ANNEXE 3

BASES DE CONNAISSANCES

Table des matières

1- Introduction 4

2- Types de biens supports 5

2.1- SYS – Systèmes informatiques et de téléphonie[1] 5

MAT – Matériels 5

LOG – Logiciels 6

RSX – Canaux informatiques et de téléphonie 6

2.2- ORG – Organisations 7

PER – Personnes 7

PAP – Supports papier 7

CAN – Canaux interpersonnels 7

2.3- LOC - Locaux 7

3- Types d'impacts 8

3.1- Impacts sur le fonctionnement 8

Impacts sur les missions 8

Impacts sur la capacité de décision 8

3.2- Impacts humains 8

Impacts sur la sécurité des personnes 8

Impacts sur le lien social interne 8

3.3- Impacts sur les biens 8

Impacts sur le patrimoine intellectuel ou culturel 8

Impacts financiers 8

Impacts sur l'image 8

3.4- Autres impacts 8

Impacts de non-conformité 8

Impacts juridiques 8

Impacts sur l'environnement 9

4- Types de sources de menaces 9

4.1- Sources humaines agissant de manière délibérée 9

Source humaine interne, malveillante, ... 9

Source humaine externe, malveillante, ... 9

4.2- Sources humaines agissant de manière accidentelle 9

Source humaine interne, sans intention de nuire, ... 9

Source humaine externe, sans intention de nuire, ... 10

4.3- Sources non humaines 10

Code malveillant d'origine inconnue 10

Phénomène naturel 10

5- Menaces et vulnérabilités génériques 10

5.1- Menaces sur les matériels 11

5.2- Menaces sur les logiciels 11

5.3- Menaces sur les canaux informatiques et de téléphonie 11

5.4- Menaces sur les personnes 12

5.5- Menaces sur les canaux interpersonnels 12

6- Mesures de sécurité génériques 12

6.1- Mesures de sécurité issues du [RGS] 12

6.2- Mesures de sécurité issues de l'Arrêté Ministériel en application de l'article 18 de la loi n°1.430 portant diverses mesures relatives à la sécurité nationale.....12

6.3- Fonctions de sécurité 13

1- Introduction

Cette annexe présente les bases de connaissances afin d'aider à rédiger les expressions des besoins de sécurité et à identifier des objectifs de sécurité.

Cela concerne les types de :

- biens supports,
- impacts,
- sources de menaces,
- menaces et vulnérabilités,
- mesures de sécurité.

Elles ne sont pas nécessaires pour utiliser la méthode, mais constituent une aide précieuse pour gérer les risques de sécurité de l'information.

Il est important de bien noter que ces bases de connaissances :

- ne constituent qu'une aide et ne sauraient remplacer le savoir et le savoir-faire des experts,
- restent bien évidemment toujours améliorables (enrichissement, rectifications…),
- traitent de sécurité de l'information, donc ne sont pas directement applicables à d'autres fins.

Cette base de connaissance est issue de la base de connaissance de la méthode EBIOS. Il est conseillé pour un travail plus approfondi de se référer à cette base que l'on trouve :

https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

2- Types de biens supports

Les types de biens supports représentent les grandes catégories de composants d'un système d'information sur lesquels reposent les biens essentiels et/ou les mesures de sécurité.

Les biens supports sont :

- les systèmes informatiques et de téléphonie (SYS), qui peuvent être décomposés en :
  - matériels (MAT),
  - logiciels (LOG),
  - canaux informatiques et de téléphonie (RSX) ;
- les organisations (ORG), qui peuvent être décomposées en :
  - personnes (PER),
  - supports papier (PAP),
  - canaux interpersonnels (CAN) ;
- les locaux (LOC), qui hébergent les autres biens supports et fournissent les ressources.

Note : les solutions de sécurité (procédures, produits…) ne sont pas considérées comme des biens supports ; elles sont en effet prises en compte en cours d'étude dans les "mesures de sécurité existantes" ou à la fin de l'étude dans les "mesures de sécurité" destinées à traiter les risques. Les risques liés à ces mesures de sécurité (induits du fait de leur intégration dans le système ou intrinsèques) doivent être gérés lors du traitement des risques afin de ne pas biaiser l'étude. De même, un type d'un haut niveau hiérarchique se verra affecté des biens essentiels liés aux types des niveaux inférieurs.

