQUES

Type Humain / Naturel / Environnemental.

Cause accidentelle Effet thermique provoqué par un sinistre ou des conditions météorologiques exceptionnelles.

Exemples *Incendie de forêt plaçant les matériels dans des conditions hors de leurs caractéristiques de fonctionnement.*

Cause délibérée Engin provoquant un effet thermique entraînant un dysfonctionnement ou une destruction des matériels.

Exemples *Dépose de déchets nucléaires à proximité du système d'information, explosion thermo-nucléaire.*

Type de conséquences Dysfonctionnement ou la destruction des matériels.
Atteinte à la sécurité des personnes.
Pertes financières.

Critères de sécurité Disponibilité / Intégrité.

16- IMPULSIONS ÉLECTROMAGNÉTIQUES

Type Environnemental.

Cause accidentelle Sinistre provoquant un effet électromagnétique exceptionnel.

Exemples *Accident industriel à proximité du site.*

Cause délibérée Impulsions électromagnétiques d'origine nucléaire.

Exemples *Bombes.*

Type de conséquences Destruction du bien.
Pertes financières.

Critères de sécurité Disponibilité / Intégrité.

Thème 5 – Compromission des informations

17- INTERCEPTION DE SIGNAUX PARASITES COMPROMETTANTS

Type Humain.

Cause délibérée Signaux parasites d'origine électromagnétique émis par les matériels (par conduction sur les câbles d'alimentation électrique ou les fils de masse ou par rayonnement en espace libre).
La capture de ces signaux dépend de la distance à l'équipement visé ou de la possibilité de se connecter aux câblages ou à tout autre conducteur passant à proximité de l'équipement (phénomène de couplage).

Exemples *Espion ou pirate interceptant et enregistrant des signaux électromagnétiques à l'aide de capteurs et de matériel électronique sur les tuyauteries.*
Espion ou pirate interceptant et enregistrant des signaux électromagnétiques provenant du rayonnement de la vidéo d'un poste informatique.

Type de conséquences Divulgation des communications ou des traitements.
Critères de sécurité Confidentialité.

18- ESPIONNAGE A DISTANCE

Type Humain.

Cause délibérée Actions d'un personnel observables à distance.

Exemples *Observation visuelle avec ou sans moyen optique, par exemple observation d'un utilisateur saisissant un code ou un mot de passe sur un clavier.*

Type de conséquences Intrusion.
Usurpation d'identité.
Critères de sécurité Confidentialité.

19- ÉCOUTE PASSIVE

Type Humain.

Cause délibérée Personne étant connectée aux équipements ou aux supports de communication ou placée dans le périmètre de couverture d'émission d'une communication. Elle utilise alors des moyens, qui peuvent être peu coûteux, pour écouter, sauvegarder et analyser les informations qui circulent (voix ou données).

Exemples *L'interception peut porter sur des signaux de type hertzien ou conduits. L'interception se fait alors par des capteurs (une antenne par exemple pour le type hertzien).*
L'interception peut avoir lieu sur des communications infra-rouges.
Dans le cas d'un support filaire, un équipement déjà connecté au réseau (par exemple poste de travail situé sur un réseau local), peut être utilisé pour stocker et analyser les informations qui circulent (par exemple les informations échangées avec un serveur). De nombreux appareils du commerce facilitent les analyses et permettent d'interpréter en temps réel les trames quels que soient les protocoles de communication.

Type de conséquences Divulgation d'information circulant sur un support de communication.
Critères de sécurité Confidentialité.

20- VOL DE SUPPORTS OU DE DOCUMENTS

Type Humain.

Cause délibérée Personne interne ou externe à l'organisme accédant à des supports numériques ou des documents papiers dans le but de voler et d'exploiter les informations qui se trouvent sur ces supports.

Exemples *Vol de disquettes, cd-rom, cartouches, bandes de sauvegarde.*
Vol de dossiers, notes, plans, rapports.
Vol d'éditions laissées temporairement sur des imprimantes situées dans des locaux partagés.
Fouille des corbeilles, des poubelles entreposées sur la voie publique.

Type de conséquences Divulgation d'information (patrimoine, mots de passe…).
Critères de sécurité Confidentialité.

21- VOL DE MATÉRIELS

Type Humain.

Cause délibérée Personne interne ou externe à l'organisme accédant au matériel, placé dans l'organisme ou transporté à l'extérieur, dans un but cupide ou stratégique.

Exemples *Vol de micro-ordinateur portable pour revendre le matériel, vol d'un PDA pour exploiter son contenu.*

Type de conséquences Indisponibilité d'informations et/ou de fonctions (par exemple équipement portable dédié à la maintenance).
Divulgation des informations stockées par l'équipement (par exemple : mots de passe, extrait du patrimoine informationnel).
Pertes financières.
Critères de sécurité Disponibilité / Confidentialité.

22- RÉCUPÉRATION DE SUPPORTS RECYCLÉS OU MIS AU REBUS

Type Humain

Cause accidentelle Récupération de supports électroniques (disques durs, disquettes, cartouches de sauvegarde, clés USB, disquettes ZIP, disques durs amovibles…) ou papier (listing, éditions incomplètes, messages…) destinés au recyclage et contenant des informations récupérables.

Exemple *Recyclage d'ordinateurs dont les disques durs n'ont pas été formatés à destination d'autres utilisateurs du même organisme, d'écoles, d'autres organismes.*
Réutilisation de papiers comme brouillons dans le même organisme ou à l'extérieur.

Cause délibérée Récupération de supports électroniques (disques durs, disquettes, cartouches de sauvegarde, clés USB, disquettes ZIP, disques durs amovibles…) ou papier (listing, éditions incomplètes, messages…) destinés à la destruction et contenant des informations récupérables.

Exemple *Fouille des corbeilles, des poubelles entreposées sur la voie publique.*

Type de conséquences Perte d'image de marque.
Divulgation d'informations.
Critère de sécurité touché Confidentialité.

23- DIVULGATION

Type Humain.

Cause accidentelle Personne interne à l'organisme qui, par négligence, diffuse de l'information à d'autres personnes de l'organisme n'ayant pas le besoin d'en connaître ou à l'extérieur (les conséquences étant généralement plus importantes vis-à-vis de l'extérieur).

Exemples *Erreur de destinataires lors d'envoi de message.*
Réponse à des sollicitations sans vérification de l'origine (demande malveillante de mots de passe).
Non-connaissance des règles de diffusion de l'information, appliquées dans l'organisme.
Négligence commise dans la définition des règles de contrôle d'accès d'informations partagées.
Non-respect des règles élémentaires de discrétion (discussion ou lecture de document dans des lieux publics).

Cause délibérée Personne diffusant consciemment de l'information au sein de l'organisme à d'autres personnes n'ayant pas le besoin d'en connaître ou à l'extérieur (les conséquences étant généralement plus importantes vis-à-vis de l'extérieur).

Exemples *Personne diffusant par messagerie des informations confidentielles par vengeance.*
Personne divulguant de l'information considérant que la détention d'informations sensibles lui donne un certain pouvoir sur les autres.
Diffusion d'informations à un tiers sous pression d'un chantage.
Exploitation financière d'informations industrielles ou commerciales (espionnage industriel).

Type de conséquences Atteinte la vie privée des usagers.
Divulgation de patrimoine informationnel.
Pertes financières.

Critères de sécurité Confidentialité.

24- INFORMATIONS SANS GARANTIE DE L'ORIGINE

Type Humain.

Cause accidentelle Réception et exploitation dans le système d'information de l'organisme de données erronées ou de matériels non adaptés provenant de sources extérieures.

Exemples *Informations provenant d'un forum de discussion.*
Téléchargement de mises à jour sur des sites Internet n'appartenant pas à l'éditeur concerné.
Information reçue sans identification, authentification de son émetteur, par exemple réception de courrier électronique transmis par une identification générique de société (support@société.com).

Cause délibérée Personne transmettant des informations fausses, destinées à être intégrées au système d'information, pour désinformer le destinataire et porter atteinte à la fiabilité du système ou à la validité de ses informations.

Exemples *Transmission de canular (« Hoax ») via la messagerie électronique.*
Personne transmettant des données en se faisant passer pour la source légitime.

Type de conséquences Altération des données voire des traitements.
Consommation de ressource humaine inutile.
Perte de l'image de marque.

Critères de sécurité Disponibilité / Intégrité

25- PIÉGEAGE DU MATÉRIEL

Type Humain.

Cause délibérée Personne ayant accès à un support de communication ou à un équipement pour y déposer un mécanisme d'interception ou de destruction.

Exemples *Insertion d'une carte dans un micro-ordinateur pendant son transport.*
Pose d'un microphone dans un équipement.
Dérivation de circuits de communication voix ou données.
Piégeage d'une fonction d'un matériel de protection pour le rendre inefficace et mener une attaque.

Type de conséquences Divulgation d'information à l'extérieur de l'organisme.
Destruction du matériel pendant un période critique.
Inefficacité d'une fonction de protection.

Critères de sécurité Intégrité / Confidentialité.

26- PIÉGEAGE DU LOGICIEL

Type Humain / Environnemental.

Cause accidentelle Action involontaire effectuée avec des moyens logiciels depuis l'intérieur ou l'extérieur de l'organisme conduisant à l'altération, la destruction de programmes ou de données, porter atteinte au bon fonctionnement de la ressource, voire exécuter des commandes au nom et à l'insu des usagers.

Exemples *Utilisateur connectant au réseau un micro-ordinateur portable infecté par un virus, introduit lors d'un échange avec un autre organisme.*
Usager du système d'information recevant de l'extérieur de l'organisme un ver et le propageant à son insu à l'intérieur de l'organisme.

Cause délibérée L'agresseur introduit un logiciel ou des commandes de manière à modifier le comportement d'un logiciel ou d'ajouter un service illicite à un système d'exploitation. Cet élément menaçant peut agir pendant la phase de conception, de pré-production, de fabrication, d'exploitation, de transport ou de maintenance dans le système d'information.

Exemples *Personne faisant exécuter par un usager un programme en simulant une action licite, mais qui contient des fonctions cachées capables d'entraver la politique de sécurité (cheval de Troie).*
Bombe logique, ajoutée à un programme par le programmeur afin d'y insérer une commande, généralement associée à un déclenchement (date, événement contextuel…) et exécutant une action illicite.

Type de conséquences Intrusion.
Perturbation du fonctionnement.
Destruction de données.
Altération du logiciel.

Critères de sécurité Disponibilité / Intégrité / Confidentialité.

27- GÉOLOCALISATION

Type Humain.

Cause délibérée Personne ayant accès à des moyens permettant de localiser un usager du système d'information.

Exemples *Accès aux registres des entrées/sorties.*
Accès aux demandes de billets.
Utilisation des antennes auxquelles sont connectés les portables lorsqu'ils

fonctionnent afin de localiser une personne.

Type de conséquences Utilisation d'informations pour conduire des attaques ciblées.

Critères de sécurité Confidentialité.

Thème 6 – Défaillances techniques

28- PANNE MATÉRIELLE

Type Humain / Naturel.

Cause accidentelle Évènement provoquant la panne d'un matériel.

Exemples *Usure, vieillissement, défaut de maintenance ou mauvais emploi (par exemple, mauvais dimensionnement, exploitation hors des caractéristiques de fonctionnement) provoquant une panne.*

Type de conséquences Indisponibilité d'un équipement.
Altération ou perte d'informations.

Critères de sécurité Disponibilité / Intégrité.

29- DYSFONCTIONNEMENT DU MATÉRIEL

Type Humain / Naturel.

Cause accidentelle Évènement logique ou physique provoquant des dysfonctionnements d'un matériel.

Exemples *Non-respect des procédures de qualification d'un équipement suite à des mises à jour ou mises à niveau.*
Dégradation involontaire d'un équipement.
Utilisation du matériel dans des conditions hors des caractéristiques de fonctionnement propre à l'équipement (température, humidité…).
Usure, vieillissement d'un matériel.

Type de conséquences Interruption de service d'un équipement qui, par effet de bord, peut conduire à une indisponibilité du système d'information.

Critères de sécurité Disponibilité / Intégrité.

30- SATURATION DU SYSTÈME INFORMATIQUE

Type Humain.

Cause accidentelle Ressource de type matériel, logiciel ou réseau, insuffisante pour faire face aux besoins des utilisateurs.

Exemples *Dépassement des capacités de stockage (par exemple : espace de sauvegarde, stockage des boîtes aux lettres, espace de travail…), par exemple saturation d'une boîte aux lettres lors d'absences prolongées de son propriétaire.*
Saturation liée à la sollicitation intense de la machine (multiples requêtes simultanées à traiter).
Mauvais dimensionnement des équipements (onduleurs, canaux de communication…).

Cause délibérée Personne simulant un besoin de ressource intense en provoquant un parasitage intense et continu de la ressource.

Exemples *Exécution d'un très grand nombre de commandes simultanées.*
Saturation volontaire des espaces de stockage des traces d'activités systèmes ou applicatives en vue de masquer la réalisation d'opérations illicites.

Type de conséquences Arrêt provoquant une indisponibilité temporaire du service.
Perte d'information.

Critères de sécurité Disponibilité.

31- DYSFONCTIONNEMENT LOGICIEL

Type Humain / Environnemental.

Cause accidentelle Erreur de conception, erreur d'installation ou négligence d'exploitation commise lors de modification provoquant une exécution non-conforme.

Exemples *Erreur d'implémentation entraînant un mauvais traitement des données aux bornes.*
Installation de logiciel provoquant des effets de bord.
Non-respect des procédures d'installation ou d'exploitation.
Négligence commise lors d'opérations de maintenance.

Type de conséquences Interruption de service.
Altération de fonctionnement.
Production de données altérées.

Critères de sécurité Disponibilité / Intégrité.

32- ATTEINTE À LA MAINTENABILITÉ DU SYSTÈME D'INFORMATION

Type Humain / Environnemental.

Cause accidentelle Absence de maîtrise du système entraînant toute mise à niveau ou évolution impossible, par exemple pour corriger une anomalie, pour répondre à de nouveaux besoins…

Exemples *Défaillance des fournisseurs des matériels et logiciels.*
Défaillance des sociétés tierces de maintenance logicielles et matérielles, arrêt de contrat de prestation de service entraînant une absence de compétences ou de moyens pour assurer l'évolution du système.
Nombreuses modifications réalisées sur le système le rendant difficile, voire impossible, à maintenir sans risquer de provoquer des effets de bord à la suite d'une modification.

Cause délibérée Personne rendant difficile, voire impossible, toute mise à jour sur le système.

Exemples *Personne qui, par vengeance, ne laisse aucune trace ni d'aide pour maintenir le système (le rendant opaque).*

Type de conséquences Interruption de service prolongée.
Atteinte à la sûreté de fonctionnement.
Pertes financières liées au changement de matériels ou fournisseurs.

Critères de sécurité Disponibilité.

Thème 7 – Actions illicites

33- UTILISATION ILLICITE DES MATÉRIELS

Type Humain.

Cause délibérée Personne interne ou externe à l'organisme accédant au système d'information et utilisant l'un de ses services pour s'y introduire, effectuer des opérations ou voler de l'information.

Exemples *Vol de données d'identification/authentification d'un usager autorisé afin de s'en arranger les droit en contournant les contrôles d'accès,*
accès à des zones protégées à partir d'un accès autorisé en utilisant une faille des mécanismes applicatifs pour contourner les moyens de protection.
Examen et recherche d'informations dans des données résiduelles sur des supports électroniques (fichier de mémoire cache, bribes d'informations résiduelles sur les disques durs, sauvegardes de contexte - points de reprise en cas d'incident - contenant des informations de l'état du système qui peuvent être consultées par un attaquant averti…
Simulation du comportement d'une machine pour tromper un utilisateur légitime et s'emparer de son nom et de son mot de passe.
Modification ou destruction volontaire de données.

Type de conséquences Intrusion dans le système d'information.
Divulgation d'information.

Critères de sécurité Disponibilité / Intégrité / Confidentialité.

34- COPIE FRAUDULEUSE DE LOGICIELS

Type Humain.

Cause délibérée Personne interne à l'organisme faisant des copies pirates (également appelées copies serviles) de progiciels ou de logiciels "maison".

Exemples *Copie de logiciels de l'organisme dans un but ludique, de vengeance (diffusion via l'Internet) ou avide (vente).*

Type de conséquences Pertes financières.
Atteinte à l'image de marque.

Critères de sécurité Confidentialité.

35- UTILISATION DE LOGICIELS CONTREFAITS OU COPIÉS

Type Humain / Environnemental.

Cause accidentelle Perte ou destruction des éléments prouvant l'achat de licences ou négligence commise dans le déploiement de logiciel sans être acquitté des droits correspondant.

Exemples *Sinistre provoquant la destruction des preuves d'achat.*
Impossibilité de constituer un inventaire des licences utilisées.

Cause délibérée Personne interne à l'organisme utilisant un logiciel copié de manière illicite.

Exemples *Copie de logiciels sans licence pour effectuer une tâche licite dans l'organisme.*

Type de conséquences Non-respect de la législation.
Atteinte à l'image de marque.

Critères de sécurité Disponibilité.

36- ALTÉRATION DES DONNÉES

Type Humain.

Cause délibérée Personne accédant aux moyens de communication du système d'information et altérant la transmission des informations (par interception, insertion, destruction…) ou sollicitant ces accès jusqu'à trouver un accès autorisé.

Exemples *La destruction, insertion, modification de messages (modification de l'information ; réagencement de l'information à l'intérieur des messages ou réagencement de la suite des messages).*
Refus de service (décalage dans le temps d'un message).
Balayage depuis l'extérieur des adresses IP jusqu'à trouver une adresse accessible du système d'information.

Type de conséquences Intrusion.
Altération des communications.

Critères de sécurité Intégrité / Confidentialité.

37- TRAITEMENT ILLICITE DES DONNÉES

Type Humain.

Cause délibérée Personne effectuant un traitement d'information non autorisé par la législation ou un règlement.

Exemples *Constitution et utilisation de fichier nominatif non déclaré (exploitation illicite de traces).*
Réalisation d'opérations interdites sur des fichiers nominatifs déclarés tels qu'un rapprochement de plusieurs fichiers.
Chiffrement de données à des fins de confidentialité utilisant des clés longues sans autorisation préalable.
Manipulation illicite de données d'un ordinateur recyclé.

Type de conséquences Atteinte à la vie privée des usagers.
Poursuites judiciaires et pénalités.

Critères de sécurité Confidentialité.

Thème 8 – Compromission des fonctions

38- ERREUR D'UTILISATION

Type Humain.

Cause accidentelle Personne commettant une erreur de manipulation, de saisie, d'utilisation de matériels ou logiciels.

Exemples *Perte de données suite à une erreur dans les opérations de sauvegarde.*
Non-respect des procédures d'installation ou de maintenance.
Saisie par des pupitreurs de nombreuses données chiffrées.
Négligence commise lors du paramétrage d'un logiciel de protection.
Erreur de saisie de l'adresse du destinataire d'un courrier électronique.

Type de conséquences Interruption de service.
Altération des données.
Dysfonctionnement, perte d'efficacité des moyens de protection, introduction de failles supplémentaires.
Divulgation involontaire de données.

Critères de sécurité Disponibilité / Intégrité / Confidentialité.

39- ABUS DE DROIT

Type Humain.

Cause accidentelle Personne possédant des droits privilégiés (administrateur de réseaux, personnel informaticien...) et pouvant modifier les caractéristiques d'exploitation des ressources sans en informer les utilisateurs.

Exemples *Création de nouveaux accès aux systèmes sans tenir compte des besoins de protection des données stockées par les utilisateurs.*
Arrêt de la procédure de sauvegarde sans en informer les utilisateurs.
Modification de paramètres de configuration sur des serveurs provoquant des effets de bord et des dysfonctionnements.

Cause délibérée Personne accédant au système pour modifier, supprimer et ajouter des caractéristiques d'exploitation ou effectuer toute autre opération illicite rendant possible par l'attribution de ces droits

Exemples *Un administrateur change les mots de passe des utilisateurs.*
Un intervenant de maintenance modifie le comportement des mécanismes de sécurité pour accéder à des informations protégées.
Suppression du journal d'événements sur les serveurs d'application.

Type de conséquences Altération de fonctionnement.
Divulgation d'informations.
Perte d'information.

Critères de sécurité Disponibilité / Intégrité / Confidentialité.

40- USURPATION DE DROIT

Type Humain.

Cause délibérée Personne se faisant passer pour une autre de manière à utiliser ces privilèges d'accès au système d'information, désinformer le destinataire, réaliser une fraude…

Exemples *Personne se faisant passer pour un usager et demandant à l'administrateur le recouvrement de son accès suite à une perte de mot de passe.*
Personne se substituant à un utilisateur en utilisant une session laissée

ouverte par ce dernier.

Type de conséquences Intrusion.

Critères de sécurité Disponibilité / Intégrité / Confidentialité.

41- RENIEMENT D'ACTIONS

Type Humain.

Cause délibérée Une personne ou une entité renie sa participation à un échange avec un tiers ou à la réalisation d'une opération.

Exemples *Personne niant avoir reçu ou émis un message déterminé, ou présentant avoir émis (reçu) un message (fichier) différent, ou prétendant ne jamais avoir réaliser une opération.*

Type de conséquences Absence de preuve.

Critères de sécurité Intégrité.

42- ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL

Type Humain / Environnemental.

Cause accidentelle Absence de personnel qualifié ou habilité suite à empêchement indépendant de la volonté des personnes.

Exemples *Maladie, décès, grève de transport.*

Cause délibérée Absence volontaire de personnel qualifié ou habilité.

Exemples *Grèves, congés non avisés par l'organisme.*

Type de conséquences Arrêt, perturbation de service.

Critères de sécurité Disponibilité.

4 Vulnérabilités génériques

Les vulnérabilités sont présentées par type d'entités et méthode d'attaque (MA). Les sous-types d'entités héritent des vulnérabilités de leur type d'entités.

4.1 MAT : Matériel

Type d'entités	MA	Vulnérabilité
MAT	6	Conditions d'utilisation dépassant les caractéristiques de fonctionnement des matériels
MAT	9	Conditions d'utilisation dépassant les caractéristiques de fonctionnement des matériels
MAT	17	Matériel susceptible d'émettre des rayonnements parasites compromettants
MAT	17	Absence de prise en compte du zonage des matériels
MAT	17	Absence de prise en compte des règles d'installation
MAT	28	Mauvaises conditions d'utilisation
MAT	28	Absence de protection contre les perturbations électriques
MAT	29	Absence de protection contre les perturbations électriques
MAT	29	Mauvaises conditions d'utilisation
MAT	30	Mauvais dimensionnement des ressources (ex: manque d'autonomie d'une batterie de portable)
MAT	38	Mauvaises conditions d'utilisation
MAT	38	Matériel d'utilisation complexe ou peu ergonomique
MAT	38	Absence de support à l'utilisateur accessible

4.1.1 MAT_ACT : Support de traitement de données (actif)

Type d'entités	MA	Vulnérabilité
MAT_ACT	1	Absence de matériels de remplacement
MAT_ACT	1	Matériel utilisant des matériaux inflammables (ex. : imprimantes de masse provoquant des poussières)
MAT_ACT	2	Absence de matériels de remplacement
MAT_ACT	4	Absence de matériels de remplacement
MAT_ACT	5	Absence de matériels de remplacement
MAT_ACT	5	Fragilité des matériels
MAT_ACT	5	Matériel accessible à des personnes autres que leurs propriétaires (ex: placé dans un lieu de passage)
MAT_ACT	7	Matériel sensible aux vibrations
MAT_ACT	12	Matériel sensible aux perturbations électrique (chutes de tension, surtensions, micro-coupure)
MAT_ACT	13	Matériel maintenu à distance par des moyens de télécommunication
MAT_ACT	19	Accès logique au matériel permettant la pose d'un logiciel d'écoute
MAT_ACT	19	Matériel disposant d'interface de communication écoutable (infra rouge, 802.11, Bluetooth…)
MAT_ACT	20	Absence d'inventaire du matériel
MAT_ACT	20	Matériels attractifs (valeurs marchande, technologique, stratégique)
MAT_ACT	21	Absence de matériels de remplacement
MAT_ACT	24	Absence de moyens permettant de garantir la provenance d'un matériel
MAT_ACT	25	Possibilité de pose d'éléments matériels additionnels pour stocker, transmettre ou altérer (ex: keylogger physique)
MAT_ACT	28	Vieillissement du matériel
MAT_ACT	28	Mauvaise fiabilité des matériels
MAT_ACT	28	Défaut de maintenance
MAT_ACT	29	Mauvaise fiabilité des matériels
MAT_ACT	29	Possibilité d'incompatibilité entre les différents matériels

Type d'entités	MA	Vulnérabilité
MAT_ACT	32	Matériels obsolètes
MAT_ACT	32	Absence de moyens de support accessible depuis l'extérieur de l'organisme ou depuis un pays dont le décalage horaire est important
MAT_ACT	32	Matériels à configurations non évolutives
MAT_ACT	32	Matériels spécifiques
MAT_ACT	33	Le matériel utilisé permet un autre usage que celui qui est prévu (développement de logiciels non destinés à l'organisme…)
MAT_ACT	33	Le matériel est connecté à des réseaux externes
MAT_ACT	38	Absence de responsabilité
MAT_ACT	38	Possibilité que certains matériels provoquent des nuisances pour le personnel utilisateur (travail devant écran, ondes...)
MAT_ACT	38	Insuffisance de compétence pour l'utilisateur
MAT_ACT	39	Absence de protection physique
MAT_ACT	40	Le matériel est connecté à des réseaux externes
MAT_ACT	41	Absence de dispositif de traces et d'audit
MAT_ACT	41	Le matériel est accessible et utilisable par tous
MAT_ACT	42	Possibilité que certains matériels provoquent des nuisances pour le personnel utilisateur (travail devant écran, ondes...)

4.1.1.1 MAT_ACT.1 : Matériel transportable

Type d'entités	MA	Vulnérabilité
MAT_ACT.1	18	Écran observable depuis l'extérieur
MAT_ACT.1	20	Disque dur facilement démontable
MAT_ACT.1	20	Absence de protection des matériels contre le vol (câble anti-vol)
MAT_ACT.1	20	Matériel en libre-service utilisable par un groupe de personnes
MAT_ACT.1	21	Absence d'inventaire du matériel
MAT_ACT.1	21	Matériels attractifs (valeurs marchande, technologique, stratégique)
MAT_ACT.1	21	Matériel en libre-service utilisable par un groupe de personnes
MAT_ACT.1	21	Revente possible du matériel (absence de marquage, utilisation sans mot de passe)
MAT_ACT.1	22	Présence de données résiduelles à l'insu de l'utilisateur de matériels ré-attribués ou mis au rebut
MAT_ACT.1	26	Le matériel est amorçable par tous à partir d'un périphérique (ex. : disquette, cédérom)
MAT_ACT.1	27	Matériel localisable (ex: triangularisation)
MAT_ACT.1	34	Matériel permettant l'enregistrement de données sur support (disquette, ZIP, graveur CD/DVD)
MAT_ACT.1	34	Absence de gestion des privilèges des profils (administrateurs, utilisateurs, invité...)
MAT_ACT.1	36	Matériels obsolètes
MAT_ACT.1	36	Absence de règles de protection des données
MAT_ACT.1	36	Le matériel est amorçable par tous à partir d'un périphérique (ex. : disquette, cédérom)
MAT_ACT.1	39	Absence de dispositif de contrôle d'accès robuste
MAT_ACT.1	40	Absence de dispositif de contrôle d'accès robuste

4.1.1.2 MAT_ACT.2 : Matériel fixe

Type d'entités	MA	Vulnérabilité
MAT_ACT.2	11	Matériel nécessitant une climatisation pour fonctionner
MAT_ACT.2	14	Matériel ou support sensible aux rayonnements électromagnétiques ou thermiques
MAT_ACT.2	15	Matériel ou support sensible aux rayonnements électromagnétiques ou thermiques
MAT_ACT.2	16	Matériel ou support sensible aux rayonnements électromagnétiques ou thermiques
MAT_ACT.2	18	Écran observable depuis l'extérieur
MAT_ACT.2	20	Disque dur facilement démontable
MAT_ACT.2	21	Matériel facilement démontable
MAT_ACT.2	22	Présence de données résiduelles à l'insu de l'utilisateur de matériels ré-attribués ou

Type d'entités	MA	Vulnérabilité
		mis au rebut
MAT_ACT.2	23	Fonctions de gestion des droits d'accès trop compliquées à utiliser et pouvant être source d'erreur
MAT_ACT.2	23	Présence de répertoire partagé pour stocker de l'information
MAT_ACT.2	23	Procédures de gestion des privilèges d'accès trop lourde à opérer
MAT_ACT.2	23	Absence de vérification des accès partagés accordés
MAT_ACT.2	26	Le matériel est amorçable par tous à partir d'un périphérique (ex. : disquette, cédérom)
MAT_ACT.2	34	Absence de gestion des privilèges des profils (administrateurs, utilisateurs, invité...)
MAT_ACT.2	34	Matériel permettant l'enregistrement de données sur support (disquette, ZIP, graveur cédérom/DVD)
MAT_ACT.2	36	Le matériel est amorçable par tous à partir d'un périphérique (ex. : disquette, cédérom)
MAT_ACT.2	36	Matériels obsolètes
MAT_ACT.2	36	Absence de règles de protection des données
MAT_ACT.2	36	Absence de redondance ou procédure de sauvegarde
MAT_ACT.2	39	Absence de dispositif de contrôle d'accès robuste
MAT_ACT.2	40	Absence de dispositif de contrôle d'accès robuste

4.1.1.3 MAT_ACT.3 : Périphérique de traitement

Type d'entités	MA	Vulnérabilité
MAT_ACT.3	11	Matériel nécessitant une climatisation pour fonctionner
MAT_ACT.3	20	Absence de protection d'accès aux équipements de sauvegarde
MAT_ACT.3	20	Présence d'imprimante dans les lieux de passage
MAT_ACT.3	21	Absence d'inventaire du matériel
MAT_ACT.3	21	Matériels attractifs (valeurs marchande, technologique, stratégique)
MAT_ACT.3	36	Usure des supports
MAT_ACT.3	36	Absence de moyens de protection et de contrôle de l'intégrité des données
MAT_ACT.3	37	Absence de protection physique
MAT_ACT.3	40	Absence de cloisonnement des équipements

4.1.2 MAT_PAS : Support de données (passif)

Type d'entités	MA	Vulnérabilité
MAT_PAS	3	Support sensible aux conditions de conservation
MAT_PAS	5	Support accessible à des personnes autres que leurs propriétaires
MAT_PAS	5	Absence de procédure d'archivage
MAT_PAS	5	Fragilité des supports
MAT_PAS	5	Absence de mesures de conservation des archives adaptées aux délais de rétention (vieillissement des bandes, usure du cédérom)
MAT_PAS	20	Les supports sont accessibles par tous
MAT_PAS	20	Transmission des supports par des services postaux (fournisseurs externes, courrier interne...)
MAT_PAS	20	Absence de protection du stockage des supports
MAT_PAS	22	Absence de moyens de destruction des supports
MAT_PAS	23	Supports capables d'effectuer des échanges d'information à caractère sensible
MAT_PAS	33	Les supports sont accessibles par tous
MAT_PAS	36	Usure des supports
MAT_PAS	36	Absence de moyens de protection et de contrôle de l'intégrité des données
MAT_PAS	37	Absence de moyen d'identification de la sensibilité des informations contenues sur les supports
MAT_PAS	37	Les supports sont accessibles par tous
MAT_PAS	37	Supports attractifs (valeurs marchande, technologique, stratégique)
MAT_PAS	37	Supports mobiles ou aisément transportables (ex. : disquette, ZIP, disque dur

Type d'entités	MA	Vulnérabilité
		extractible)
MAT_PAS	38	Absence de labellisation des supports
MAT_PAS	41	Les supports sont accessibles par tous
MAT_PAS	42	Absence de procédure d'archivage

4.1.2.1 MAT_PAS.1 : Support électronique

Type d'entités	MA	Vulnérabilité
MAT_PAS.1	1	Absence de sauvegarde des données contenues sur les supports
MAT_PAS.1	2	Absence de sauvegarde des données contenues sur les supports
MAT_PAS.1	4	Absence de sauvegarde des données contenues sur les supports
MAT_PAS.1	5	Absence de sauvegarde des données contenues sur les supports
MAT_PAS.1	11	Archives nécessitant une climatisation pour leur conservation
MAT_PAS.1	20	Absence d'inventaire des supports utilisés
MAT_PAS.1	20	Absence de sauvegarde des données contenues sur les supports
MAT_PAS.1	20	Supports aisément transportables (ex: disque dur extractible, cartouche de sauvegarde)
MAT_PAS.1	22	Présence de données résiduelles à l'insu de l'utilisateur de matériels ré-attribués ou mis au rebut
MAT_PAS.1	26	Absence de moyens permettant le contrôle d'innocuité des supports lors de leurs entrées dans l'organisme
MAT_PAS.1	28	Support non adapté à la durée de vie des données à archiver
MAT_PAS.1	28	Mauvaise condition de stockage
MAT_PAS.1	29	Support non adapté à la durée de vie des données à archiver
MAT_PAS.1	29	Mauvaise condition de stockage
MAT_PAS.1	30	Persistance involontaire des données sur les supports
MAT_PAS.1	32	Modification des équipements, des logiciels ou des procédures de sauvegarde sans prise en compte des anciennes sauvegardes ou archives
MAT_PAS.1	32	Support obsolète
MAT_PAS.1	37	Absence de moyen de chiffrement
MAT_PAS.1	37	Absence de procédure et moyen de destruction
MAT_PAS.1	38	Supports d'utilisation complexe ou peu ergonomique
MAT_PAS.1	38	Insuffisance de compétence pour l'utilisateur
MAT_PAS.1	38	Absence de responsabilité
MAT_PAS.1	39	Absence de protection physique
MAT_PAS.1	40	Absence de protection des supports

4.1.2.2 MAT_PAS.2 : Autres supports

Type d'entités	MA	Vulnérabilité
MAT_PAS.2	1	Supports originaux
MAT_PAS.2	2	Supports originaux
MAT_PAS.2	4	Supports originaux
MAT_PAS.2	5	Supports originaux
MAT_PAS.2	11	Archives nécessitant une climatisation pour leur conservation
MAT_PAS.2	18	Lecture de documents sensibles dans des lieux publics (observation des documents par des personnes extérieures…)
MAT_PAS.2	20	Supports originaux
MAT_PAS.2	32	Perte ou mauvaise gestion des documents originaux (contrats de support, licences…)
MAT_PAS.2	39	Absence d'audit des procédures de contrôle d'accès physique
MAT_PAS.2	40	Absence d'audit des procédures de contrôle d'accès physique
MAT_PAS.2	41	Absence de procédure d'accès à l'information classifiée

4.2 LOG : Logiciel

Type d'entités	MA	Vulnérabilité
LOG	18	Absence de dispositif de protège écran en cas d'inactivité
LOG	18	Utilisation de mots de passe d'accès au système ou à l'application simples à observer (forme sur un clavier, mot de passe court)
LOG	18	Pas ou peu de changement de mot de passe d'accès au système ou à l'application
LOG	19	Absence de dispositif de contrôle d'accès en cas d'inactivité
LOG	19	Possibilité d'ajout d'un logiciel d'écoute de type cheval de Troie
LOG	22	Présence de données résiduelles utilisées par les logiciels
LOG	23	Absence de vérification des accès partagés accordés
LOG	23	Procédures de gestion des privilèges d'accès trop lourde à opérer
LOG	24	Récupération de logiciels depuis un moyen de collecte non authentifié
LOG	24	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…
LOG	26	La liaison de télémaintenance est activée en permanence
LOG	26	Possibilité d'existence de fonctions cachées introduites en phase de conception et développement
LOG	30	Absence de filtre protégeant le système contre un engorgement
LOG	30	Consommation inutile de ressources
LOG	30	Application nécessitant des ressources informatiques non adaptée au matériel (ex.: manque de mémoire vive)
LOG	30	Absence de prise en compte dans la définition des exigences d'un projet des situations particulières plaçant le système dans des conditions aux limites
LOG	30	Absence de qualification des développements dans un contexte représentatif de l'exploitation
LOG	31	Possibles effets de bord liés à la mise à jour d'un composant logiciel
LOG	31	Absence de conservation des traces des traitements
LOG	31	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels
LOG	31	Absence de procédure de maintenance
LOG	31	Absence de procédure de qualification avant toute installation ou mise à jour
LOG	31	Absence de procédure de synchronisation des horloges
LOG	31	Absence de remontée d'information pour le traitement centralisé des dysfonctionnements
LOG	31	Possibilité de mal configurer, installer ou modifier le système d'exploitation
LOG	31	Absence de compte rendu des opérations de maintenance
LOG	31	Absence ou erreur de gestion en configuration des composants logiciels (ex: application d'un patch UK non adapté à une version FR)
LOG	32	Aucune vérification des applicatifs n'est faite avant l'installation
LOG	32	Absence de procédure de secours
LOG	32	Absence de procédure de retour arrière en cas d'anomalie lors d'une modification
LOG	32	Absence de procédure de maintenance
LOG	32	Absence de documentation à jour
LOG	32	Absence de compte rendu des opérations de maintenance
LOG	32	Absence de conservation des traces des traitements et des modifications
LOG	32	Logiciels spécifiques
LOG	32	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels
LOG	32	Logiciels obsolètes
LOG	32	Logiciels à configurations non évolutives
LOG	33	Absence de gestion de licence, de dispositif d'enregistrement et d'activation
LOG	33	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation
LOG	34	Absence de gestion des privilèges des profils (administrateurs, utilisateurs, invité...)
LOG	34	Absence de gestion de licence, de dispositif d'enregistrement et d'activation
LOG	36	Absence de contrôle de l'intégrité des données
LOG	36	Absence de procédure et de dispositif d'habilitation à la modification des données

Type d'entités	MA	Vulnérabilité
LOG	39	Absence de politique d'audit
LOG	40	Absence de politique d'audit
LOG	41	Absence de politique d'audit