Chaque type fait l'objet d'une description. Les exemples figurent en *italique*.

2.1- SYS – Systèmes informatiques et de téléphonie[1]

Ce type de biens supports est constitué de la combinaison de matériels (MAT), de logiciels (LOG) et de canaux informatiques et de téléphonie (RSX) en interaction, organisés pour élaborer, traiter, stocker, acheminer, présenter ou détruire tout ou partie des biens essentiels.

Tel ordinateur isolé, tel réseau ou combinaison de réseaux (petit réseau local, réseau Ethernet d'entreprise, réseau local à jeton – token ring, réseau mobile, réseau sans fil en maillage complet, réseau sans fil à maillage partiel – point à point, point à multipoints, multipoints à multipoints ou métropolitain, réseau point à point, réseau en grille, réseau toroïdal ou en hypercube), telle interconnexion.

MAT – Matériels

Ce type de biens supports est constitué de l'ensemble des éléments physiques d'un système informatique (*hardware* et des supports de données électroniques) participant au stockage et au traitement de tout ou partie des biens essentiels.

Il peut être utile de différencier les matériels selon la typologie suivante.

Ordinateur

Serveur, poste de travail, ordinateur central (mainframe), centre multimédia (media center), micro-ordinateur portable, assistant personnel (PDA), ardoise électronique.

Périphérique informatique

Imprimante, scanner, copieur multifonctions, périphérique de sauvegarde amovible (lecteur/graveur

CD-ROM ou DVD-ROM…), microphone, caméra, télécommande.

Périphérique de téléphonie

Téléphone analogique fixe, téléphone analogique sans fil, téléphone IP, téléphone mobile.

Relais de communication

Pont, routeur, hub, commutateur téléphonique (PABX, IPBX), modem.

Support électronique

Cédérom, DVD-Rom, clé USB, cartouche de sauvegarde, disque dur amovible, bande, carte mémoire (Compact Flash, Memory Stick, Multimedia Card, Secure Digital, Smartmedia…), disquette, cassettes.

LOG – Logiciels

Ce type de biens supports est constitué de l'ensemble des programmes participant au traitement de tout ou partie des biens essentiels (*software*).

Il peut être utile de différencier les logiciels selon la typologie suivante.

Application

Navigateur web, portail web, client de courrier électronique, suite bureautique, logiciel de comptabilité, téléprocédure administrative, application de pilotage de machine-outil, forum de discussion, logiciel réseau.

Système de gestion de base de données

Ingres, PostgreSQL, DB2, Oracle, SQL Server, Informix.

Intergiciel (middleware)

EAI (Enterprise Application Integration), ETL (Extract-Transform-Load), CORBA (Common Object Request Broker Architecture), ODBC (Open DataBase Connectivity), NEXUS, ORB (Open Request Broker).

Système d'exploitation

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

Micrologiciel (firmware)

BIOS (Basic Input Output System), gestionnaire de composants d'un téléphone mobile, programme stocké dans une clé USB équipée d'un microprocesseur.

RSX – Canaux informatiques et de téléphonie

Ce type de biens supports est constitué de l'ensemble des vecteurs physiques de communication et de télécommunication qui transportent tout ou partie des biens essentiels.

Il peut être utile de différencier canaux informatiques et de téléphonie selon la typologie suivante.

Canal Informatique

Cordon réseau, fibre optique, ondes radio, wifi.

Canal de téléphonie analogique

Ligne téléphonique.

2.2- ORG – Organisations

Ce type de biens supports est constitué de la combinaison de personnes (PER), de supports papier (PAP) et des canaux interpersonnels (CAN) en interaction, organisées pour satisfaire les objectifs d'un organisme (en réalisant des activités métiers spécifiques) et manipulant tout ou partie des biens essentiels dans des locaux (LOC).

Telle personne morale, telle entreprise, tel ministère, tel organisme sous tutelle, tel partenaire, tel fournisseur, tel client, tel service, telle organisation projet, tel cadre organisationnel pour homologuer un système.

PER – Personnes

Employés (développeur d'applications métiers, direction générale, chef de projet, manager, autorité d'homologation, utilisateur standard, exploitant, administrateur système ou de données, opérateur de sauvegarde, Help Desk…), personnes ne faisant pas partie de l'organisme mais placées sous sa responsabilité (stagiaire, thésard, prestataire en régie…), groupe projet.