4.2.1 LOG_OS : Système d'exploitation

Type d'entités	MA	Vulnérabilité
LOG_OS	1	Exemplaire unique des contrats de licence
LOG_OS	2	Exemplaire unique des contrats de licence
LOG_OS	3	Exemplaire unique des contrats de licence
LOG_OS	4	Exemplaire unique des contrats de licence
LOG_OS	5	Exemplaire unique des contrats de licence
LOG_OS	19	Pas ou peu de changement de mot de passe d'accès au système ou à l'application
LOG_OS	19	Absence de protection contre l'usage de privilèges avancés
LOG_OS	26	Possibilité de créer ou modifier des commandes systèmes
LOG_OS	26	Récupération de logiciels depuis un moyen de collecte non authentifié
LOG_OS	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés
LOG_OS	26	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels
LOG_OS	26	Insuffisance de la complexité des mots de passe de connexion
LOG_OS	26	Possibilité d'installer des correctifs, mises à jours, patches, hotfixes…
LOG_OS	26	Possibilité d'administrer le système à distance
LOG_OS	26	Utilisation d'un système d'exploitation standard pour lequel des attaques logiques ont déjà été réalisées
LOG_OS	26	Possibilité d'administrer le système à distance depuis n'importe quel poste
LOG_OS	26	Possibilité d'effacer, de modifier ou d'installer des nouveaux programmes
LOG_OS	26	La couche SNMP est activée
LOG_OS	28	Absence de fonction de diagnostic pour la prévention des pannes matérielles
LOG_OS	29	Absence de fonction de diagnostic pour la prévention des pannes matérielles
LOG_OS	31	Aucune vérification des applicatifs n'est faite avant l'installation
LOG_OS	31	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs
LOG_OS	33	Le partage des ressources facilite l'utilisation du système par des personnes non autorisées
LOG_OS	34	Possibilité de copier facilement les distributions des systèmes d'exploitation propriétaires
LOG_OS	34	Système d'exploitation attractifs ou "grand public"
LOG_OS	35	Possibilité que les systèmes fonctionnent avec des systèmes d'exploitation copiés illicitement ou contrefaits
LOG_OS	36	La liaison de télémaintenance est activée en permanence
LOG_OS	36	Absence de restriction sur les points d'entrée dans le logiciel
LOG_OS	36	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels
LOG_OS	36	Possibilité d'administrer le système à distance depuis n'importe quel poste
LOG_OS	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés
LOG_OS	36	Le système d'exploitation permet d'accéder à des données (base de données…)
LOG_OS	36	Insuffisance de la complexité des mots de passe de connexion
LOG_OS	36	Aucune vérification du système d'exploitation n'est faite avant l'installation
LOG_OS	36	Le partage des ressources facilite l'utilisation du système par des personnes non autorisées
LOG_OS	36	Possibilité d'administrer le système à distance
LOG_OS	36	La couche SNMP est activée
LOG_OS	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation

Type d'entités	MA	Vulnérabilité
LOG_OS	37	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)
LOG_OS	37	Absence de dispositif de chiffrement
LOG_OS	38	Utilisation non intuitive du logiciel
LOG_OS	38	Insuffisance de compétence
LOG_OS	38	Absence de support accessible
LOG_OS	38	Absence de formation à l'utilisation et la maintenance des nouveaux logiciels
LOG_OS	39	Fichiers d'imputation complexes ou peu ergonomiques
LOG_OS	39	Insuffisance de la complexité des mots de passe de connexion
LOG_OS	39	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés
LOG_OS	39	La base de mots de passe du système d'exploitation est déchiffrable
LOG_OS	39	La couche SNMP est activée
LOG_OS	39	Possibilité que le système d'exploitation soit soumis à des requêtes ou données mal formées (ex: buffer overflow)
LOG_OS	39	La liaison de télémaintenance est activée en permanence
LOG_OS	39	Possibilité d'administrer le système à distance
LOG_OS	39	Les logs ou journaux du système d'exploitation sont modifiables par tous
LOG_OS	39	Le partage des ressources facilite l'utilisation du système par des personnes non autorisées
LOG_OS	39	Le système d'exploitation est accessible et utilisable par tous (ex: connexion sur le compte "invité")
LOG_OS	39	Le système d'exploitation ne journalise pas les logs ou les événements systèmes
LOG_OS	39	Le système d'exploitation permet l'établissement de connexions anonymes
LOG_OS	39	Le système d'exploitation permet l'ouverture de session sans mot de passe
LOG_OS	39	Possibilité d'administrer le système à distance depuis n'importe quel poste
LOG_OS	39	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs
LOG_OS	39	Les mots de passe saisis pour accéder au système d'exploitation sont déchiffrables
LOG_OS	39	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)
LOG_OS	40	Les logs ou journaux du système d'exploitation sont modifiables par tous
LOG_OS	40	Le système d'exploitation permet l'ouverture de session sans mot de passe
LOG_OS	40	Le système d'exploitation permet l'établissement de connexions anonymes
LOG_OS	40	Le système d'exploitation ne journalise pas les logs ou les événements systèmes
LOG_OS	40	Le système d'exploitation est accessible et utilisable par tous (ex: connexion sur le compte "invité")
LOG_OS	40	Le partage des ressources facilite l'utilisation du système par des personnes non autorisées
LOG_OS	40	La base de mots de passe du système d'exploitation est déchiffrable
LOG_OS	40	La couche SNMP est activée
LOG_OS	40	Fichiers d'imputation complexes ou peu ergonomiques
LOG_OS	40	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés
LOG_OS	40	Possibilité d'administrer le système à distance
LOG_OS	40	La liaison de télémaintenance est activée en permanence
LOG_OS	40	Les mots de passe saisis pour accéder au système d'exploitation sont déchiffrables
LOG_OS	40	Insuffisance de la complexité des mots de passe de connexion
LOG_OS	40	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs
LOG_OS	40	Possibilité que le système d'exploitation soit soumis à des requêtes ou données mal formées (ex: buffer overflow)
LOG_OS	40	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)
LOG_OS	40	Possibilité d'administrer le système à distance depuis n'importe quel poste
LOG_OS	41	Le système d'exploitation ne journalise pas les logs ou les événements systèmes
LOG_OS	41	La couche SNMP est activée

Type d'entités	MA	Vulnérabilité
LOG_OS	41	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés
LOG_OS	41	Fichiers d'imputation complexes ou peu ergonomiques
LOG_OS	41	Insuffisance de la complexité des mots de passe de connexion
LOG_OS	41	Les mots de passe saisis pour accéder au système d'exploitation sont déchiffrables
LOG_OS	41	La base de mots de passe du système d'exploitation est déchiffrable
LOG_OS	41	Le système d'exploitation permet l'établissement de connexions anonymes
LOG_OS	41	Possibilité que le système d'exploitation soit soumis à des requêtes ou données mal formées (ex: buffer overflow)
LOG_OS	41	Possibilité d'administrer le système à distance depuis n'importe quel poste
LOG_OS	41	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs
LOG_OS	41	Le système d'exploitation est accessible et utilisable par tous (ex: connexion sur le compte "invité")
LOG_OS	41	Possibilité d'administrer le système à distance
LOG_OS	41	Les logs ou journaux du système d'exploitation sont modifiables par tous
LOG_OS	41	Possibilité d'amorcer plusieurs systèmes d'exploitation sur la même machine (ex: accès aux partitions NTFS via Linux)
LOG_OS	41	Le système d'exploitation permet l'ouverture de session sans mot de passe
LOG_OS	41	La liaison de télémaintenance est activée en permanence
LOG_OS	41	Le partage des ressources facilite l'utilisation du système par des personnes non autorisées

4.2.2 LOG_SRV : Logiciel de service, maintenance ou administration

Type d'entités	MA	Vulnérabilité
LOG_SRV	1	Exemplaire unique des contrats de licence
LOG_SRV	2	Exemplaire unique des contrats de licence
LOG_SRV	3	Exemplaire unique des contrats de licence
LOG_SRV	4	Exemplaire unique des contrats de licence
LOG_SRV	5	Exemplaire unique des contrats de licence
LOG_SRV	19	Pas ou peu de changement de mot de passe d'accès aux logiciels de support
LOG_SRV	24	Absence de conservation des traces des activités
LOG_SRV	24	Absence de moyen sûr d'identification
LOG_SRV	26	Absence de protection contre l'usage de privilèges avancés
LOG_SRV	26	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels
LOG_SRV	26	Possibilité de modifier, d'altérer le logiciel
LOG_SRV	26	Utilisation de logiciels non évalués
LOG_SRV	28	Absence de fonction de diagnostic pour la prévention des pannes matérielles
LOG_SRV	29	Absence de fonction de diagnostic pour la prévention des pannes matérielles
LOG_SRV	31	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs
LOG_SRV	31	Aucune vérification des applicatifs n'est faite avant l'installation
LOG_SRV	33	Utilisation partagée d'identifiant de connexion
LOG_SRV	34	Logiciels attractifs ou "grand public"
LOG_SRV	34	Possibilité de copier facilement des logiciels ou progiciels
LOG_SRV	35	Possibilité de copier facilement des logiciels ou progiciels
LOG_SRV	35	Logiciels attractifs ou "grand public"
LOG_SRV	35	Absence de gestion de licence, de dispositif d'enregistrement et d'activation
LOG_SRV	36	Le logiciel permet d'accéder à des données (contenu du disque dur, base de données…)
LOG_SRV	36	Aucune vérification des applicatifs n'est faite avant l'installation
LOG_SRV	36	La liaison de télémaintenance est activée en permanence
LOG_SRV	36	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels
LOG_SRV	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de troie dans le système

Type d'entités	MA	Vulnérabilité
		d'exploitation
LOG_SRV	37	Absence de dispositif de chiffrement
LOG_SRV	37	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)
LOG_SRV	38	Insuffisance de compétence pour l'utilisateur
LOG_SRV	38	Logiciel d'utilisation complexe
LOG_SRV	38	Absence de support à l'utilisateur accessible
LOG_SRV	38	Absence de responsabilité
LOG_SRV	39	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)
LOG_SRV	39	Absence de journalisation des événements
LOG_SRV	39	Absence de sauvegarde des journaux d'événements
LOG_SRV	40	Absence de sauvegarde des journaux d'événements
LOG_SRV	40	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)
LOG_SRV	40	Absence de journalisation des événements
LOG_SRV	41	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)
LOG_SRV	41	Absence de sauvegarde des journaux d'événements
LOG_SRV	41	Absence de journalisation des événements

4.2.3 LOG_STD : Progiciel ou logiciel standard

Type d'entités	MA	Vulnérabilité
LOG_STD	1	Applications uniques développées en interne
LOG_STD	1	Exemplaire unique des contrats de licence
LOG_STD	2	Applications uniques développées en interne
LOG_STD	2	Exemplaire unique des contrats de licence
LOG_STD	3	Applications uniques développées en interne
LOG_STD	3	Exemplaire unique des contrats de licence
LOG_STD	4	Applications uniques développées en interne
LOG_STD	4	Exemplaire unique des contrats de licence
LOG_STD	5	Applications uniques développées en interne
LOG_STD	5	Exemplaire unique des contrats de licence
LOG_STD	19	Absence de protection des journaux récoltant la trace des activités
LOG_STD	19	Pas ou peu de changement de mot de passe d'accès au système ou à l'application
LOG_STD	24	Absence de moyen sûr d'identification
LOG_STD	24	Absence de conservation des traces des activités
LOG_STD	26	Absence de protection contre l'usage de privilèges avancés
LOG_STD	26	Utilisation de logiciels non évalués
LOG_STD	26	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels
LOG_STD	26	Possibilité de modifier, d'altérer le logiciel
LOG_STD	31	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs
LOG_STD	31	Aucune vérification des applicatifs n'est faite avant l'installation
LOG_STD	33	Utilisation partagée d'identifiant de connexion
LOG_STD	34	Logiciels attractifs ou "grand public"
LOG_STD	34	Possibilité de copier facilement des logiciels ou progiciels
LOG_STD	35	Absence de gestion de licence, de dispositif d'enregistrement et d'activation
LOG_STD	35	Possibilité de copier facilement des logiciels ou progiciels
LOG_STD	35	Logiciels attractifs ou "grand public"
LOG_STD	36	Absence de restriction sur les points d'entrée dans le logiciel
LOG_STD	36	Absence de restriction sur les points d'entrée dans le logiciel
LOG_STD	36	Aucune vérification des applicatifs n'est faite avant l'installation

Type d'entités	MA	Vulnérabilité
LOG_STD	36	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels
LOG_STD	36	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels
LOG_STD	36	Le logiciel permet d'accéder à des données (contenu du disque dur, base de données…)
LOG_STD	36	La liaison de télémaintenance est activée en permanence
LOG_STD	37	Absence de dispositif de chiffrement
LOG_STD	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation
LOG_STD	37	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)
LOG_STD	38	Insuffisance de compétence pour l'utilisateur
LOG_STD	38	Absence de support à l'utilisateur accessible
LOG_STD	38	Absence de responsabilité
LOG_STD	38	Logiciel d'utilisation complexe
LOG_STD	39	Absence de sauvegarde des journaux d'événements
LOG_STD	39	Possibilité que le système d'exploitation soit soumis à des requêtes ou données mal formées (ex: buffer overflow)
LOG_STD	39	Absence de journalisation des événements
LOG_STD	40	Possibilité que le système d'exploitation soit soumis à des requêtes ou données mal formées (ex: buffer overflow)
LOG_STD	40	Absence de journalisation des événements
LOG_STD	40	Absence de sauvegarde des journaux d'événements
LOG_STD	41	Absence de sauvegarde des journaux d'événements
LOG_STD	41	Absence de journalisation des événements
LOG_STD	41	Possibilité que le système d'exploitation soit soumis à des requêtes ou données mal formées (ex: buffer overflow)

4.2.4 LOG_APP : Application métier

Type d'entités	MA	Vulnérabilité
LOG_APP	19	Absence de protection des journaux récoltant la trace des activités
LOG_APP	24	Absence de moyen sûr d'identification
LOG_APP	24	Absence de conservation des traces des activités
LOG_APP	26	Possibilité de modifier, d'altérer le logiciel
LOG_APP	26	Absence de protection contre l'usage de privilèges avancés
LOG_APP	26	Utilisation de logiciels non évalués
LOG_APP	26	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels
LOG_APP	31	Absence de documentation à jour
LOG_APP	33	Utilisation partagée d'identifiant de connexion
LOG_APP	34	Logiciels attractifs ou "grand public"
LOG_APP	34	Possibilité de copier facilement des logiciels ou progiciels
LOG_APP	35	Absence de gestion de licence, de dispositif d'enregistrement et d'activation
LOG_APP	35	Possibilité de copier facilement des logiciels ou progiciels
LOG_APP	35	Logiciels attractifs ou "grand public"
LOG_APP	36	La liaison de télémaintenance est activée en permanence
LOG_APP	36	Absence de restriction sur les points d'entrée dans le logiciel
LOG_APP	36	Aucune vérification des applicatifs n'est faite avant l'installation
LOG_APP	36	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels
LOG_APP	36	Absence de restriction sur les points d'entrée dans le logiciel
LOG_APP	36	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels

Type d'entités	MA	Vulnérabilité
LOG_APP	36	Le logiciel permet d'accéder à des données (contenu du disque dur, base de données…)
LOG_APP	37	Logiciel utilisable par tous (ex: absence de mot de passe requis pour l'administration distante d'un poste)
LOG_APP	37	Absence de dispositif de chiffrement
LOG_APP	37	Possibilité d'utiliser une porte dérobée (trappe) ou cheval de Troie dans le système d'exploitation
LOG_APP	38	Absence de documentation explicite sur les systèmes applicatifs
LOG_APP	38	Insuffisance de compétence pour l'utilisateur
LOG_APP	38	Absence de procédure de tests et de réception conforme aux spécifications
LOG_APP	38	Absence de validation des données d'entrées (de saisie)
LOG_APP	38	Absence de responsabilité
LOG_APP	38	Application d'utilisation complexe
LOG_APP	38	Absence de support à l'utilisateur accessible
LOG_APP	39	Absence de sauvegarde des journaux d'événements
LOG_APP	39	Absence de journalisation des événements
LOG_APP	40	Absence de sauvegarde des journaux d'événements
LOG_APP	40	Absence de journalisation des événements
LOG_APP	41	Absence de sauvegarde des journaux d'événements
LOG_APP	41	Absence de journalisation des événements

4.2.4.1 LOG_APP .1 : Application métier standard

Type d'entités	MA	Vulnérabilité
LOG_APP.1	1	Exemplaire unique des contrats de licence
LOG_APP.1	2	Exemplaire unique des contrats de licence
LOG_APP.1	3	Exemplaire unique des contrats de licence
LOG_APP.1	4	Exemplaire unique des contrats de licence
LOG_APP.1	5	Exemplaire unique des contrats de licence
LOG_APP.1	19	Pas ou peu de changement de mot de passe d'accès au système ou à l'application

4.2.4.2 LOG_APP .2 : Application métier spécifique

Type d'entités	MA	Vulnérabilité
LOG_APP.2	1	Applications uniques développées en interne
LOG_APP.2	2	Applications uniques développées en interne
LOG_APP.2	3	Applications uniques développées en interne
LOG_APP.2	4	Applications uniques développées en interne
LOG_APP.2	5	Applications uniques développées en interne
LOG_APP.2	19	Pas ou peu de changement de mot de passe d'accès au système ou à l'application
LOG_APP.2	20	Applications uniques développées en interne

4.3 RES : Réseau

Type d'entités	MA	Vulnérabilité
RES	5	Supports accessibles à des personnes non autorisées
RES	6	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)
RES	7	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)
RES	8	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)
RES	9	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)
RES	10	Support ou équipement non prévu pour résister à des conditions extrêmes (d'humidité, de température, ou de perturbations physiques)
RES	17	Absence de prise en compte des règles d'installation
RES	25	Possibilité de pose d'éléments matériels additionnels pour stocker, transmettre ou altérer (ex: keylogger physique)
RES	25	Possibilité de pose d'une dérivation de circuit
RES	28	Défaut de maintenance
RES	33	Les équipements permettent d'utiliser les ressources du système depuis l'extérieur
RES	33	Les équipements sont accessibles à tous
RES	33	Les équipements sont connectés à des réseaux externes
RES	33	Les équipements utilisés permettent un autre usage que celui qui est prévu
RES	36	Absence de protection physique et logique (cloisonnement…)
RES	38	Matériel d'utilisation complexe ou peu ergonomique
RES	40	Absence de protection physique et logique (cloisonnement…)

4.3.1 RES_INF : Médium et supports

Type d'entités	MA	Vulnérabilité
RES_INF	5	Supports enterrés non repérés
RES_INF	14	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques
RES_INF	15	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques
RES_INF	16	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques
RES_INF	17	Médium et supports susceptibles d'émettre des rayonnements parasites compromettants
RES_INF	19	Médium et supports disposant des caractéristiques permettant l'écoute passive (ex:Ethernet, systèmes de communication sans fil)
RES_INF	19	Support ou équipement de communication physiquement accessible permettant la pose d'un matériel d'écoute
RES_INF	23	Présence d'un réseau de communication avec l'extérieur permettant l'échange d'information
RES_INF	24	Possibilité d'altérer une communication
RES_INF	28	Mauvaise fiabilité des supports
RES_INF	28	Vieillissement du support
RES_INF	28	Mauvaises conditions d'utilisation
RES_INF	29	Vieillissement du support
RES_INF	29	Possibilité d'incompatibilité entre les supports et d'autres composants
RES_INF	29	Médium et supports intégrants des caractéristiques techniques spécifiques à sa localisation (ex. : paramètres de configuration ADSL différents entre la France et le Royaume Uni)
RES_INF	29	Mauvaises conditions d'utilisation
RES_INF	29	Mauvaise fiabilité des supports
RES_INF	29	Défaut de maintenance
RES_INF	32	Défaut de maintenance

Type d'entités	MA	Vulnérabilité
RES_INF	32	Absence de plan de câblage
RES_INF	32	La maintenance ou l'exploitation des équipements nécessite la disponibilité des supports réseau
RES_INF	36	Possibilité d'agir sur les données transmises par l'intermédiaire du média de communication
RES_INF	37	Présence de point d'écoute illicite
RES_INF	38	Absence de support à l'utilisateur accessible
RES_INF	38	Absence d'étiquetage et de schéma d'architecture à jour
RES_INF	38	Absence de plan de câblage
RES_INF	39	Absence de protection physique et logique
RES_INF	40	Absence de cloisonnement réseau
RES_INF	40	Les interfaces sont connectées à des réseaux externes
RES_INF	40	Les supports et médium sont connectés à des réseaux externes
RES_INF	40	Possibilité de modifier des caractéristiques techniques (ex. : adresse MAC d'une carte Ethernet)
RES_INF	40	Absence de protection physique
RES_INF	41	Les relais sont accessibles à tous
RES_INF	41	Fichiers d'imputation complexes ou peu ergonomiques
RES_INF	41	Absence de dispositif de traces et d'audit
RES_INF	41	Le support permet d'utiliser les services du système depuis l'extérieur
RES_INF	41	Les supports et médium sont accessibles à tous et actifs par défaut (ex. : ensemble des prises RJ45 brassées)
RES_INF	42	Possibilité de nuisances pour le personnel utilisateur (transmission par voie hertzienne, ondes…)

4.3.2 RES_REL : Relais passif ou actif

Type d'entités	MA	Vulnérabilité
RES_REL	5	Équipement accessible à des personnes non autorisées
RES_REL	5	Fragilité des équipements
RES_REL	12	Matériel sensible aux perturbations électrique (chutes de tension, surtensions, micro-coupure)
RES_REL	13	Matériel maintenu à distance par des moyens de télécommunication
RES_REL	14	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques
RES_REL	15	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques
RES_REL	16	Médium et supports sensibles aux rayonnements électromagnétiques ou thermiques
RES_REL	17	Matériel susceptible d'émettre des rayonnements parasites compromettants
RES_REL	17	Médium et supports susceptibles d'émettre des rayonnements parasites compromettants
RES_REL	19	Communication s'effectuant en mode Broadcast
RES_REL	19	Accès physique ou logique à un relais permettant la pose d'un dispositif d'écoute
RES_REL	23	Absence de notification des utilisateurs
RES_REL	23	Absence de filtrage et de journalisation sur les relais de communication inter-réseaux
RES_REL	24	Possibilité d'utiliser les ressources sans trace
RES_REL	24	Les relais n'identifient ni les sources ni les destinations (exemple d'impact : système vulnérable aux attaques basées sur "spoofing")
RES_REL	24	Fichiers d'imputation complexes ou peu ergonomiques
RES_REL	26	Fichiers d'imputation complexes ou peu ergonomiques
RES_REL	26	Le réseau facilite l'utilisation des ressources par des personnes non autorisées
RES_REL	26	La couche SNMP est activée
RES_REL	26	La liaison de télémaintenance est activée en permanence
RES_REL	26	Le réseau permet de modifier ou d'agir sur les ressources du système
RES_REL	26	Possibilité d'administrer le système à distance
RES_REL	26	Possibilité d'administrer le système à distance avec des outils d'administration non

Type d'entités	MA	Vulnérabilité
		chiffrés
RES_REL	26	Possibilité d'ajouter des dérivations logicielles
RES_REL	26	Possibilité d'ajouter des logiciels additionnels pour stocker, transmettre ou altérer (ex. : keylogger)
RES_REL	26	Possibilité d'utiliser les ressources sans trace
RES_REL	26	Possibilité d'administrer le système à distance depuis n'importe quel poste
RES_REL	28	Mauvaise fiabilité des matériels
RES_REL	28	Vieillissement du matériel
RES_REL	29	Défaut de maintenance
RES_REL	29	Mauvaise fiabilité des matériels
RES_REL	29	Possibilité de mal configurer, installer ou de modifier les relais
RES_REL	29	Vieillissement du matériel
RES_REL	30	Possibilité de mal configurer, installer ou de modifier les relais
RES_REL	30	Possibilité que les relais soient soumis à un nombre trop important de requêtes ou à un parasitage intense (ex: attaque de déni de service type "smurf", "SYN flood"...)
RES_REL	30	Mauvais dimensionnement (ex: trop de données par rapport à la bande passante maximale)
RES_REL	31	Absence de procédure de maintenance
RES_REL	31	Possibilité de mal configurer, installer ou de modifier les relais
RES_REL	32	Matériels obsolètes
RES_REL	32	Matériels à configurations non évolutives
RES_REL	32	La maintenance ou l'exploitation du système se fait par l'intermédiaire du réseau
RES_REL	32	Absence de garantie de supports des délais maximums
RES_REL	32	Défaut de maintenance
RES_REL	32	Matériels spécifiques
RES_REL	36	Possibilité d'administrer le système à distance depuis n'importe quel poste
RES_REL	36	La liaison de télémaintenance est activée en permanence
RES_REL	36	Absence de dispositif de contrôle d'accès robuste
RES_REL	36	Le réseau facilite l'utilisation des ressources par des personnes non autorisées
RES_REL	36	Le réseau permet de modifier ou d'agir sur les ressources du système
RES_REL	36	Possibilité d'administrer le système à distance
RES_REL	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés
RES_REL	36	La couche SNMP est activée
RES_REL	37	Présence de point d'écoute illicite
RES_REL	38	Médium et supports intégrants des caractéristiques techniques spécifiques à sa localisation (ex. : paramètres de configuration ADSL différents entre la France et le Royaume Uni)
RES_REL	38	Absence d'étiquetage et de schéma d'architecture à jour
RES_REL	38	Absence de support à l'utilisateur accessible
RES_REL	39	Fichiers d'imputation complexes ou peu ergonomiques
RES_REL	39	Possibilité d'utiliser les ressources sans trace
RES_REL	39	Le principe du moindre privilège n'est pas appliqué
RES_REL	40	Les relais n'identifient ni les sources ni les destinations (exemple d'impact : système vulnérable aux attaques basées sur "spoofing")
RES_REL	40	Le réseau permet de modifier ou d'agir sur les ressources du système
RES_REL	40	Présence de protocole ne disposant pas de fonction d'authentification
RES_REL	40	Possibilité d'administrer le système à distance
RES_REL	40	Le réseau facilite l'utilisation des ressources par des personnes non autorisées
RES_REL	40	Fichiers d'imputation complexes ou peu ergonomiques
RES_REL	40	Absence de dispositif de contrôle d'accès robuste
RES_REL	40	Absence de protection physique
RES_REL	40	Absence de cloisonnement réseau
RES_REL	40	La liaison de télémaintenance est activée en permanence
RES_REL	41	Le réseau permet de modifier ou d'agir sur les ressources du système

Type d'entités	MA	Vulnérabilité
RES_REL	41	Le réseau facilite l'utilisation des ressources par des personnes non autorisées
RES_REL	41	Les relais sont accessibles à tous
RES_REL	41	Fichiers d'imputation complexes ou peu ergonomiques
RES_REL	41	Absence de dispositif de traces et d'audit
RES_REL	42	Possibilité de nuisances pour le personnel utilisateur (transmission par voie hertzienne, ondes…)

4.3.3 RES_INT : Interface de communication

Type d'entités	MA	Vulnérabilité
RES_INT	5	Équipement accessible à des personnes non autorisées
RES_INT	5	Fragilité des équipements
RES_INT	17	Matériel susceptible d'émettre des rayonnements parasites compromettants
RES_INT	19	Absence d'authentification des matériels connectés au réseau
RES_INT	19	Accès physique ou logique à un relais permettant la pose d'un dispositif d'écoute
RES_INT	19	Communication s'effectuant en mode Broadcast
RES_INT	19	Complexité du routage entre les sous-réseaux
RES_INT	19	Interface disposant d'une fonction permettant à l'écoute
RES_INT	23	Fichiers d'imputation complexes ou peu ergonomiques
RES_INT	23	Interface standard permettant les échanges de l'information (ex: interface Bluetooth acceptant toutes les communications par défaut)
RES_INT	23	Possibilité d'utiliser les ressources sans trace
RES_INT	23	Absence de notification des utilisateurs
RES_INT	23	Complexité du routage entre les sous-réseaux
RES_INT	23	Absence de routage strict entre les sous-réseaux
RES_INT	24	Protocole ne permettant pas d'authentifier de manière sûre l'émetteur d'une communication
RES_INT	24	Possibilité d'utiliser les ressources sans trace
RES_INT	24	Fichiers d'imputation complexes ou peu ergonomiques
RES_INT	26	La couche SNMP est activée
RES_INT	26	Le réseau facilite l'utilisation des ressources par des personnes non autorisées
RES_INT	26	Fichiers d'imputation complexes ou peu ergonomiques
RES_INT	26	Possibilité d'ajouter des dérivations logicielles
RES_INT	26	Le réseau permet de modifier ou d'agir sur les ressources du système
RES_INT	26	Possibilité d'ajouter des logiciels additionnels pour stocker, transmettre ou altérer (ex. : keylogger)
RES_INT	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés
RES_INT	26	La liaison de télémaintenance est activée en permanence
RES_INT	26	Possibilité d'administrer le système à distance
RES_INT	26	Possibilité d'administrer le système à distance depuis n'importe quel poste
RES_INT	26	Possibilité d'utiliser les ressources sans trace
RES_INT	28	Mauvaise fiabilité des matériels
RES_INT	28	Vieillissement du matériel
RES_INT	29	Interface intégrant des caractéristiques techniques relatives au pays (ex: prises téléphoniques différentes entre la France et le Royaume Uni)
RES_INT	29	Possibilité de mal configurer, installer ou de modifier les relais
RES_INT	29	Mauvaise fiabilité des matériels
RES_INT	29	Vieillissement du matériel
RES_INT	29	Possibilité d'incompatibilité entre les différentes ressources
RES_INT	30	Possibilité que les relais soient soumis à un nombre trop important de requêtes ou à un parasitage intense (ex: attaque de déni de service type "smurf", "SYN flood"...)
RES_INT	30	Possibilité de mal configurer, installer ou de modifier les relais
RES_INT	31	Possibilité de mal configurer, installer ou de modifier les relais
RES_INT	31	Absence de procédure de maintenance

Type d'entités	MA	Vulnérabilité
RES_INT	31	Mauvaise gestion des versions et configurations des pilotes
RES_INT	31	Effets de bord des interfaces (problèmes de compatibilité entre protocoles...)
RES_INT	32	Matériels spécifiques
RES_INT	32	Matériels obsolètes
RES_INT	32	Matériels à configurations non évolutives
RES_INT	32	La maintenance ou l'exploitation du système se fait par l'intermédiaire du réseau
RES_INT	32	Absence de garantie de supports des délais maximums
RES_INT	36	Possibilité d'administrer le système à distance depuis n'importe quel poste
RES_INT	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés
RES_INT	36	Possibilité d'administrer le système à distance
RES_INT	36	Le réseau permet de modifier ou d'agir sur les ressources du système
RES_INT	36	Le réseau facilite l'utilisation des ressources par des personnes non autorisées
RES_INT	36	La liaison de télémaintenance est activée en permanence
RES_INT	36	La couche SNMP est activée
RES_INT	38	Insuffisance de compétence pour l'utilisateur
RES_INT	38	Interface intégrant des caractéristiques techniques relatives au pays (ex: prises téléphoniques différentes entre la France et le Royaume Uni)
RES_INT	39	Le principe du moindre privilège n'est pas appliqué
RES_INT	39	Possibilité d'utiliser les ressources sans trace
RES_INT	39	Fichiers d'imputation complexes ou peu ergonomiques
RES_INT	40	Le réseau permet de modifier ou d'agir sur les ressources du système
RES_INT	40	Présence de protocole ne disposant pas de fonction d'authentification
RES_INT	40	Possibilité d'administrer le système à distance
RES_INT	40	Les interfaces sont accessibles à tous
RES_INT	40	Fichiers d'imputation complexes ou peu ergonomiques
RES_INT	40	La liaison de télémaintenance est activée en permanence
RES_INT	40	Le réseau facilite l'utilisation des ressources par des personnes non autorisées
RES_INT	41	Le réseau facilite l'utilisation des ressources par des personnes non autorisées
RES_INT	41	Le protocole ne permet pas l'identification sûr de l'émetteur
RES_INT	41	Le réseau permet de modifier ou d'agir sur les ressources du système
RES_INT	41	Le protocole ne permet pas l'envoi d'accusé de réception
RES_INT	41	Possibilité d'utiliser les ressources sans trace

4.4 PER : Personnel

Type d'entités	MA	Vulnérabilité
PER	1	Méconnaissance des mesures de sécurité
PER	1	Absence de test des procédures de réaction et d'information en cas de sinistre
PER	2	Absence de test des procédures de réaction et d'information en cas de sinistre
PER	2	Méconnaissance des mesures de sécurité
PER	3	Absence de test des procédures de réaction et d'information en cas de sinistre
PER	3	Méconnaissance des mesures de sécurité
PER	4	Méconnaissance des mesures de sécurité
PER	5	Méconnaissance des mesures de sécurité
PER	6	Méconnaissance des mesures de sécurité
PER	7	Méconnaissance des mesures de sécurité
PER	8	Méconnaissance des mesures de sécurité
PER	9	Méconnaissance des mesures de sécurité
PER	11	Méconnaissance des mesures de sécurité
PER	12	Méconnaissance des mesures de sécurité
PER	13	Méconnaissance des mesures de sécurité
PER	18	Méconnaissance des mesures de sécurité
PER	18	Faible sensibilisation à la protection de l'information
PER	18	Absence de soutien de la direction à l'application de la politique de sécurité
PER	19	Manque de formation aux mesures et outils de protection des échanges externe et interne
PER	19	Personnel manipulable
PER	19	Absence de soutien de la direction à l'application de la politique de sécurité
PER	19	Faible sensibilisation à la protection en confidentialité des échanges d'information
PER	19	Obtention d'un avantage à la captation d'information
PER	20	Personnel manipulable
PER	20	Non-respect des règles associées à la classification des informations
PER	20	Absence de sensibilisation à la protection des documents à caractère confidentiel provoquant un manque de vigilance
PER	20	Obtention d'un avantage à la divulgation d'information
PER	21	Absence de soutien de la direction à l'application de la politique de sécurité
PER	21	Faible sensibilisation à la protection des matériels en dehors de l'organisme
PER	21	Personnel manipulable
PER	21	Non-respect des règles de protection physique applicables aux équipements transportables
PER	21	Obtention d'un avantage à la revente d'un matériel
PER	22	Personnel manipulable
PER	22	Non-respect des règles de destruction des supports associées à la classification de l'information
PER	22	Absence d'information et de sensibilisation à la rémanence des données informatiques sur les supports
PER	22	Obtention d'un avantage à la divulgation d'information
PER	22	Absence de soutien de la direction à l'application de la politique de sécurité
PER	23	Non-respect des règles de classification de l'information
PER	23	Absence de soutien de la direction à l'application de la politique de sécurité
PER	23	Personnel manipulable
PER	23	Absence de sensibilisation à la protection de l'information à caractère sensible
PER	23	Non-respect du devoir de réserve
PER	23	Obtention d'un avantage à la divulgation d'information
PER	24	Absence de soutien de la direction à l'application de la politique de sécurité
PER	25	Personnel manipulable
PER	25	Absence de vigilance lors d'une intervention d'un personnel de maintenance sur un poste de travail ou un serveur

Type d'entités	MA	Vulnérabilité
PER	25	Faible sensibilisation à la protection des matériels en dehors de l'organisme
PER	25	Obtention d'un avantage à la désinformation
PER	27	Méconnaissance des mesures de sécurité
PER	27	Manque de discrétion ou de vigilance
PER	27	Absence de soutien de la direction à l'application de la politique de sécurité
PER	33	Méconnaissance des mesures de sécurité
PER	34	Absence de soutien de la direction à l'application de la politique de sécurité
PER	34	Méconnaissance des mesures de sécurité
PER	34	Obtention d'un avantage
PER	35	Absence de sensibilisation du personnel au risque de sanction
PER	35	Non-respect de la charte informatique précisant les exigences d'utilisation
PER	35	Méconnaissance des mesures de sécurité
PER	35	Absence de soutien de la direction à l'application de la politique de sécurité
PER	36	Non-respect de la charte informatique précisant les exigences d'utilisation
PER	36	Absence de protection et de classification de l'information
PER	36	Absence de sensibilisation du personnel au risque de sanction
PER	36	Méconnaissance des mesures de sécurité
PER	36	Personnel manipulable
PER	36	Situation conflictuelle entre personnes
PER	36	Absence de soutien de la direction à l'application de la politique de sécurité
PER	37	Absence de sensibilisation du personnel au risque de sanction
PER	37	Absence de formation précisant les conditions d'utilisation licite de l'information
PER	37	Absence de protection et de classification de l'information
PER	37	Méconnaissance des mesures de sécurité
PER	39	Prééminence de la catégorie de personnel
PER	39	Absence de soutien de la direction à l'application de la politique de sécurité
PER	39	Il existe des opérations très sensibles opérables par une personne unique
PER	39	Obtention d'un avantage
PER	39	La notion de droit n'est pas définie pour le personnel
PER	40	Droits accordés en dehors du besoin légitime
PER	40	Situation conflictuelle entre personnes
PER	40	Absence de règles morales ou d'éthique
PER	40	Obtention d'un avantage
PER	40	Il existe des opérations très sensibles opérables par une personne unique
PER	40	Organisation inadaptée
PER	40	Absence de soutien de la direction à l'application de la politique de sécurité
PER	40	Missions peu adaptées au personnel
PER	41	Absence de soutien de la direction à l'application de la politique de sécurité

4.4.1 PER_DEC : Décisionnel

Type d'entités	MA	Vulnérabilité
PER_DEC	1	Absence de sensibilisation à la protection des équipements de sécurité
PER_DEC	2	Absence de sensibilisation à la protection des équipements de sécurité
PER_DEC	3	Absence de sensibilisation à la protection des équipements de sécurité
PER_DEC	6	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_DEC	7	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_DEC	8	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_DEC	9	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_DEC	20	Absence de soutien de la direction à l'application de la politique de sécurité
PER_DEC	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)
PER_DEC	24	Crédulité
PER_DEC	24	Méconnaissance de l'importance de la qualification de l'information