PAP – Supports papier

Document manuscrit, document imprimé, diapositive, transparent, documentation, fax, photographie, radiographie.

CAN – Canaux interpersonnels

Circuit de validation par parapheur, processus de décision, circuit courrier, réunions, discussions de couloir.

2.3- LOC - Locaux

Ce type de biens supports est constitué des infrastructures immobilières hébergeant, et nécessaires au bon fonctionnement, des systèmes informatiques (SYS) et des organisations (ORG), dans lesquels sont utilisés tout ou partie des biens essentiels.

Site de Rennes, site d'exploitation au Maroc, usine au Pays-Bas, siège à Paris, locaux de l'organisme, périmètre particulier au sein des locaux, bureaux, bâtiment ou partie de bâtiment à usage de bureaux, de stockage, industriel, d'habitation ou mixte, pièce de stockage, salle serveur, salle de conférence, salle de réunion.

3- Types d'impacts

Les types impacts constituent les catégories de conséquences, directes et indirectes, sur l'organisme et sur les tiers, de la réalisation d'un sinistre.

Chaque type d'impacts fait l'objet d'une description. Les exemples figurent en italique.

3.1- Impacts sur le fonctionnement

Impacts sur les missions

Incapacité à fournir un service, perte de savoir-faire, changement de stratégie, impossibilité d'assurer un service, conséquences sur la production ou la distribution de biens ou de services considérés comme vitaux (atteinte à la satisfaction des besoins essentiels des populations, à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense, à la sécurité de la nation).

Impacts sur la capacité de décision

Perte de souveraineté, perte ou limitation de l'indépendance de jugement ou de décision, limitation des marges de négociation, perte de capacité d'influence, prise de contrôle de l'organisme

3.2- Impacts humains

Impacts sur la sécurité des personnes

Accident du travail, maladie professionnelle, perte de vies humaines, mise en danger.

Impacts sur le lien social interne

Perte de confiance des employés dans la pérennité de l'entreprise, exacerbation d'un ressentiment ou de tensions entre groupes sociaux (direction / employés, nationaux / étrangers, fonctionnaires / non-fonctionnaires, jeunes / seniors), affaiblissement de l'engagement d'employés vis-à-vis de l'entreprise, affaiblissement des valeurs éthiques communes au personnel (humanitaire, service public pour tous, progrès social, contribution à la santé dans le monde…).

3.3- Impacts sur les biens

Impacts sur le patrimoine intellectuel ou culturel

Perte de mémoire de l'entreprise (anciens projets, succès ou échecs…), perte de connaissances implicites (savoir-faire transmis entre générations, optimisations dans l'exécution de tâches ou de processus, captation d'idées novatrices, perte de patrimoine culturel (références esthétiques, modèles, styles…) ou scientifique (espèces biologiques rares ou disparues…).

Impacts financiers

Perte de chiffre d'affaire, dépenses imprévues, chute de valeur en bourse, baisse de revenus, pénalités.

Impacts sur l'image

Publication d'un article satirique dans la presse, perte de crédibilité vis-à-vis de clients, mécontentement des actionnaires, perte d'avance concurrentielle, perte de notoriété.

3.4- Autres impacts

Impacts de non-conformité

Refus d'obtention ou perte de labels du fait de non conformités à l'ISO 27001, Sarbanes-Oxley.

Impacts juridiques

Procès, amende, condamnation d'un dirigeant, dépôt de bilan, avenant, amendements de contrats.

Impacts sur l'environnement

Nuisances dues à des déchets ou des rejets sources de pollution (chimique, bactériologique, radiologique, sonore, visuelle, olfactive, …) générée par l'organisme et touchant son périmètre, son voisinage ou une zone.

4- Types de sources de menaces

Les sources de menaces représentent une typologie des choses ou personnes à l'origine des risques.

On distingue les sources par :

- leur origine humaine ou non humaine,
- leur facilité d'accès au sujet de l'étude (interne ou externe),
- dans le cas de sources humaines :
  - leur caractère intentionnel ou accidentel,
  - leurs capacités (force intrinsèque, selon leurs ressources, expertise, dangerosité…),
- dans le cas de sources non humaines :
  - leur type (naturelle, animale, contingence…).

Chaque type de source de menace fait l'objet d'exemples, qui figurent en *italique*.

4.1- Sources humaines agissant de manière délibérée

Personnes ou groupes de personnes mal intentionnées, qu'elles soient physiques ou morales, et qui peuvent être à l'origine de risques. Elles peuvent être internes ou externes au sujet de l'étude.

Source humaine interne, malveillante,

Collaborateur malveillant avec des connaissances et des possibilités d'action sur le système d'information, sous- traitant ou prestataire, personnel de maintenance ou d'assistance à distance, administrateur système ou réseau agissant par vengeance, dirigeant,...

Source humaine externe, malveillante,

Script-kiddies, vandale, militant, pirate, casseur ou fraudeur, ancien employé désirant se venger d'un licenciement, concurrent, groupement professionnel, organisation de lobbying, syndicat, journaliste, organisation non gouvernementale, organisation criminelle, agence gouvernementale ou organisation sous le contrôle d'un État étranger, espions, organisation terroriste.

4.2- Sources humaines agissant de manière accidentelle

Personnes ou groupes (internes ou externes) de personnes sans intention de nuire, qui peuvent être à l'origine de risques. Leurs capacités (force intrinsèque) dépendent principalement de leurs ressources, de leur expertise et du temps qu'elles peuvent accorder. Leur action involontaire peut être due à une faute d'attention, à une erreur de manipulation, à un manque d'investissement, à la malchance…

Source humaine interne, sans intention de nuire,

Collaborateur maladroit ou inconscient, personnel à faible conscience d'engagement, peu sensibilisé ou peu motivé dans sa relation contractuelle avec l'organisme, personnel d'entretien maladroit, stagiaire, thésard, intérimaire, utilisateur, fournisseur, prestataire, sous-traitant, client, actionnaires, manager, développeur, administrateur système ou réseau, dirigeant,...

Source humaine externe, sans intention de nuire,

Entourage du personnel, personne réalisant des travaux dans le voisinage, manifestants, visiteur maladroit, matériels émettant des ondes, des vibrations, activités industrielles dégageant des substances chimiques toxiques ou susceptibles de provoquer des sinistres mineurs, trafic routier ou aérien pouvant générer des accidents, matériels émettant des radiations ou des impulsions électromagnétiques, activités industrielles susceptibles de provoquer des sinistres majeurs, explosion dans le voisinage.

4.3- Sources non humaines

Choses ou objets qui peuvent être à l'origine de risques. Elles peuvent être internes au sujet de l'étude ou externe à celui-ci. Il ne peut s'agir que de contingences ou de malchance. Leurs capacités dépendent principalement de leurs ressources disponibles et de leur dangerosité.

Code malveillant d'origine inconnue

Virus informatique, code malveillant non ciblé, ou ciblé mais d'origine inconnue.

Phénomène naturel

Phénomène météorologique ou climatique aléatoire (foudre, canicule…), chute de roches, infiltration de sable, usure (temps qui s'écoule), phénomène naturel imprévisible mais récurrent, phénomène géologique (affaissement de terrain, séisme, éruption volcanique…), météorologique (tempête, ouragan…), naturel (feu de forêt, crue…), sanitaire (pandémie) de grande ampleur.

5- Menaces et vulnérabilités génériques

Les menaces génériques représentent les incidents ou les sinistres types qui peuvent affecter les biens supports.

Elles peuvent être classées selon :

- le type de biens supports sur lequel elles portent (MAT, LOG, CAN, PER) ;
- le critère de sécurité des biens essentiels qu'elles sont susceptibles d'affecter (disponibilité, intégrité, confidentialité) ;
- leur mode opératoire :
  - les détournements d'usages (USG) : les biens supports sont détournés de leur cadre d'utilisation nominal (usage des fonctionnalités possibles, prévues ou autorisées) sans être modifiés ni endommagés ;
  - l'espionnage (ESP) : les biens supports sont observés, avec ou sans équipement supplémentaire, sans être endommagés ;
  - les dépassements de limites de fonctionnement (DEP) : les biens supports sont surchargés ou utilisés au-delà de leurs limites de fonctionnement ;
  - les détériorations (DET) : les biens supports sont endommagés, partiellement ou totalement, temporairement ou définitivement ;
  - les modifications (MOD) : les biens supports sont transformés ;
  - les pertes de propriété (PTE) : les biens supports sont aliénés (perdus, volés, vendus, donnés…), sans être modifiés ni endommagés, de telle sorte qu'il n'est plus possible d'exercer les droits de propriété.