Type d'entités	MA	Vulnérabilité
PER_DEC	24	Personnel manipulable
PER_DEC	24	Climat social conflictuel
PER_DEC	24	Obtention d'un avantage à la désinformation
PER_DEC	26	Utilisation de logiciels sans garantie de leur origine
PER_DEC	26	Climat social conflictuel
PER_DEC	26	Manque de sensibilisation à la menace des codes malveillants
PER_DEC	26	Méconnaissance des réactions réflexes en cas de détection d'anomalie
PER_DEC	26	Non-respect des règles de mises à jour des logiciels anti-virus
PER_DEC	26	Personnel manipulable
PER_DEC	26	Obtention d'un avantage à la perturbation du système informatique
PER_DEC	28	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)
PER_DEC	29	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)
PER_DEC	30	Absence de décision de redimensionnement à la vu d'augmentations significatives de l'utilisation des ressources informatiques
PER_DEC	31	Absence de suivi des incidents permettant de prévenir d'éventuels dysfonctionnements (tableaux de bord)
PER_DEC	32	Choix de technologie sans assurance de pérennité
PER_DEC	32	Faible budget alloué à la maintenance
PER_DEC	32	Existence de composants désuets dans l'infrastructure de traitement de l'information (développement dans des langages plus utilisés…)
PER_DEC	33	Absence de sensibilisation du personnel au risque de sanction
PER_DEC	33	Droits accordés en dehors du besoin légitime
PER_DEC	33	Obtention d'un avantage
PER_DEC	33	Non-respect de la charte informatique précisant les exigences d'utilisation
PER_DEC	34	Non-respect de la charte informatique précisant les exigences d'utilisation
PER_DEC	34	Absence de sensibilisation du personnel au risque de sanction
PER_DEC	38	Mauvaise connaissance des responsabilités
PER_DEC	38	Absence de formalisation des responsabilités connues de tous
PER_DEC	38	Conditions de travail défavorables
PER_DEC	38	Manque de professionnalisme
PER_DEC	38	Non-respect des consignes
PER_DEC	38	Personnel utilisateur peu ou mal formé
PER_DEC	38	Il existe des opérations très sensibles opérables par une personne unique
PER_DEC	41	Obtention d'un avantage
PER_DEC	41	Manque de confiance dans l'organisation
PER_DEC	41	Responsabilité de chacun non connue
PER_DEC	41	Situation conflictuelle entre personnes
PER_DEC	41	Changement de politique ou de stratégie d'organisation
PER_DEC	42	Indisponibilité provoquée par un enjeu concurrentiel

4.4.2 PER_UTI : Utilisateurs

Type d'entités	MA	Vulnérabilité
PER_UTI	1	Climat social conflictuel
PER_UTI	2	Climat social conflictuel
PER_UTI	3	Climat social conflictuel
PER_UTI	4	Absence de procédures de gestion de situation d'urgence
PER_UTI	5	Manque de sensibilisation à la protection physique des équipements
PER_UTI	5	Climat social conflictuel
PER_UTI	6	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_UTI	7	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_UTI	8	Absence de test des procédures de réaction et d'information en cas de sinistre

Type d'entités	MA	Vulnérabilité
PER_UTI	9	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_UTI	12	Manque d'information concernant les conditions d'utilisation des points d'énergie secourue
PER_UTI	20	Absence d'engagement individuel pour la protection des documents à caractère confidentiel
PER_UTI	24	Personnel manipulable
PER_UTI	24	Obtention d'un avantage à la désinformation
PER_UTI	24	Climat social conflictuel
PER_UTI	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)
PER_UTI	24	Méconnaissance de l'importance de la qualification de l'information
PER_UTI	24	Crédulité
PER_UTI	26	Manque de sensibilisation à la menace des codes malveillants
PER_UTI	26	Non-respect des règles de mises à jour des logiciels anti-virus
PER_UTI	26	Climat social conflictuel
PER_UTI	26	Méconnaissance des réactions réflexes en cas de détection d'anomalie
PER_UTI	26	Utilisation de logiciels sans garantie de leur origine
PER_UTI	26	Obtention d'un avantage à la perturbation du système informatique
PER_UTI	26	Personnel manipulable
PER_UTI	28	Absence de remontée d'information pour une analyse centralisée des pannes
PER_UTI	28	Méconnaissance des consignes d'usage des matériels
PER_UTI	29	Méconnaissance des consignes d'usage des matériels
PER_UTI	29	Absence de remontée d'information pour une analyse centralisée des pannes
PER_UTI	30	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)
PER_UTI	30	Obtention d'un avantage à la perturbation du système informatique
PER_UTI	30	Manque de sensibilisation aux besoins d'économie des ressources informatiques de l'organisme (mauvaise utilisation des espaces de stockage…)
PER_UTI	31	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)
PER_UTI	32	Non-respect des règles qualité
PER_UTI	32	Utilisation de logiciels ou développements hors des normes et standards de l'organisme
PER_UTI	32	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)
PER_UTI	33	Non-respect de la charte informatique précisant les exigences d'utilisation
PER_UTI	33	Obtention d'un avantage
PER_UTI	33	Droits accordés en dehors du besoin légitime
PER_UTI	33	Absence de sensibilisation du personnel au risque de sanction
PER_UTI	34	Non-respect de la charte informatique précisant les exigences d'utilisation
PER_UTI	34	Absence de sensibilisation du personnel au risque de sanction
PER_UTI	38	Absence de motivation pour les travaux associés à la saisie
PER_UTI	38	Manque de professionnalisme
PER_UTI	38	Conditions de travail défavorables
PER_UTI	38	Non-respect des consignes
PER_UTI	38	Personnel peu habitué à la saisie
PER_UTI	38	Personnel utilisateur peu ou mal formé
PER_UTI	38	Absence de documentation d'utilisation des applicatifs existantes
PER_UTI	41	Changement de politique ou de stratégie d'organisation
PER_UTI	41	Manque de confiance dans l'organisation
PER_UTI	41	Situation conflictuelle entre personnes
PER_UTI	41	Responsabilité de chacun non connue
PER_UTI	41	Obtention d'un avantage
PER_UTI	42	Indisponibilité causée par l'absentéisme
PER_UTI	42	Indisponibilité causée par la maladie

Type d'entités	MA	Vulnérabilité
PER_UTI	42	Climat social conflictuel
PER_UTI	42	Indisponibilité provoquée (agression physique, prise d'otage…)
PER_UTI	42	Absence de procédures de transfert de connaissances

4.4.3 PER_EXP : Exploitant / Maintenance

Type d'entités	MA	Vulnérabilité
PER_EXP	1	Climat social conflictuel
PER_EXP	2	Climat social conflictuel
PER_EXP	3	Climat social conflictuel
PER_EXP	4	Absence de procédures de gestion de situation d'urgence
PER_EXP	5	Manque de sensibilisation à la protection physique des équipements
PER_EXP	5	Climat social conflictuel
PER_EXP	6	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_EXP	7	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_EXP	8	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_EXP	9	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_EXP	20	Absence d'engagement individuel pour la protection des documents à caractère confidentiel
PER_EXP	24	Absence de sensibilisation aux risques d'usurpation d'identité (mauvais usage des moyens garantissant l'authentification tels que les mots de passe)
PER_EXP	24	Obtention d'un avantage à la désinformation
PER_EXP	24	Climat social conflictuel
PER_EXP	24	Méconnaissance de l'importance de la qualification de l'information
PER_EXP	24	Crédulité
PER_EXP	24	Personnel manipulable
PER_EXP	26	Exploitant ou mainteneur disposant de privilèges étendus
PER_EXP	26	Manque de sensibilisation à la menace des codes malveillants
PER_EXP	26	Méconnaissance des procédures d'intervention en cas de détection d'anomalie
PER_EXP	26	Non-respect des règles de mises à jour des logiciels anti-virus
PER_EXP	26	Personnel manipulable
PER_EXP	26	Obtention d'un avantage à la perturbation du système informatique
PER_EXP	26	Utilisation de logiciels sans garantie de leur origine
PER_EXP	26	Situation conflictuelle
PER_EXP	28	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)
PER_EXP	29	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)
PER_EXP	30	Absence de mise en œuvre du suivi des incidents permettant de prévenir d'éventuelles pannes ou saturation (tableaux de bord)
PER_EXP	31	Manque de formation à la maintenance et l'exploitation de nouveaux équipements
PER_EXP	31	Mauvais dimensionnement des ressources d'exploitation ou de maintenance
PER_EXP	31	Non-respect des procédures d'intervention
PER_EXP	32	Manque de formation aux bons usages de l'outil informatique (perturbation du système, installation de logiciel incompatible…)
PER_EXP	32	Utilisation de logiciels ou développements hors des normes et standards de l'organisme
PER_EXP	32	Non-respect des règles qualité
PER_EXP	33	Absence de charte informatique précisant les exigences d'utilisation
PER_EXP	33	Obtention d'un avantage
PER_EXP	33	Absence de sensibilisation du personnel au risque de sanction
PER_EXP	33	Absence de gestion de parc du matériel
PER_EXP	34	Absence de sensibilisation du personnel au risque de sanction
PER_EXP	34	Non-respect de la charte informatique précisant les exigences d'utilisation
PER_EXP	38	Absence de documentation d'utilisation des applicatifs existantes

Type d'entités	MA	Vulnérabilité
PER_EXP	38	Manque de professionnalisme
PER_EXP	38	Conditions de travail défavorables
PER_EXP	38	Personnel peu habitué à la saisie
PER_EXP	38	Personnel utilisateur peu ou mal formé
PER_EXP	38	Absence de motivation pour les travaux associés à la saisie
PER_EXP	38	Non-respect des consignes
PER_EXP	41	Situation conflictuelle entre personnes
PER_EXP	41	Responsabilité de chacun non connue
PER_EXP	41	Manque de confiance dans l'organisation
PER_EXP	42	Indisponibilité causée par l'absentéisme
PER_EXP	42	Problèmes sociaux
PER_EXP	42	Indisponibilité provoquée (agression physique, prise d'otage…)
PER_EXP	42	Indisponibilité causée par la maladie

4.4.4 PER_DEV : Développeur

Type d'entités	MA	Vulnérabilité
PER_DEV	1	Climat social conflictuel
PER_DEV	2	Climat social conflictuel
PER_DEV	3	Climat social conflictuel
PER_DEV	5	Climat social conflictuel
PER_DEV	5	Manque de sensibilisation à la protection physique des équipements
PER_DEV	6	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_DEV	7	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_DEV	8	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_DEV	9	Absence de test des procédures de réaction et d'information en cas de sinistre
PER_DEV	20	Absence d'engagement individuel pour la protection des documents à caractère confidentiel
PER_DEV	24	Absence de moyens permettant de garantir l'authenticité des codes
PER_DEV	24	Méconnaissance des mesures de sécurité
PER_DEV	26	Obtention d'un avantage à la perturbation du système informatique
PER_DEV	26	Situation conflictuelle
PER_DEV	26	Méconnaissance des mesures de sécurité
PER_DEV	26	Absence de moyens permettant de garantir l'authenticité des développements
PER_DEV	26	Personnel manipulable
PER_DEV	31	Manque de formation
PER_DEV	31	Absence de règles de sécurité dans les développements
PER_DEV	32	Non-respect des règles qualité
PER_DEV	32	Absence de standard ou de norme
PER_DEV	32	Non-respect des règles de développement
PER_DEV	33	Manque de contrôle des besoins matériels pour développer une application
PER_DEV	33	Absence de règles morales ou d'éthique
PER_DEV	33	Obtention d'un avantage
PER_DEV	33	Absence de sensibilisation du personnel au risque de sanction
PER_DEV	33	Absence de charte informatique précisant les exigences d'utilisation
PER_DEV	33	Non-respect de la charte informatique précisant les exigences d'utilisation
PER_DEV	35	Aucune certification des produits
PER_DEV	35	Aucune procédure d'évaluation des produits
PER_DEV	35	Absence de procédure et moyens de vérification de l'origine du logiciel (signature du code, du binaire...)
PER_DEV	38	Absence de documentation d'utilisation des applicatifs existantes
PER_DEV	38	Absence de motivation pour les travaux associés à la saisie
PER_DEV	38	Personnel peu habitué à la saisie
PER_DEV	38	Personnel utilisateur peu ou mal formé

Type d'entités	MA	Vulnérabilité
PER_DEV	38	Non-respect des consignes
PER_DEV	38	Conditions de travail défavorables
PER_DEV	38	Manque de professionnalisme
PER_DEV	41	Manque de confiance dans l'organisation
PER_DEV	41	Responsabilité de chacun non connue
PER_DEV	41	Situation conflictuelle entre personnes
PER_DEV	42	Indisponibilité causée par la maladie
PER_DEV	42	Indisponibilité causée par l'absentéisme
PER_DEV	42	Indisponibilité provoquée (agression physique, prise d'otage…)
PER_DEV	42	Problèmes sociaux

4.5 PHY : Site

4.5.1 PHY_LIE : Lieu

Type d'entités	MA	Vulnérabilité
PHY_LIE	14	Aucune prise en compte de risque des rayonnements électromagnétiques ou thermiques à la conception
PHY_LIE	14	Proximité d'une source de rayonnements électromagnétiques ou thermiques
PHY_LIE	15	Proximité d'une source de rayonnements électromagnétiques ou thermiques
PHY_LIE	15	Aucune prise en compte de risque des rayonnements électromagnétiques ou thermiques à la conception
PHY_LIE	16	Proximité d'une source de rayonnements électromagnétiques ou thermiques
PHY_LIE	16	Aucune prise en compte de risque des rayonnements électromagnétiques ou thermiques à la conception
PHY_LIE	17	Absence de réalisation de zonage TEMPEST

4.5.1.1 PHY_LIE.1 : Externe

Type d'entités	MA	Vulnérabilité
PHY_LIE.1	2	Site placé dans une zone inondable
PHY_LIE.1	3	Proximité de sources de pollution (source sonore, fumée, vapeur…)
PHY_LIE.1	4	Possibilités de destruction causée par un événement extérieur (collisions, attentats)
PHY_LIE.1	4	Proximité d'activité industrielle ou de site à risque
PHY_LIE.1	5	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_LIE.1	8	Site recensé comme à risque
PHY_LIE.1	9	Site dans lequel des phénomènes météorologiques extrêmes se produisent périodiquement (tempête, ouragan, cyclone…)
PHY_LIE.1	10	Site placé dans une zone inondable
PHY_LIE.1	18	Présence de lieu d'observation à l'extérieur du site
PHY_LIE.1	19	Possibilité de capter les transmissions depuis l'extérieur du site
PHY_LIE.1	20	Supports ou documents transmis ou présents à l'extérieur du site
PHY_LIE.1	21	Utilisation de matériel à l'extérieur (domicile des personnels, autre organisme…)
PHY_LIE.1	22	Présence de support mis au rebut à l'extérieur du site
PHY_LIE.1	25	Utilisation de matériel à l'extérieur (domicile des personnels, autre organisme…)
PHY_LIE.1	26	Utilisation de matériel à l'extérieur (domicile des personnels, autre organisme…)
PHY_LIE.1	42	Climat social difficile pouvant provoquer des grèves de transport

4.5.1.2 PHY_LIE.2 : Locaux

Type d'entités	MA	Vulnérabilité
PHY_LIE.2	1	Présence d'ouverture sur la voie publique (fenêtre)
PHY_LIE.2	1	Vieillissement des locaux
PHY_LIE.2	1	Absence de contrôle d'accès au site ou aux locaux
PHY_LIE.2	1	Absence de cloisonnement anti-feu
PHY_LIE.2	2	Absence de contrôle des accès physiques aux locaux
PHY_LIE.2	2	Ouverture à l'extérieur non étanche
PHY_LIE.2	2	Présence d'un dispositif d'extinction incendie à eau
PHY_LIE.2	3	Atmosphère polluée (hangar, atelier…)
PHY_LIE.2	3	Proximité de sources de pollution (source sonore, fumée, vapeur…)
PHY_LIE.2	4	Locaux dans lesquels les risques d'explosion/implosion n'ont pas été pris en compte
PHY_LIE.2	5	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_LIE.2	6	Absence de moyens de ventilation ou de climatisation lors de chaleur estivale excessive

Type d'entités	MA	Vulnérabilité
PHY_LIE.2	6	Non prise en compte des conditions climatiques dans la construction des locaux
PHY_LIE.2	7	Non prise en compte des risques sismiques dans la construction des bâtiments
PHY_LIE.2	8	Non prise en compte des risques sismiques dans la construction des bâtiments
PHY_LIE.2	9	Absence de protection contre la foudre
PHY_LIE.2	10	Absence de protection contre la montée des eaux
PHY_LIE.2	17	Accès public à proximité des bâtiments
PHY_LIE.2	19	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_LIE.2	20	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_LIE.2	21	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_LIE.2	22	Présence de support mis au rebut dans des locaux publics
PHY_LIE.2	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur
PHY_LIE.2	25	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_LIE.2	26	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_LIE.2	28	Absence de prise en compte d'environnement spécifique augmentant les risques de panne (atmosphère surchauffée, environnement industriel...)
PHY_LIE.2	29	Absence de prise en compte d'environnement spécifique augmentant les risques de panne (atmosphère surchauffée, environnement industriel...)
PHY_LIE.2	33	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux
PHY_LIE.2	33	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones
PHY_LIE.2	33	Absence de journalisation des entrées des personnes
PHY_LIE.2	34	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones
PHY_LIE.2	34	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux
PHY_LIE.2	34	Absence de journalisation des entrées des personnes
PHY_LIE.2	35	Absence de journalisation des entrées des personnes
PHY_LIE.2	35	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux
PHY_LIE.2	35	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones
PHY_LIE.2	36	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones
PHY_LIE.2	36	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux
PHY_LIE.2	36	Absence de journalisation des entrées des personnes
PHY_LIE.2	38	Environnement de travail défavorable (locaux trop petit, manque d'espace de rangement…)
PHY_LIE.2	39	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux
PHY_LIE.2	40	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux
PHY_LIE.2	41	Absence d'historisation des entrées et sorties des personnes
PHY_LIE.2	42	Personnels spécialisés hébergés dans des locaux distants
PHY_LIE.2	42	Personnels habitant loin des locaux

4.5.1.3 PHY_LIE.3 : Zone

Type d'entités	MA	Vulnérabilité

Type d'entités	MA	Vulnérabilité
PHY_LIE.3	1	Absence de prise en compte dans la phase d'installation des risques d'incendie spécifiques aux équipements hébergés
PHY_LIE.3	1	Absence ou mauvais dimensionnement ou inadéquation du dispositif d'extinction automatique d'incendie
PHY_LIE.3	1	Présence d'ouverture sur la voie publique (fenêtre)
PHY_LIE.3	2	Plafond ou ouverture à l'extérieur non étanche
PHY_LIE.3	2	Absence d'identification claire des vannes de coupure d'eau
PHY_LIE.3	2	Accès non protégé
PHY_LIE.3	2	Canalisation d'eau à proximité des équipements
PHY_LIE.3	2	Dispositif d'extinction incendie à eau
PHY_LIE.3	2	Plafond ou ouverture à l'extérieur non étanche
PHY_LIE.3	2	Canalisation d'eau à proximité des équipements de terminaison
PHY_LIE.3	2	Absence de puisard
PHY_LIE.3	4	Locaux dans lesquels les risques d'explosion/implosion n'ont pas été pris en compte
PHY_LIE.3	5	Accès physique non protégé aux locaux hébergeant des matériels ou supports
PHY_LIE.3	6	Absence de moyens de ventilation ou de climatisation lors de chaleur estivale excessive
PHY_LIE.3	6	Non prise en compte des conditions climatiques dans la construction des locaux
PHY_LIE.3	9	Absence de protection contre la foudre
PHY_LIE.3	10	Absence de protection contre la montée des eaux
PHY_LIE.3	11	Absence de révision des besoins de climatisation en cas de modification des locaux ou d'ajout de matériel
PHY_LIE.3	17	Salle située à proximité de la voie publique
PHY_LIE.3	18	Zone disposant d'ouverture sur la voie publique
PHY_LIE.3	18	Zone observable depuis un lieu de passage
PHY_LIE.3	19	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_LIE.3	20	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_LIE.3	21	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_LIE.3	22	Présence de support mis au rebut dans des zones accessibles à des personnes n'ayant pas le besoin d'en connaître
PHY_LIE.3	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur
PHY_LIE.3	25	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_LIE.3	26	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_LIE.3	28	Absence de prise en compte d'environnement spécifique augmentant les risques de panne (atmosphère surchauffée, environnement industriel...)
PHY_LIE.3	29	Absence de prise en compte d'environnement spécifique augmentant les risques de panne (atmosphère surchauffée, environnement industriel...)
PHY_LIE.3	33	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones
PHY_LIE.3	33	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux
PHY_LIE.3	33	Absence de journalisation des entrées des personnes
PHY_LIE.3	34	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux
PHY_LIE.3	34	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones
PHY_LIE.3	34	Absence de journalisation des entrées des personnes
PHY_LIE.3	35	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones

Type d'entités	MA	Vulnérabilité
PHY_LIE.3	35	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux
PHY_LIE.3	35	Absence de journalisation des entrées des personnes
PHY_LIE.3	36	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux
PHY_LIE.3	36	Absence de journalisation des entrées des personnes
PHY_LIE.3	36	Absence de procédures de contrôle de l'identité de toute personne entrant dans les locaux ou zones
PHY_LIE.3	38	Environnement de travail défavorable (locaux trop petit, manque d'espace de rangement…)
PHY_LIE.3	39	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux
PHY_LIE.3	40	Absence de procédures de contrôles des habilitations du personnel accédant au site ou aux locaux
PHY_LIE.3	41	Absence d'historisation des entrées et sorties des personnes

4.5.2 PHY_SRV : Service essentiel

Type d'entités	MA	Vulnérabilité
PHY_SRV	4	Locaux dans lesquels les risques d'explosion/implosion n'ont pas été pris en compte
PHY_SRV	5	Accès physique non protégé aux locaux hébergeant des matériels ou supports
PHY_SRV	10	Absence de protection contre la montée des eaux
PHY_SRV	14	Aucune prise en compte des risques liés à la proximité d'une source électromagnétique
PHY_SRV	15	Aucune prise en compte des risques liés à la proximité d'une source électromagnétique
PHY_SRV	16	Aucune prise en compte des risques liés à la proximité d'une source électromagnétique
PHY_SRV	28	Absence de contrôle du bon fonctionnement des ressources de secours
PHY_SRV	28	Déclenchement manuel de la solution de secours
PHY_SRV	29	Absence de contrôle du bon fonctionnement des ressources de secours
PHY_SRV	29	Déclenchement manuel de la solution de secours

4.5.2.1 PHY_SRV.1 : Communication

Type d'entités	MA	Vulnérabilité
PHY_SRV.1	1	Absence de prise en compte dans la phase d'installation des risques d'incendie spécifiques aux équipements hébergés
PHY_SRV.1	1	Absence ou mauvais dimensionnement ou inadéquation du dispositif d'extinction automatique d'incendie
PHY_SRV.1	1	Présence d'ouverture sur la voie publique (fenêtre)
PHY_SRV.1	2	Plafond ou ouverture à l'extérieur non étanche
PHY_SRV.1	2	Canalisation d'eau à proximité des équipements de terminaison
PHY_SRV.1	2	Accès non protégé aux locaux hébergeant les équipements de production ou de distribution des services essentiels
PHY_SRV.1	2	Câblage posé sur le sol
PHY_SRV.1	12	Équipement terminal de communication ne disposant pas d'alimentation secourue
PHY_SRV.1	13	Absence de maintenance des équipements de terminaison et de distribution
PHY_SRV.1	13	Défauts d'exploitation du réseau téléphonique interne
PHY_SRV.1	13	Dysfonctionnement déjà constaté dans la fourniture du service de télécommunication
PHY_SRV.1	13	Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques ou moyens de télécommunication
PHY_SRV.1	17	Support facilitant la capture des signaux parasites compromettants (câbles électriques, tuyauteries…)
PHY_SRV.1	17	Absence de protection des accès aux équipements

Type d'entités	MA	Vulnérabilité
PHY_SRV.1	17	Absence de prise en compte des règles d'installation
PHY_SRV.1	19	Absence de protection des accès aux équipements terminaux de communication
PHY_SRV.1	23	Absence de contrôle (voire de traces) des échanges avec l'extérieur
PHY_SRV.1	25	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_SRV.1	26	Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects
PHY_SRV.1	30	Mauvais dimensionnement des ressources Télécom par exemple suite à l'exploitation au quotidien de ressources destinées à la solution de secours
PHY_SRV.1	33	Absence de sécurisation des lignes et équipements de communication
PHY_SRV.1	36	Absence de sécurisation des lignes et équipements de communication
PHY_SRV.1	38	Absence d'étiquetage des câbles ou de plan de câblage
PHY_SRV.1	38	Insuffisance d'espace des locaux techniques

4.5.2.2 PHY_SRV.2 : Énergie

Type d'entités	MA	Vulnérabilité
PHY_SRV.2	1	Présence d'ouverture sur la voie publique (fenêtre)
PHY_SRV.2	1	Absence de prise en compte dans la phase d'installation des risques d'incendie spécifiques aux équipements hébergés
PHY_SRV.2	1	Absence ou mauvais dimensionnement ou inadéquation du dispositif d'extinction automatique d'incendie
PHY_SRV.2	2	Câblage posé sur le sol
PHY_SRV.2	2	Plafond ou ouverture à l'extérieur non étanche
PHY_SRV.2	2	Accès non protégé aux locaux hébergeant les équipements de production ou de distribution des services essentiels
PHY_SRV.2	2	Canalisation d'eau à proximité des équipements de terminaison
PHY_SRV.2	12	Les locaux renfermant des batteries dont la composition est à base d'acide ne sont pas dédiés et isolés physiquement des matériels auxquels ils sont raccordés
PHY_SRV.2	12	Mauvais dimensionnement des dispositifs de secours énergie (onduleur, batteries…)
PHY_SRV.2	12	Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques
PHY_SRV.2	12	Les locaux renfermant des batteries dont la composition est à base d'acide ne sont pas munis de ventilation mécanique et aménagés électriquement en antidéflagrant
PHY_SRV.2	12	Les divers revêtements de sols ou muraux ne sont pas anti-statiques
PHY_SRV.2	12	Le tableau général basse tension n'est pas accessible
PHY_SRV.2	12	Le poste de transformation moyenne tension / basse tension n'est pas implanté sur le site (avec accès contrôlé du fournisseur)
PHY_SRV.2	12	Absence d'analyse de la puissance énergétique de secours nécessaire en cas d'ajout de matériel
PHY_SRV.2	12	Les masses et terres ne sont pas conformes à la réglementation
PHY_SRV.2	13	Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques ou moyens de télécommunication
PHY_SRV.2	17	Absence de prise en compte des règles d'installation
PHY_SRV.2	17	Absence de protection des accès aux équipements
PHY_SRV.2	17	Support facilitant la capture des signaux parasites compromettants (câbles électriques, tuyauteries…)
PHY_SRV.2	30	Mauvais dimensionnement des ressources de secours
PHY_SRV.2	38	Absence de procédure d'exploitation

4.5.2.3 PHY_SRV.3 : Refroidissement /pollution

Type d'entités	MA	Vulnérabilité
PHY_SRV.3	1	Absence de maintenance des équipements de climatisation
PHY_SRV.3	2	Vieillissement des canalisations de refroidissement

Type d'entités	MA	Vulnérabilité
PHY_SRV.3	2	Absence de maintenance des équipements de climatisation
PHY_SRV.3	2	Absence de vanne d'arrêt d'eau
PHY_SRV.3	3	Absence de maintenance des équipements de climatisation
PHY_SRV.3	3	Absence de matériel redondant suffisamment dimensionné
PHY_SRV.3	3	Vieillissement des filtres de climatisation
PHY_SRV.3	3	Accès non protégé aux équipements
PHY_SRV.3	11	Dispositif dépendant d'un fournisseur en eau glacé ou alimentation
PHY_SRV.3	11	Dispositif non suffisamment dimensionné par rapport aux besoins
PHY_SRV.3	11	Absence de maintenance des équipements de climatisation
PHY_SRV.3	11	Absence de matériel redondant suffisamment dimensionné
PHY_SRV.3	11	Accès non protégé aux dispositifs d'alimentation en eau et énergie
PHY_SRV.3	30	Mauvais dimensionnement des ressources de secours
PHY_SRV.3	38	Absence de procédure d'exploitation

4.6 ORG : Organisation

Type d'entités	MA	Vulnérabilité
ORG	1	Absence de couverture d'assurance en cas de sinistre grave
ORG	2	Absence de couverture d'assurance en cas de sinistre grave
ORG	34	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information

4.6.1 ORG_DEP : Organisation dont dépend l'organisme

Type d'entités	MA	Vulnérabilité
ORG_DEP	1	Absence de visite du site par les services de secours (pompiers)
ORG_DEP	1	Absence de norme pour l'installation des sites appartenant à l'organisme
ORG_DEP	2	Absence de norme pour l'installation des sites appartenant à l'organisme
ORG_DEP	3	Absence de norme pour l'installation des sites appartenant à l'organisme
ORG_DEP	4	Absence de service d'urgence proche de l'organisme
ORG_DEP	4	Absence de norme pour l'installation des sites appartenant à l'organisme
ORG_DEP	6	Absence de norme pour l'installation des sites appartenant à l'organisme
ORG_DEP	6	Absence de service d'urgence proche de l'organisme
ORG_DEP	7	Absence de norme pour l'installation des sites appartenant à l'organisme
ORG_DEP	7	Absence de service d'urgence proche de l'organisme
ORG_DEP	8	Absence de norme pour l'installation des sites appartenant à l'organisme
ORG_DEP	8	Absence de service d'urgence proche de l'organisme
ORG_DEP	9	Absence de service d'urgence proche de l'organisme
ORG_DEP	9	Absence de norme pour l'installation des sites appartenant à l'organisme
ORG_DEP	10	Absence de service d'urgence proche de l'organisme
ORG_DEP	10	Absence de norme pour l'installation des sites appartenant à l'organisme
ORG_DEP	11	Absence de norme pour l'installation des sites appartenant à l'organisme
ORG_DEP	12	Absence de norme pour l'installation des sites appartenant à l'organisme
ORG_DEP	13	Absence de norme pour l'installation des sites appartenant à l'organisme
ORG_DEP	17	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique
ORG_DEP	17	Absence de règles imposant l'utilisation de normes
ORG_DEP	18	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme
ORG_DEP	18	Absence de règles de protection pour l'échange d'informations à caractère confidentiel
ORG_DEP	19	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme
ORG_DEP	19	Absence de règles de protection pour l'échange d'informations à caractère confidentiel
ORG_DEP	20	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme
ORG_DEP	21	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme
ORG_DEP	22	Absence d'identification des biens sensibles
ORG_DEP	22	Absence de contrôle des biens sensibles
ORG_DEP	22	Absence de contrôle de l'application de la politique de sécurité
ORG_DEP	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut
ORG_DEP	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information
ORG_DEP	23	Absence d'identification des biens sensibles
ORG_DEP	23	La politique de sécurité n'est pas appliquée
ORG_DEP	23	Absence d'engagement personnel de protection de la confidentialité

Type d'entités	MA	Vulnérabilité
ORG_DEP	23	Procédures de gestion et d'application des habilitations trop lourde à exploiter
ORG_DEP	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous
ORG_DEP	23	Absence de contrôle des biens sensibles
ORG_DEP	23	Absence de politique de protection de l'information
ORG_DEP	24	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique
ORG_DEP	24	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme
ORG_DEP	26	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme
ORG_DEP	26	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique
ORG_DEP	27	Absence de politique de sécurité pour la protection de l'information applicable dans les sites de l'organisme
ORG_DEP	29	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)
ORG_DEP	29	Absence de règles imposant l'utilisation de normes
ORG_DEP	30	Absence de règles imposant l'utilisation de normes
ORG_DEP	30	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)
ORG_DEP	31	Absence de règles imposant l'utilisation de normes
ORG_DEP	31	Absence de suivi des incidents permettant de prévenir d'éventuelles pannes ou saturations (tableaux de bord)
ORG_DEP	32	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme
ORG_DEP	33	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur
ORG_DEP	33	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme
ORG_DEP	33	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique
ORG_DEP	34	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur
ORG_DEP	34	Absence de politique de contrôle des licences imposée aux sites de l'organisme
ORG_DEP	35	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur
ORG_DEP	35	Absence de politique de contrôle des licences imposée aux sites de l'organisme
ORG_DEP	36	Absence de règles et de procédure sur l'habilitation des personnels
ORG_DEP	36	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme
ORG_DEP	36	Absence de politique de protection de l'information imposée aux sites de l'organisme
ORG_DEP	36	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur
ORG_DEP	37	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information
ORG_DEP	37	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique
ORG_DEP	37	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur
ORG_DEP	37	Absence de politique de protection de l'information imposée aux sites de l'organisme
ORG_DEP	38	Absence d'un contrôle de l'organisme mère sur les processus critiques
ORG_DEP	39	Absence de politique de gestion et de contrôle des habilitations imposée aux sites de l'organisme

Type d'entités	MA	Vulnérabilité
ORG_DEP	39	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur
ORG_DEP	39	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique
ORG_DEP	40	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique
ORG_DEP	40	Absence de règles et de procédure sur l'habilitation des personnels
ORG_DEP	40	Absence de sensibilisation sur les risques de sanction
ORG_DEP	40	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur
ORG_DEP	40	Absence de procédure de contrôle
ORG_DEP	41	Changement de politique ou de stratégie d'organisation
ORG_DEP	41	Absence de définition des responsabilités
ORG_DEP	41	Absence de thème traitant des responsabilités de sécurité des systèmes d'information dans le règlement intérieur
ORG_DEP	41	Absence de procédures disciplinaires
ORG_DEP	41	Présence d'enjeu politico-économique fort
ORG_DEP	41	Absence de politique globale de gestion et d'archivage des traces et autres éléments de preuves
ORG_DEP	42	Présence d'un climat social défavorable
ORG_DEP	42	Présence d'un conflit politico-économique entre le pays d'appartenance de l'organisation et le pays accueillant l'organisation

4.6.2 ORG_GEN : Organisation de l'organisme

Type d'entités	MA	Vulnérabilité
ORG_GEN	1	Absence de gestion des procès verbaux de contrôle des équipements de secours
ORG_GEN	1	Absence d'affichage des informations à jour pour l'appel des services d'urgence
ORG_GEN	1	Absence d'organisation de lutte contre l'incendie (description des rôles, responsabilités)
ORG_GEN	1	Absence de suivi des contrats de maintenance des équipements de protection incendie
ORG_GEN	2	Absence de gestion des procès verbaux de contrôle des équipements de secours
ORG_GEN	2	Absence d'affichage des informations à jour pour l'appel des services d'urgence
ORG_GEN	2	Absence de consignes d'alerte, de réaction, d'information en cas de dégât des eaux (absence d'identification des vanne d'arrêts...)
ORG_GEN	2	Absence de garantie de bon fonctionnement des détecteurs de présence d'eau
ORG_GEN	3	Absence de suivi des contrats de maintenance
ORG_GEN	3	Absence de mesures en cas d'interruption du service de climatisation
ORG_GEN	4	Absence d'affichage des informations à jour pour l'appel des services d'urgence
ORG_GEN	4	Absence de couverture d'assurance en cas de sinistre grave
ORG_GEN	4	Absence d'organisation de gestion de crise
ORG_GEN	5	Absence de couverture d'assurance en cas de destruction de matériel
ORG_GEN	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)
ORG_GEN	6	Absence de consignes (alerte, prévention, réaction...)
ORG_GEN	7	Absence de consignes (alerte, prévention, réaction...)
ORG_GEN	8	Absence de consignes (alerte, prévention, réaction...)
ORG_GEN	9	Absence de consignes (alerte, prévention, réaction...)
ORG_GEN	10	Absence de consignes (alerte, prévention, réaction...)
ORG_GEN	11	Absence de consignes (alerte, prévention, réaction...)
ORG_GEN	12	Absence de consignes (alerte, prévention, réaction...)
ORG_GEN	13	Absence de consignes (alerte, prévention, réaction...)
ORG_GEN	17	Absence de contrôle de l'application de la politique de sécurité
ORG_GEN	17	Absence de politique de protection de l'information

Type d'entités	MA	Vulnérabilité
ORG_GEN	17	La politique de sécurité n'est pas appliquée
ORG_GEN	18	La politique de sécurité n'est pas appliquée
ORG_GEN	18	Absence d'identification des biens sensibles
ORG_GEN	18	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées
ORG_GEN	18	Absence de contrôle de l'application de la politique de sécurité
ORG_GEN	19	Absence de contrôle de l'application de la politique de sécurité
ORG_GEN	19	Absence d'identification des biens sensibles
ORG_GEN	19	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées
ORG_GEN	19	La politique de sécurité n'est pas appliquée
ORG_GEN	20	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous
ORG_GEN	20	La politique de sécurité n'est pas appliquée
ORG_GEN	20	Absence d'organisation de gestion des incidents de sécurité
ORG_GEN	20	Absence d'identification des biens sensibles
ORG_GEN	20	Absence de contrôle des biens sensibles
ORG_GEN	20	Absence de contrôle de l'application de la politique de sécurité
ORG_GEN	21	Absence d'organisation de gestion et de traitement des incidents de sécurité liés au vol
ORG_GEN	21	Absence de contrôle de l'application de la politique de sécurité
ORG_GEN	21	Absence de règles de contrôle des entrées/sorties des matériels dans l'organisme
ORG_GEN	21	Absence d'identification des biens sensibles
ORG_GEN	22	Absence d'identification des biens sensibles
ORG_GEN	22	Absence de contrôle des biens sensibles
ORG_GEN	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut
ORG_GEN	22	Absence de contrôle de l'application de la politique de sécurité
ORG_GEN	23	Absence de politique de protection de l'information
ORG_GEN	23	Absence de contrôle des biens sensibles
ORG_GEN	23	Absence d'engagement personnel de protection de la confidentialité
ORG_GEN	23	La politique de sécurité n'est pas appliquée
ORG_GEN	23	Absence d'identification des biens sensibles
ORG_GEN	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information
ORG_GEN	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous
ORG_GEN	23	Procédures de gestion et d'application des habilitations trop lourde à exploiter
ORG_GEN	24	Absence de contrôle de l'application de la politique de sécurité
ORG_GEN	24	Absence de politique de conservation et d'analyse des traces des activités
ORG_GEN	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête
ORG_GEN	24	Absence d'organisation permettant de garantir l'identification d'une personne au sein de l'organisme ou d'un projet
ORG_GEN	25	Absence de contrôle de l'application de la politique de sécurité
ORG_GEN	25	Absence de politique de sécurité pour la protection de l'infrastructure de traitement de l'information dans les sites de l'organisme
ORG_GEN	25	Les responsables n'ont pas de contact avec des services d'expertise ou de veille technologique
ORG_GEN	25	Absence de procédures de qualification opérationnelle
ORG_GEN	25	Absence de contrôle des biens sensibles
ORG_GEN	25	Absence d'identification des biens sensibles
ORG_GEN	25	Absence de procédures de validation des composants matériels lors de leur livraison ou de retour de maintenance
ORG_GEN	26	Absence de politique globale de lutte contre le code malveillant

Type d'entités	MA	Vulnérabilité
ORG_GEN	26	Absence d'identification des biens sensibles
ORG_GEN	26	Absence de contrôle de l'application de la politique de sécurité
ORG_GEN	26	Absence de contrôle des biens sensibles
ORG_GEN	26	Absence de politique de protection des postes de travail
ORG_GEN	26	Absence de politique de conservation et d'analyse des traces des activités
ORG_GEN	27	Absence de règles de protection en confidentialité des informations, exploitables pour localiser un personnel (demandes de billets, registre d'entrée/sortie…)
ORG_GEN	28	Absence d'organisation du suivi des contrats de maintenance
ORG_GEN	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs
ORG_GEN	28	Absence de reporting sur les pannes (les volumes, le coût des incidents, la durée)
ORG_GEN	28	Absence de règles traitant des conditions d'usage des infrastructures de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)
ORG_GEN	28	Absence de plan de reprise des activités essentielles de l'organisme
ORG_GEN	28	Absence de consignes de réaction rapide pour la protection des matériels en cas de dégât des eaux ou d'incendie
ORG_GEN	28	Absence d'organisation pour l'analyse de l'adéquation des besoins avec les capacités des équipements
ORG_GEN	29	Absence de reporting sur les dysfonctionnements
ORG_GEN	29	Absence de plan de reprise des activités essentielles de l'organisme
ORG_GEN	29	Absence de procédures de qualification opérationnelle
ORG_GEN	29	Absence de règles traitant de l'environnement d'exploitation des infrastructures de traitement de l'information (température, hydrométrie...)
ORG_GEN	29	Absence d'organisation pour l'analyse de l'adéquation des besoins avec les capacités des équipements
ORG_GEN	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours
ORG_GEN	30	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements conduisant à la saturation des espaces de stockage ou des ressources de traitement
ORG_GEN	30	Absence de consignes relatives aux incidents (détection, action...)
ORG_GEN	31	Absence de politique permettant le cloisonnement des environnements utilisateurs afin d'éviter d'accorder des droits de modification des systèmes et application
ORG_GEN	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque
ORG_GEN	31	Absence de consignes relatives aux incidents (détection, action...)
ORG_GEN	31	Absence de plan de reprise des activités essentielles de l'organisme
ORG_GEN	31	Absence d'homogénéité du parc informatique
ORG_GEN	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs
ORG_GEN	32	Absence de consignes relatives aux incidents (détection, action...)
ORG_GEN	32	Absence de Manuel d'Assurance Qualité
ORG_GEN	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes
ORG_GEN	32	Absence de plan de reprise des activités essentielles de l'organisme
ORG_GEN	32	Absence de procédures de gestion en configuration des systèmes
ORG_GEN	32	Non utilisation de normes ou standard dans le cadre du développement du système d'information
ORG_GEN	32	Absence de plan de formation à la maintenance des nouveaux systèmes
ORG_GEN	33	Absence de consignes relatives à l'utilisation du matériel informatique
ORG_GEN	33	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)
ORG_GEN	33	Absence de procédure de contrôle
ORG_GEN	33	La politique de sécurité n'est pas appliquée
ORG_GEN	33	Absence de sensibilisation sur les risques de sanction
ORG_GEN	33	Absence de charte informatique précisant les exigences d'utilisation

Type d'entités	MA	Vulnérabilité
ORG_GEN	34	Absence de charte informatique précisant les exigences d'utilisation
ORG_GEN	34	Absence de sensibilisation sur les risques de sanction
ORG_GEN	34	Absence de sensibilisation ou d'information sur la législation des droits d'auteur
ORG_GEN	34	Absence de procédure de contrôle
ORG_GEN	34	La politique de sécurité n'est pas appliquée
ORG_GEN	35	Absence de sensibilisation ou d'information sur la législation des droits d'auteur
ORG_GEN	35	Absence de contrôle de certification des produits
ORG_GEN	35	Absence de contrôle de l'origine des produits
ORG_GEN	35	Absence de charte informatique précisant les exigences d'utilisation
ORG_GEN	35	La politique de sécurité ne traite pas du rappel des obligations et des responsabilités de chacun en matière civile, pénale et réglementaire
ORG_GEN	36	Absence de contrôle de l'application de la politique de sécurité
ORG_GEN	36	Absence de consignes relatives à l'utilisation du matériel informatique
ORG_GEN	36	Absence de prévention et la détection des virus et d'autres logiciels malveillants
ORG_GEN	36	Absence de contrôle d'accès à l'information
ORG_GEN	36	Absence de plan de formation sur les problèmes de sécurité
ORG_GEN	36	Absence de politique des habilitations d'accès à l'information
ORG_GEN	36	Absence de procédures de contrôle des disquettes extérieures
ORG_GEN	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité...)
ORG_GEN	36	Absence de charte informatique précisant les exigences d'utilisation
ORG_GEN	36	Absence de règles et de procédure sur l'habilitation des personnels
ORG_GEN	37	Absence de consignes relatives aux incidents (détection, action...)
ORG_GEN	37	Absence de contrôle d'accès à l'information
ORG_GEN	37	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information
ORG_GEN	37	Absence de sensibilisation aux responsabilités individuelles
ORG_GEN	37	Absence de responsable de la protection des données et des informations liées aux individus
ORG_GEN	37	La politique de sécurité n'est pas appliquée notamment concernant le traitement des données nominatives
ORG_GEN	38	Absence de double contrôle sur les processus critiques
ORG_GEN	38	Absence de formation sur les matériels ou logiciels utilisés
ORG_GEN	39	Absence de définition du droit d'en connaître
ORG_GEN	39	Absence de dispositif de contrôle et de sanction
ORG_GEN	39	Absence d'un règlement définissant les droits
ORG_GEN	39	Les attributions des utilisateurs ne sont pas clairement définies
ORG_GEN	40	Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées
ORG_GEN	40	Absence de communication et d'information des procédures d'habilitation au personnel
ORG_GEN	40	Absence de procédure de remontée d'information en cas de détection
ORG_GEN	40	Absence de procédure d'habilitation du personnel
ORG_GEN	40	La politique de sécurité n'est pas appliquée
ORG_GEN	40	Organisation inadaptée
ORG_GEN	40	Absence de procédure de contrôle
ORG_GEN	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)
ORG_GEN	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes
ORG_GEN	41	Absence de définition des responsabilités
ORG_GEN	41	Changement de politique ou de stratégie d'organisation
ORG_GEN	41	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)
ORG_GEN	41	Absence de procédures disciplinaires
ORG_GEN	42	Absence d'équipe de protection du personnel

Type d'entités	MA	Vulnérabilité
ORG_GEN	42	Présence d'une épidémie virale locale
ORG_GEN	42	Absence de procédures de transfert de connaissances
ORG_GEN	42	Présence d'un climat social de l'organisation défavorable à l'activité
ORG_GEN	42	Présence d'un conflit politico-économique entre le pays d'appartenance de l'organisation et le pays accueillant l'organisation
ORG_GEN	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles
ORG_GEN	42	Absence de processus de gestion de la continuité des activités professionnelles de l'organisme

4.6.3 ORG_PRO : Organisation de projet ou d'un système

Type d'entités	MA	Vulnérabilité
ORG_PRO	1	Absence d'organisation de gestion de crise
ORG_PRO	2	Absence d'organisation de gestion de crise
ORG_PRO	4	Absence de couverture d'assurance en cas de sinistre grave
ORG_PRO	4	Absence d'organisation de gestion de crise
ORG_PRO	5	Absence de règles pour l'usage et le stockage des matériels et supports informatiques (conditions de protection lors du transport, interdiction de fumer…)
ORG_PRO	5	Absence de couverture d'assurance en cas de destruction de matériel
ORG_PRO	6	Absence de consignes (alerte, prévention, réaction...)
ORG_PRO	7	Absence de consignes (alerte, prévention, réaction...)
ORG_PRO	8	Absence de consignes (alerte, prévention, réaction...)
ORG_PRO	9	Absence de consignes (alerte, prévention, réaction...)
ORG_PRO	10	Absence de consignes (alerte, prévention, réaction...)
ORG_PRO	11	Absence de consignes (alerte, prévention, réaction...)
ORG_PRO	12	Absence de consignes (alerte, prévention, réaction...)
ORG_PRO	13	Absence de consignes (alerte, prévention, réaction...)
ORG_PRO	18	Absence de politique de protection de l'information
ORG_PRO	18	Absence d'identification des biens sensibles
ORG_PRO	18	Absence d'identification des besoins de sécurité d'un projet
ORG_PRO	19	Absence de politique de protection de l'information
ORG_PRO	19	Absence d'identification des biens sensibles
ORG_PRO	19	Absence d'identification des besoins de sécurité d'un projet
ORG_PRO	20	Absence d'identification des besoins de sécurité d'un projet
ORG_PRO	20	Absence de politique de protection de l'information
ORG_PRO	21	Absence d'identification des besoins de sécurité d'un projet
ORG_PRO	22	Absence de contrôle de l'application de la politique de sécurité
ORG_PRO	22	Absence de politique de protection de l'information applicable traitant du recyclage et de la mise au rebut
ORG_PRO	22	Absence d'identification des biens sensibles
ORG_PRO	22	Absence de contrôle des biens sensibles
ORG_PRO	23	Absence d'organisation responsable de la définition, de la mise en œuvre et du contrôle des privilèges d'accès à l'information
ORG_PRO	23	La politique de sécurité n'est pas appliquée
ORG_PRO	23	Absence de politique de protection de l'information
ORG_PRO	23	Absence d'engagement personnel de protection de la confidentialité
ORG_PRO	23	Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous
ORG_PRO	23	Absence d'identification des biens sensibles
ORG_PRO	23	Absence de contrôle des biens sensibles
ORG_PRO	23	Procédures de gestion et d'application des habilitations trop lourde à exploiter
ORG_PRO	24	Absence d'information concernant la répartition des responsabilités et les moyens de garantir la légitimité d'une requête

Type d'entités	MA	Vulnérabilité
ORG_PRO	24	Absence de contrôle de l'application de la politique de sécurité
ORG_PRO	24	Absence d'organisation permettant de garantir l'identification d'une personne au sein de l'organisme ou d'un projet
ORG_PRO	24	Absence de politique de conservation et d'analyse des traces des activités
ORG_PRO	25	Logiciel non suffisamment recetté notamment dans le cadre des valeurs aux limites
ORG_PRO	25	Absence de procédures de qualification opérationnelle
ORG_PRO	25	Absence de contrôle des biens sensibles
ORG_PRO	25	Absence de contrôle de l'application de la politique de sécurité
ORG_PRO	25	Absence de procédures de validation des composants matériels lors de leur livraison ou de retour de maintenance
ORG_PRO	25	Absence d'identification des biens sensibles
ORG_PRO	26	Absence de mesures de contrôle des développements
ORG_PRO	26	Absence de mesures de protection de l'intégrité des codes dans les phases de conception, installation et exploitation
ORG_PRO	26	Absence de politique de conservation et d'analyse des traces des activités
ORG_PRO	26	Absence d'identification des biens sensibles
ORG_PRO	27	Absence de règles de protection en confidentialité des informations, exploitables pour localiser un personnel (demandes de billets, registre d'entrée/sortie…)
ORG_PRO	28	Absence de suivi des contrats de maintenance et de support avec les fournisseurs
ORG_PRO	28	Absence d'organisation du suivi des contrats de maintenance
ORG_PRO	28	Absence d'organisation pour l'analyse de l'adéquation des besoins avec les capacités des équipements
ORG_PRO	28	Absence de reporting sur les pannes (les volumes, le coût des incidents, la durée)
ORG_PRO	28	Absence de règles traitant des conditions d'usage des infrastructure de traitement de l'information (interdiction dans les locaux hébergeant du matériel informatique de consommation de tabac, de boisson, d'aliments)
ORG_PRO	28	Absence de plan de reprise des activités essentielles de l'organisme
ORG_PRO	28	Absence de consignes de réaction rapide pour la protection des matériels en cas de dégât des eaux ou d'incendie
ORG_PRO	29	Absence d'organisation pour l'analyse de l'adéquation des besoins avec les capacités des équipements
ORG_PRO	29	Absence de reporting sur les dysfonctionnements
ORG_PRO	29	Absence de règles traitant de l'environnement d'exploitation des infrastructures de traitement de l'information (température, hydrométrie...)
ORG_PRO	29	Absence de procédures de qualification opérationnelle
ORG_PRO	29	Absence de plan de reprise des activités essentielles de l'organisme
ORG_PRO	30	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements conduisant à la saturation des espaces de stockage ou des ressources de traitement
ORG_PRO	30	Absence de politique de suivi du bon dimensionnement des équipements de l'infrastructure de traitement de l'information, y compris des équipements de secours
ORG_PRO	31	Absence de plan de reprise des activités essentielles de l'organisme
ORG_PRO	31	Logiciel non suffisamment recetté (ensemble de jeux de test ne couvrant pas la totalité des conditions de fonctionnement -sollicitation intense du système, entrée de données non conformes, entrée de données correspond aux limites de fonctionnement)
ORG_PRO	31	Absence de consignes de bon usage des ressources informatiques afin d'éviter des comportements à risque
ORG_PRO	32	Non utilisation de normes ou standard dans le cadre du développement du système d'information
ORG_PRO	32	Absence de plan de reprise des activités essentielles de l'organisme
ORG_PRO	32	Absence d'organisation de protection des documentations et moyens de maintenance des systèmes
ORG_PRO	32	Absence de consignes relatives aux incidents (détection, action...)
ORG_PRO	32	Absence de suivi des contrats de maintenance et de support avec les fournisseurs

Type d'entités	MA	Vulnérabilité
ORG_PRO	32	Absence de procédures de gestion en configuration des systèmes
ORG_PRO	32	Absence de Manuel d'Assurance Qualité
ORG_PRO	32	Absence de plan de formation à la maintenance des nouveaux systèmes
ORG_PRO	33	Absence de consignes relatives à l'utilisation du matériel informatique
ORG_PRO	33	Absence de sensibilisation sur les risques de sanction
ORG_PRO	33	Absence de procédure de contrôle
ORG_PRO	34	Absence de sensibilisation ou d'information sur la législation des droits d'auteur
ORG_PRO	34	Absence de sensibilisation sur les risques de sanction
ORG_PRO	34	Absence de procédure de contrôle
ORG_PRO	35	Absence de sensibilisation ou d'information sur la législation des droits d'auteur
ORG_PRO	35	Absence de définition de privilèges limitant la possibilité d'installation sur les postes de travail
ORG_PRO	36	Absence de plan de formation sur les problèmes de sécurité
ORG_PRO	36	Absence de contrôle de l'application de la politique de sécurité
ORG_PRO	36	Absence de charte informatique précisant les exigences d'utilisation
ORG_PRO	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité...)
ORG_PRO	36	Absence de politique des habilitations d'accès à l'information
ORG_PRO	36	Absence de prévention et la détection des virus et d'autres logiciels malveillants
ORG_PRO	36	Absence de procédures de contrôle des disquettes extérieures
ORG_PRO	36	Absence de consignes relatives à l'utilisation du matériel informatique
ORG_PRO	37	Manque d'informations sur les lois et les règlements appliqués au traitement de l'information
ORG_PRO	37	Absence de sensibilisation du personnel
ORG_PRO	37	Absence de consignes relatives aux incidents (détection, action...)
ORG_PRO	37	Absence de protection et d'audit d'accès aux informations sensibles
ORG_PRO	37	Absence de dispositif de contrôle et de sanction
ORG_PRO	37	Absence de responsable de la protection des données et des informations liées aux individus
ORG_PRO	38	Absence de formation sur les matériels ou logiciels utilisés
ORG_PRO	38	Absence de double contrôle sur les processus critiques
ORG_PRO	39	Absence de contrôle sur les attributions des droits des utilisateurs
ORG_PRO	39	Absence d'un règlement définissant les droits
ORG_PRO	39	Absence de définition du droit d'en connaître
ORG_PRO	40	Absence de procédure d'habilitation du personnel
ORG_PRO	40	Organisation inadaptée
ORG_PRO	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)
ORG_PRO	40	Absence de climat de confiance entre les individus
ORG_PRO	41	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)
ORG_PRO	41	Absence d'organisation hiérarchique et de procédure de reporting
ORG_PRO	41	Absence de procédures disciplinaires
ORG_PRO	41	Absence de mécanisme de suivi d'action, de journaux d'événements et d'alertes
ORG_PRO	41	Changement de politique ou de stratégie d'organisation
ORG_PRO	41	Absence de définition des responsabilités
ORG_PRO	41	Absence de fonctions d'audit séparées des fonctions de suivi
ORG_PRO	42	Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles
ORG_PRO	42	Absence de procédures de transfert de connaissances
ORG_PRO	42	Sous-dimensionnement de l'organisation
ORG_PRO	42	Non redondance du personnel stratégique
ORG_PRO	42	Absence d'organisation redondante des fonctions sensibles
ORG_PRO	42	Absence de processus de gestion de la continuité des activités professionnelles de l'équipe projet

Type d'entités	MA	Vulnérabilité
ORG_PRO	42	Absence de base documentaire des règles et procédures

4.6.4 ORG_EXT : Sous-traitant/Fournisseurs/Industriels

Type d'entités	MA	Vulnérabilité
ORG_EXT	1	Absence de clauses contractuelles pour le recouvrement des activités dans le cas d'une crise déclarée chez le fournisseur
ORG_EXT	1	Absence de consignes de sécurité fournies aux personnes extérieures intervenant dans les locaux
ORG_EXT	2	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs
ORG_EXT	2	Absence de consignes de sécurité fournies aux personnes extérieures intervenant dans les locaux
ORG_EXT	4	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs
ORG_EXT	5	Absence de consignes fournies aux personnes extérieures intervenant dans les locaux
ORG_EXT	6	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs
ORG_EXT	7	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs
ORG_EXT	8	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs
ORG_EXT	9	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs
ORG_EXT	10	Absence de clauses contractuelles dans le cas d'une crise déclarée chez des sous-traitants ou fournisseurs
ORG_EXT	11	Absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service essentiel
ORG_EXT	11	Absence de clauses contractuelles traitant de la réparation du préjudice en cas d'arrêt de la fourniture d'un service essentiel
ORG_EXT	12	Absence de clauses contractuelles traitant de la réparation du préjudice en cas d'arrêt de la fourniture d'un service essentiel
ORG_EXT	12	Absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service essentiel
ORG_EXT	13	Absence de clauses contractuelles traitant de la réparation du préjudice en cas d'arrêt de la fourniture d'un service essentiel
ORG_EXT	13	Absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service essentiel
ORG_EXT	14	Absence de clause contractuelle liée à la compatibilité électromagnétique
ORG_EXT	17	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs
ORG_EXT	17	Absence de procédure de vérification des matériels avant achat ou après une maintenance
ORG_EXT	18	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs
ORG_EXT	19	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs
ORG_EXT	20	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs
ORG_EXT	21	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs
ORG_EXT	22	Absence de clauses contractuelles traitant des mesures de sécurité à respecter par les sous-traitants et fournisseurs
ORG_EXT	24	Absence de moyens permettant de garantir la provenance des fournitures