On peut citer :

5.1- Menaces sur les matériels

- Détournement de l'usage prévu d'un matériel

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	**Confidentialité**

- Espionnage d'un matériel

Critère(s) de sécurité concerné(s) :	Disponibilité	Intégrité	**Confidentialité**

- Dépassement des limites de fonctionnement d'un matériel

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

- Détérioration d'un matériel

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

- Modification d'un matériel

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	**Confidentialité**

- Perte d'un matériel

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	**Confidentialité**

5.2- Menaces sur les logiciels

- Détournement de l'usage prévu d'un logiciel

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	**Confidentialité**

Principales vulnérabilités exploitables :

- Analyse d'un logiciel

Critère(s) de sécurité concerné(s) :	Disponibilité	Intégrité	**Confidentialité**

- Dépassement des limites d'un logiciel

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

- Suppression de tout ou partie d'un logiciel

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

- Modification d'un logiciel

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	**Confidentialité**

- Disparition d'un logiciel

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	**Confidentialité**

5.3- Menaces sur les canaux informatiques et de téléphonie

- Attaque du milieu sur un canal informatique ou de téléphonie

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	Confidentialité

- Écoute passive d'un canal informatique ou de téléphonie

Critère(s) de sécurité concerné(s) :	Disponibilité	Intégrité	**Confidentialité**

- Saturation, modification, dégradation, disparition d'un canal informatique ou de téléphonie

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

5.4- Menaces sur les personnes

- Dissipation de l'activité d'une personne

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

- Espionnage d'une personne à distance

Critère(s) de sécurité concerné(s) :	Disponibilité	Intégrité	**Confidentialité**

- Surcharge des capacités d'une personne

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	Confidentialité

- Dégradation d'une personne

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

- Influence sur une personne

Critère(s) de sécurité concerné(s) :	Disponibilité	**Intégrité**	**Confidentialité**

- Départ d'une personne

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	**Confidentialité**

5.5- Menaces sur les canaux interpersonnels

- Saturation d'un canal informatique interpersonnel (mail, fichiers, alerte, …)

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

- Modification d'un canal interpersonnel informatique (par ex : règles de messagerie

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	**Confidentialité**

6- Mesures de sécurité génériques

6.1- Mesures de sécurité issues du [RGS]

Les mesures du [RGS] intègrent des clauses qui peuvent être interprétées comme des mesures de sécurité.

6.2- Mesures de sécurité issues de l'Arrêté Ministériel en application de l'article 18 de la loi n°1.430 portant diverses mesures relatives à la sécurité nationale

Les mesures de l'Arrêté Ministériel intègrent des clauses qui peuvent être interprétées comme des mesures de sécurité.

6.3- Fonctions de sécurité

- Authentification
- Signature électronique
- Confidentialité
- Horodatage
- Accusé d'enregistrement et de réception
- Qualification
- Infrastructures de gestion de clés (IGC)
- Politique de sécurité de l'information
- Organisation de la sécurité de l'information
- Gestion des biens
- Sécurité liée aux ressources humaines
- Avant le recrutement
- Pendant la durée du contrat
- Fin ou modification de contrat
- Sécurité physique et environnementale
    - Zones sécurisées
    - Voies d'eau
    - Incendies
- Gestion de l'exploitation et des télécommunications
    - Procédures et responsabilités liées à l'exploitation
    - Gestion de la prestation de service par un tiers
    - Planification et acceptation du système
- Protection contre les codes malveillant et mobile
- Sauvegarde
- Gestion de la sécurité des réseaux
- Manipulation des supports
- Échange des informations
- Surveillance
- Contrôle d'accès aux réseaux, systèmes, serveurs, machines, applications, fichiers, …
- Acquisition, développement et maintenance des systèmes d'information
    - Exigences de sécurité applicables aux systèmes d'information
    - Mesures cryptographiques
    - Sécurité en matière de développement et d'assistance technique
    - Gestion des vulnérabilités techniques
- Gestion des incidents liés à la sécurité de l'information
- Gestion du plan de continuité de l'activité
- Conformité avec les exigences légales, les audits.