Type d'entités	MA	Vulnérabilité
ORG_EXT	25	Absence de procédure pour le contrôle des interventions de personnel extérieur sur les équipements de l'organisme
ORG_EXT	26	Absence de procédure pour le contrôle des interventions de personnel extérieur sur les équipements de l'organisme
ORG_EXT	26	Absence de clauses contractuelles traitant de la garantie d'innocuité des fournitures livrées par le sous-traitant ou fournisseur
ORG_EXT	28	Absence de clause traitant des délais d'intervention et de remplacement en cas de panne matérielle
ORG_EXT	29	Absence de clause traitant des délais d'intervention et de traitement en cas de dysfonctionnement
ORG_EXT	30	Absence de clause contractuelle traitant de la qualité de service des systèmes placés dans des conditions limites (sollicitation intense du système, entrée de données non conformes, entrée de données correspond aux limites de fonctionnement)
ORG_EXT	31	Absence des clauses contractuelles traitant des conditions de support et d'intervention
ORG_EXT	32	Absence de clause contractuelle assurant le recouvrement de l'activité (en cas de cessation de l'activité, en cas de faillite du fournisseur...)
ORG_EXT	32	Absence de garantie relative à la pérennité de l'organisme
ORG_EXT	33	Absence de sensibilisation sur les risques de sanction
ORG_EXT	33	Absence de clauses relatives à l'utilisation du matériel informatique dans le contrat
ORG_EXT	34	Absence de clauses sur l'utilisation de copie frauduleuse de logiciels dans le contrat
ORG_EXT	35	Absence de clauses sur l'identification et la vérification de l'origine du logiciel dans le contrat
ORG_EXT	36	Absence de politique des habilitations d'accès à l'information
ORG_EXT	36	Absence de sécurisation des accès au SI (passerelles, détection d'intrusion, supervision des événements de sécurité...)
ORG_EXT	36	Absence de clauses relatives à la protection du matériel informatique dans le contrat
ORG_EXT	37	Absence de clause de confidentialité dans le contrat
ORG_EXT	37	Absence de dispositif de contrôle et de sanction
ORG_EXT	38	Absence de double contrôle sur les processus critiques
ORG_EXT	39	Absence des clauses contractuelles limitant les responsabilités des 2 parties
ORG_EXT	40	Possibilité d'utiliser les ressources de l'organisme sans contrôle (matériel en libre service...)
ORG_EXT	40	Absence de protection des espaces dédiés à l'échange ou au partage d'information
ORG_EXT	40	Absence de procédure d'habilitation du personnel
ORG_EXT	40	Absence de climat de confiance entre les individus
ORG_EXT	41	Absence de clause relative à la définition des procédures de communication et d'échange dans le contrat
ORG_EXT	41	Absence de contrôle mutuel des codes
ORG_EXT	41	Présence de clause de pénalité ou de sanction démesurée ou non adaptée au contexte
ORG_EXT	42	Absence de clause ou de procédures de transfert des connaissances
ORG_EXT	42	Absence de pérennité financière ou technologique de l'organisme
ORG_EXT	42	Absence de clause de continuité de la fourniture du service

4.7 SYS : Système

Type d'entités	MA	Vulnérabilité
SYS	19	Circulation en clair des échanges
SYS	23	Le système est connecté à des réseaux externes
SYS	32	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs
SYS	32	Utilisation d'une version obsolète du serveur de messagerie
SYS	32	Utilisation de système obsolète
SYS	32	Utilisation de système non standard
SYS	32	Absence de suivi des procédures d'installation et de maintenance (cahiers de configuration et de paramétrage)
SYS	32	Absence de moyen de support interne
SYS	33	Le dispositif utilisé permet un autre usage que celui qui est prévu
SYS	33	Absence d'audit ou de supervision des accès (notamment inventaire des accès avec l'extérieur de l'organisme et typologie des flux)
SYS	33	Absence de règle d'accès
SYS	33	Le dispositif est connecté à des réseaux externes
SYS	33	Le dispositif est accessible par tous
SYS	34	Aucune vérification de l'origine n'est faite avant l'installation des applicatifs
SYS	34	Le dispositif d'accès permet le stockage de logiciels
SYS	34	Le dispositif d'accès permet le téléchargement de logiciels
SYS	35	Aucune vérification de l'origine n'est faite avant l'installation des applicatifs
SYS	35	Le dispositif d'accès permet le stockage de logiciels
SYS	35	Le dispositif d'accès permet le téléchargement de logiciels
SYS	38	Insuffisance de compétence pour l'utilisateur
SYS	38	Absence de mesure de protection (lecture seule…)
SYS	38	Absence de responsabilité
SYS	38	Absence de support à l'utilisateur accessible
SYS	38	Absence d'outil de supervision
SYS	39	Le dispositif est accessible par tous
SYS	39	Absence de politique d'audit
SYS	39	Le principe du moindre privilège n'est pas appliqué
SYS	39	Absence de journalisation des événements
SYS	41	Absence de journalisation des événements
SYS	41	Le dispositif d'accès ne journalise pas les traces issues de son exploitation
SYS	41	L'accès au dispositif de traces n'est pas protégé
SYS	41	Absence de politique d'audit
SYS	41	Le dispositif est accessible par tous (ex: dispositif n'authentifiant pas les postes client ni les utilisateurs)
SYS	41	Le dispositif est connecté à des réseaux externes

4.7.1 SYS_INT : Dispositif d'accès Internet

Type d'entités	MA	Vulnérabilité
SYS_INT	19	Absence de protection des journaux récoltant la trace des activités
SYS_INT	23	Absence de journalisation des accès
SYS_INT	23	Absence de dispositif de filtrage
SYS_INT	24	Le dispositif permet d'accéder à des données non authentifiables (ex. : hoax)
SYS_INT	24	Le système ne dispose pas de moyen de conservation de l'historique des activités
SYS_INT	26	Absence de sensibilisation aux risques induits par le téléchargement de logiciels
SYS_INT	26	Absence de contrôle anti-virus des échanges
SYS_INT	26	Le dispositif permet d'exploiter le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation (ex. : composants javascript explorant le contenu du disque dur)
SYS_INT	30	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans

Type d'entités	MA	Vulnérabilité
		limitation
SYS_INT	30	Mauvais dimensionnement des ressources (ex. : trop d'utilisateurs par rapport aux nombres possibles de connexions et à la bande passante)
SYS_INT	31	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation
SYS_INT	31	Non-respect des procédures d'installation ou de maintenance
SYS_INT	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance
SYS_INT	36	Le dispositif permet d'introduire des logiciels hostiles tel que chevaux de Troie, virus, vers, bombes logiques…
SYS_INT	36	Le dispositif permet d'exploiter le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation (ex. : composants javascript explorant le contenu du disque dur)
SYS_INT	37	Absence d'audit ou de supervision des accès
SYS_INT	37	Absence de contrôle de contenu
SYS_INT	37	Absence de gestion d'habilitation des accès
SYS_INT	37	Absence d'identification des niveaux de protection des systèmes
SYS_INT	37	Le dispositif est connecté à des réseaux externes
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations
SYS_INT	37	Le dispositif facilite la divulgation à l'extérieur d'informations
SYS_INT	40	Absence de journalisation des événements
SYS_INT	40	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow)
SYS_INT	40	Le dispositif est accessible par tous
SYS_INT	40	Absence de politique d'audit

4.7.2 SYS_MES : Messagerie

Type d'entités	MA	Vulnérabilité
SYS_MES	19	Possibilité d'introduire sur les clients un logiciel d'écoute
SYS_MES	19	Possibilité de pose d'un dispositif d'écoute logique sur les passerelles de messagerie
SYS_MES	19	Lacunes dans la gestion des privilèges d'accès aux passerelles de messagerie
SYS_MES	23	Absence de mesure permettant d'éviter une négligence lors de l'envoi d'informations
SYS_MES	23	Le système est utilisable par tout le personnel
SYS_MES	23	Le système permet l'échange de pièces jointes
SYS_MES	23	Absence de protection anti-virus efficace et opérationnelle
SYS_MES	24	Le système permet l'émission et la réception d'information sans authentification des émetteurs ni des destinataires
SYS_MES	24	Le système ne dispose pas de filtre pour empêcher la réception de canulars provenant de l'extérieur
SYS_MES	24	Le système permet le relayage
SYS_MES	26	Possibilité d'administrer le système à distance
SYS_MES	26	Utilisation d'une version obsolète du serveur de messagerie
SYS_MES	26	Utilisation de liste de diffusion incluant une grande partie des personnels
SYS_MES	26	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés
SYS_MES	26	Présence de protocole ne disposant pas de fonction d'authentification
SYS_MES	26	La messagerie permet l'émission automatique de messages
SYS_MES	26	Absence de sensibilisation aux risques induits par l'exécution de pièces jointes
SYS_MES	26	La messagerie permet d'exploiter le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation (ex: lancement automatique des pièces jointes)
SYS_MES	26	La liaison de télémaintenance est activée en permanence
SYS_MES	26	Insuffisance de la complexité des mots de passe de connexion
SYS_MES	26	Aucune vérification des applicatifs n'est faite avant l'installation

Type d'entités	MA	Vulnérabilité
SYS_MES	26	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels
SYS_MES	26	La messagerie permet d'installer des mises à jour logicielles (ex. : patches, antivirus...)
SYS_MES	26	Absence de moyens de filtrage anti-virus
SYS_MES	26	Possibilité d'administrer le système à distance depuis n'importe quel poste
SYS_MES	30	Utilisation de liste de diffusion interne accessibles à tous
SYS_MES	30	Mauvais dimensionnement des espaces de stockage des messages reçus
SYS_MES	30	La messagerie permet l'émission automatique de messages
SYS_MES	30	Absence de protection contre le spam
SYS_MES	30	Absence de limitation des tailles des pièces jointes
SYS_MES	30	Mauvais usage des utilisateurs du service de messagerie (utilisation des boîtes aux lettres comme espace d'archivage)
SYS_MES	30	Existence de période ou d'événement provoquant une augmentation très significative de l'usage du système
SYS_MES	31	Aucune vérification des applicatifs n'est faite avant l'installation
SYS_MES	31	Incompatibilité logiciel (ex. : effet de bord d'un logiciel anti-virus filtrant les messages...)
SYS_MES	31	Non-respect des procédures d'installation ou de maintenance
SYS_MES	31	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow, déni de service sur serveur SMTP, POP3, IMAP)
SYS_MES	31	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs
SYS_MES	31	Utilisation d'une version obsolète du serveur de messagerie
SYS_MES	36	La messagerie permet d'exploiter le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation (ex: lancement automatique des pièces jointes)
SYS_MES	36	Absence de procédure de sauvegarde
SYS_MES	36	Aucune vérification des applicatifs n'est faite avant l'installation
SYS_MES	36	Insuffisance de la complexité des mots de passe de connexion
SYS_MES	36	Possibilité d'administrer le système à distance depuis n'importe quel poste
SYS_MES	36	La liaison de télémaintenance est activée en permanence
SYS_MES	36	Absence de mise en œuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels
SYS_MES	36	Possibilité d'administrer le système à distance
SYS_MES	36	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés
SYS_MES	36	La couche SNMP est activée
SYS_MES	37	Absence d'audit ou de supervision des accès
SYS_MES	37	Absence de contrôle de contenu
SYS_MES	37	Absence de gestion d'habilitation des accès
SYS_MES	37	Absence d'identification des niveaux de protection des systèmes
SYS_MES	37	Le dispositif est connecté à des réseaux externes
SYS_MES	37	Le dispositif facilite la divulgation à l'extérieur d'informations
SYS_MES	40	Possibilité d'administrer le système à distance depuis n'importe quel poste
SYS_MES	40	Aucune vérification des applicatifs n'est faite avant l'installation
SYS_MES	40	Insuffisance de la complexité des mots de passe de connexion
SYS_MES	40	La couche SNMP est activée
SYS_MES	40	La liaison de télémaintenance est activée en permanence
SYS_MES	40	Le dispositif de messagerie est accessible depuis Internet
SYS_MES	40	Possibilité d'administrer le système à distance
SYS_MES	40	Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés
SYS_MES	40	Le dispositif est accessible par tous
SYS_MES	40	Absence de politique d'audit
SYS_MES	40	Utilisation d'une version obsolète du serveur de messagerie

Type d'entités	MA	Vulnérabilité
SYS_MES	40	Utilisation d'une version obsolète du système d'exploitation ou des applicatifs
SYS_MES	40	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow)
SYS_MES	40	Absence de journalisation des événements

4.7.3 SYS_ITR : Intranet

Type d'entités	MA	Vulnérabilité
SYS_ITR	19	Absence de protection des journaux récoltant la trace des activités
SYS_ITR	19	Absence de cloisonnement des réseaux de communication
SYS_ITR	19	Possibilité d'écouter des échanges avec les serveurs d'authentification
SYS_ITR	19	Possibilité d'écouter des échanges avec les serveurs d'application
SYS_ITR	23	Absence ou difficulté à gérer les privilèges d'accès aux informations partagés (définition, mise en œuvre, contrôle)
SYS_ITR	23	Absence de cloisonnement des réseaux de communication
SYS_ITR	24	Le système ne dispose pas de moyen de conservation de l'historique des activités
SYS_ITR	24	Le système permet le stockage ou la modification d'information sans authentification de leurs auteurs
SYS_ITR	26	Présence de dispositif pour modifier ou installer des applications à distance
SYS_ITR	26	Utilisation d'espace de stockage partagé
SYS_ITR	30	Absence de gestion des droits d'écriture sur les espaces de stockage partagés
SYS_ITR	30	Mauvais dimensionnement des ressources (ex: espace de stockage ou de partage de fichier trop limitée)
SYS_ITR	30	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation
SYS_ITR	30	Absence de cloisonnement des réseaux de communication
SYS_ITR	31	Non-respect des procédures d'installation ou de maintenance
SYS_ITR	31	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow, déni de service sur serveur LDAP)
SYS_ITR	36	Le dispositif permet d'effacer de modifier ou d'installer des programmes à distance
SYS_ITR	36	Le dispositif permet d'introduire des logiciels hostiles tel que chevaux de Troie, virus, vers, bombes logiques…
SYS_ITR	36	Absence de procédure de sauvegarde
SYS_ITR	36	Absence de cloisonnement des réseaux de communication
SYS_ITR	36	Le dispositif permet d'exploiter le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation (ex. : composants javascript explorant le contenu du disque dur)
SYS_ITR	37	Absence de contrôle de contenu
SYS_ITR	37	Absence d'identification des niveaux de protection des systèmes
SYS_ITR	37	Absence d'audit ou de supervision des accès
SYS_ITR	37	Absence de gestion d'habilitation des accès
SYS_ITR	37	Le dispositif est connecté à des réseaux externes
SYS_ITR	40	Le dispositif est accessible par tous
SYS_ITR	40	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow)
SYS_ITR	40	Absence de journalisation des événements
SYS_ITR	40	Absence de politique d'audit

4.7.4 SYS_ANU : Annuaire d'entreprise

Type d'entités	MA	Vulnérabilité
SYS_ANU	23	Absence de contrôle d'accès aux informations stockés dans l'annuaire
SYS_ANU	24	Possibilité d'usurper la fonction de l'annuaire
SYS_ANU	24	Le système ne permet pas d'identifier l'auteur d'une modification

Type d'entités	MA	Vulnérabilité
SYS_ANU	26	Possibilité d'existence de fonctions cachées introduites en phase de conception et développement
SYS_ANU	26	Possibilité de modifier ou changer des applicatifs
SYS_ANU	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes
SYS_ANU	30	Mauvais dimensionnement des ressources (ex: trop d'utilisateurs par rapport à la capacité maximale de l'annuaire)
SYS_ANU	30	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation
SYS_ANU	30	Existence de période ou d'événement provoquant une augmentation très significative de l'usage du système
SYS_ANU	31	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow, déni de service sur serveur LDAP)
SYS_ANU	31	Non-respect des procédures d'installation ou de maintenance
SYS_ANU	36	Absence de procédure de sauvegarde
SYS_ANU	37	Absence d'identification des niveaux de protection des systèmes
SYS_ANU	37	Absence de contrôle de contenu
SYS_ANU	37	Absence d'audit ou de supervision des accès
SYS_ANU	37	Absence de gestion d'habilitation des accès
SYS_ANU	37	Le dispositif facilite la divulgation à l'extérieur d'informations
SYS_ANU	37	Le dispositif est connecté à des réseaux externes
SYS_ANU	40	Absence de journalisation des événements
SYS_ANU	40	Le dispositif est accessible par tous
SYS_ANU	40	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow)
SYS_ANU	40	Absence de politique d'audit

4.7.5 SYS_WEB : Portail externe

Type d'entités	MA	Vulnérabilité
SYS_WEB	19	Absence de protection des journaux récoltant la trace des activités
SYS_WEB	23	Absence de gestion des privilèges d'accès aux informations (possibilité d'altérer des informations publiques...)
SYS_WEB	23	Le système facilite la divulgation à l'extérieur d'informations
SYS_WEB	24	Le système ne permet pas l'identification de la personne ayant émis une requête
SYS_WEB	24	Le système ne dispose pas de moyen de conservation de l'historique des activités
SYS_WEB	26	Possibilité de modifier ou changer des applicatifs
SYS_WEB	26	Possibilité de créer ou modifier des commandes systèmes
SYS_WEB	26	Possibilité d'effacer ou modifier des programmes ou fichiers systèmes
SYS_WEB	26	Possibilité d'implanter des programmes pirates
SYS_WEB	26	Possibilité d'existence de fonctions cachées introduites en phase de conception et développement
SYS_WEB	30	Accès public au portail
SYS_WEB	30	Existence de période ou d'événement provoquant une augmentation très significative de l'usage du système
SYS_WEB	30	Mauvais dimensionnement des ressources (ex: trop de connexions simultanées)
SYS_WEB	30	Possibilité de soumettre le dispositif à un nombre trop important de requêtes sans limitation
SYS_WEB	31	Possibilité que le dispositif soit soumis à des requêtes ou données mal formées (ex: buffer overflow, déni de service sur serveur SMTP, POP3, IMAP)
SYS_WEB	31	Non-respect des procédures d'installation ou de maintenance
SYS_WEB	36	Absence de procédure de sauvegarde
SYS_WEB	36	Absence d'audit ou de supervision des accès
SYS_WEB	36	Absence de règle d'accès
SYS_WEB	37	Absence d'audit ou de supervision des accès
SYS_WEB	40	Le dispositif est accessible par tous

Type d'entités	MA	Vulnérabilité
SYS_WEB	40	Absence de politique d'audit
SYS_WEB	40	Absence de journalisation des événements

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?
.....
.....

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution