Introduction à la sécurité de l'information

Novembre 2016

Plan de la présentation

I - Introduction,

II - Analyse des risques,

III - Architecture de sécurité (7498-2),

IV - Authentification,

V - Éléments à retenir,

VI - La sécurité informatique et le droit,

VII - Quelques références.

I – Introduction

Systèmes d'information

Définition récente et champ en extension :

Ensemble des moyens dont le fonctionnement fait appel, d'une façon ou d'une autre, à l'électricité et destinés à élaborer, traiter, stocker, acheminer ou présenter l'information (décret du 3 mars 1986, directive 3122/SG du 14 mars 1986)

Depuis, on dispose de la définition des systèmes automatisés de traitement de l'information dans la loi sur la fraude informatique ou de celle du système d'information dans la méthode EBIOS (ensemble d'entités organisé pour accomplir des fonctions de traitement d'informations)

Plus généralement, depuis le début des années 1990, c'est la notion de sécurité de l'information qui est traitée (BS 7799 en Grande-Bretagne puis ISMS au SC 27 du JTC 1 de l'ISO), avec une tendance à prendre en compte la « sécurité globale ».

I – Introduction

Sécurité : deux notions

Liberté individuelle (*Privacy*)

Protection des individus contre l'utilisation abusive d'informations les concernant. Domaine en forte évolution (informations nominatives, données personnelles).

En France : CNIL, Loi "Informatique et Libertés".

Sécurité des informations (*Security)*

Protection contre l'usage abusif de ressources ou contre la dégradation de services ou de biens.

En France : Loi sur la fraude informatique, loi sur le droit d'auteur, instructions ministérielles.

I – Introduction

Évolution du contexte (1)

Développement de l'informatique :

- du support papier au support électronique,
- des machines isolées aux réseaux,
- du lent au rapide.

Ethique et déontologie :

- difficultés d'adaptation (mentalités, réglementation,...)

Extension des réseaux :

- du monosite au multisite,
- de l'intra-entreprise à l'inter-entreprises.

I – Introduction

Évolution du contexte (2)

Quelques éléments favorisant la fraude informatique :

- facilité d'intrusion et de "furetage",
- absence de traces,
- évolution lente des mentalités,
- multiplication des micro-ordinateurs,
- interconnexions de systèmes dans des réseaux mondiaux,
- échanges d'informations volumineux et rapides par les réseaux,
- dépendance des entreprises vis-à-vis de leur SI.

I – Introduction

Les obligations : 3 classes de secteurs de sécurité

- **I – Secteurs réglementés : données classifiées – Secret de défense**

Ministère de la défense : sécurité "militaire",

Secrétariat Général de la Défense Nationale (SGDSN) : protection du patrimoine et du "secret de défense" hors le Ministère de la Défense.

- **II – Secteurs non réglementés soumis à contrôle**

Secteurs sensibles : industrie, recherche (industriels travaillant pour la défense), patrimoine, produits soumis à contrôle à l'exportation.

- **III – Secteurs non réglementés, non contrôlés**

Données sensibles mais non classifiées.

Tous les autres secteurs d'activité.

II – Gestion des risques

Lien entre risque et sécurité

On définit souvent la **sécurité** comme l'**absence de risque**. Ce qui conduit à examiner ce qu'est un risque. Il en existe plusieurs définitions :

Combinaison de la **probabilité** d'un événement et de son **impact** (ISO/CEI 27002:2005)
Mais aussi :
Tout ce qui contribue à **empêcher**, par action ou par inaction, la **réalisation d'un objectif** (ISACA, Audit)
Ou encore :
Effet de l'incertitude sur les objectifs (ISO Guide 73:2009)

II – Gestion des risques

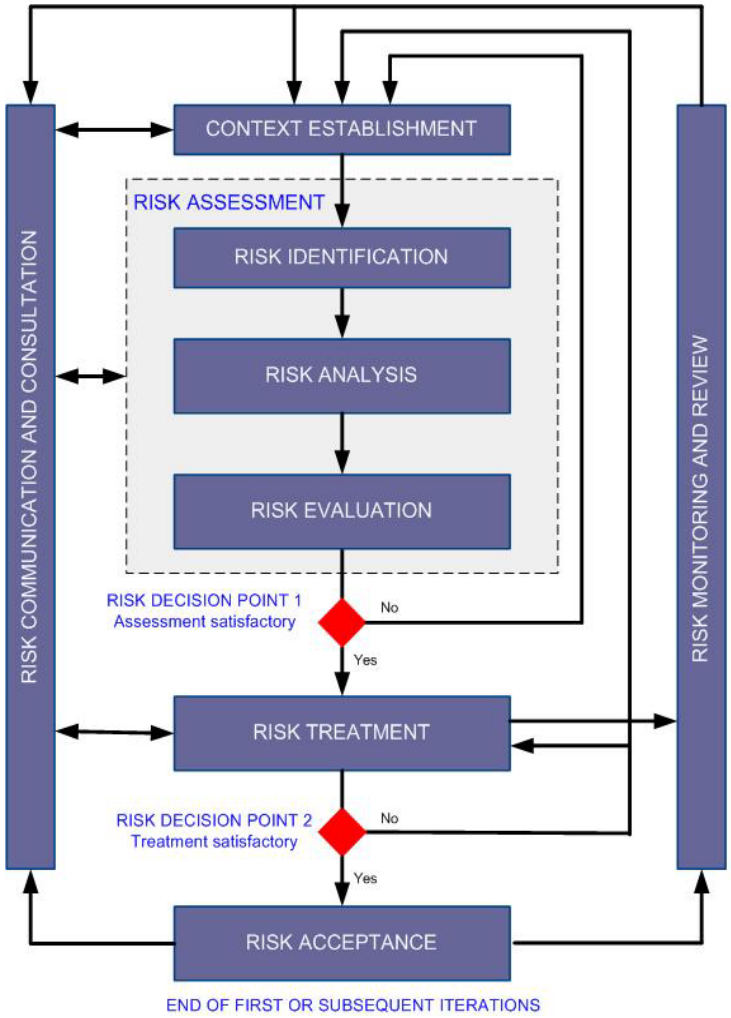
Processus de gestion du risque en sécurité de l'information (norme ISO/CEI 27005:2011)

Processus **continu et itératif**

Identifier les risques potentiels

- **Vraisemblance et conséquences** de ces risques. Pouvoir comprendre et **communiquer**
- Ordre de **priorité** pour le traitement
- **Mesures appropriées** pour les risques dépassant le niveau maximum acceptable
- **Surveillance** de l'efficacité du traitement
- **Acquisition d'informations** pour améliorer l'approche
- Surveillance, **révision et amélioration**

II – Gestion des risques



D'après ISO/IEC 27005:2011

II – Gestion des risques

Paramètres de base

Critères d'évaluation (valeur stratégique du processus ; criticité de l'information ; conséquences financières ; obligations légales, réglementaires ou contractuelles ; conséquences en terme de DIC ; atteintes à l'image ;…)

Critères d'impact (niveau de classification des biens, critères de sécurité, opérations concernées, valeurs financières ou commerciales, réputation)

Critères d'acceptation

Ressources disponibles

II – Gestion des risques

Champ et frontière du processus

Lois et règlements applicables

Objectifs, stratégies, politiques de l'organisation

Domaine **géographique**

Architecture du système d'information

Justification sur les **thèmes exclus** du processus

Environnement socio-culturel

II – Gestion des risques

Appréciation du risque

Identification : Identification des biens, des menaces et des impacts.
Évaluation des mesures existantes et prévues.
Estimation : Identification des risques,
Méthodologies d'estimation du risque,
Évaluation des conséquences,
Évaluation de la probabilité des menaces et des vulnérabilités.
Options de traitement du risque
Évitement,
Réduction,
Transfert,
Acceptation.
Risque résiduel.
Communication.
Supervision et révision.

II – Gestion des risques

ISO/CEI 27005:2011 - Annexes (1/2)

Annexe A - Définir champ et frontières du processus de gestion du risque
Étude de l'organisation, listes des contraintes, liste des lois et règlements, description fonctionnelle du système d'information, étude du système cible.

Annexe B - Identification et évaluation des biens, identification des biens essentiels, liste et description des biens supports, évaluation des biens, détermination d'impact.

Annexe C - Types de menaces **(**A Accident, D Intentionnel, E Environnement)
Types : dommage physique, événement naturel, perte de services essentiels, perturbations électroniques, compromission de l'information, défaillance technique, action non autorisée, compromission de fonctions.
Une attention particulière est à porter aux **sources humaines** des menaces (origine, motivation, conséquences possibles)

II – Gestion des risques

ISO/CEI 27005:2011 - Annexes (2/2)

Annexe D - Vulnérabilités et méthodes de détermination des vulnérabilités.
6 catégories de vulnérabilités : hardware, software, réseau, personnel, site, organisation.
Méthodes pour déterminer les vulnérabilités techniques : automates de tests, *Security Testing* and Evaluation (STE), tests de pénétration.

Annexe E - Approches d'estimation du risque en sécurité de l'information.

Annexe F – Contraintes en cas de modification du risque.

Annexe G – Différences de définition entre ISO/IEC 27005:2008 et ISO/IEC 27005:2011

II – Gestion des risques

ISO 31000

Norme élaborée au TMB (*Technical Management Board*) de l'ISO.

Lignes directrices pour les principes et la mise en œuvre de la gestion du risque.

Norme générique pouvant s'appliquer à toutes les étapes du cycle de vie d'un organisme et de son activité, processus, fonction, projet, produit, service ou actif.

Cette norme fournit une **approche commune** en soutien des normes portant sur des risques plus spécifiques et ne les remplace pas.
Elle ne peut servir de base à une certification ou à des fins contractuelles.
Elle se réfère, pour le vocabulaire, à l'ISO Guide 73.
Elle entre en révision en 2015.

II – Gestion des risques

Les méthodes de la sécurité de l'information

Ces méthodes visent à informer sur le niveau de sécurité du système d'information dans une entreprise ou dans une partie de celle-ci.

Elles permettent de déterminer les domaines pour lesquels des actions sont prioritaires ainsi que les choix budgétaires ou d'organisation qui en découlent.

Les deux méthodes initialement les plus utilisées en France ont été la méthode **MARION** (origine compagnies d'assurance) et la méthode **MELISA** (origine armement). **MEHARI**, synthèse de **MARION** et de **MELISA,** est parue en mai 1997.

II – Gestion des risques

Autres méthodes

D'autres méthodes ont été développées qui analysent les besoins de sécurité très en amont, dès la phase de conception. Ces méthodes intègrent la notion de système d'information et son évolution. Ainsi en France, l'**ANSSI** propose un ensemble cohérent de guides et méthodes parmi lesquels on peut mentionner :

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité. (une nouvelle version, EBIOS 2010, est parue en avril 2010)

PSSI : Guide pour l'élaboration d'une Politique de Sécurité Interne.

RGS : Référentiel Général de Sécurité (arrêté du 6 mai 2010 paru au J.O. du 18 mai, V.2 depuis le 1er juillet 2014)

Ces documents sont cohérents avec les principales normes internationales du domaine.

II – Gestion des risques

Normes en sécurité de l'information (1/4)

Des normes se sont développées dans le domaine de la sécurité de l'information. Elles sont souvent liées à une approche qualité. On peut ainsi mentionner dans la série IS 2700x :

IS 27002:2013 : Issue de la partie 1 de la BS 7799 d'origine britannique, initialement nommée **IS 17799**.
IS 27001:2013, basée sur la partie 2 de la BS 7799 et orientée certification.
IS 27005:2011, *Information Security Risk management*.

La nouvelle version des normes IS 27001 et IS 27002, parue en octobre 2013, a entraîné la révision de plusieurs normes de la série 27000 dont l'IS 27005.

II – Gestion des risques

Normes en sécurité de l'information (2/4)

Autres normes d'**orientation générale** et normes **métiers** développées au **WG1**

IS 27000	ISMS *fundamentals and vocabulary*,
IS 27003	ISMS *Implementation,*
IS 27004	ISM *measurements,*
IS 27006	*Requirements for bodies providing audit and certification of* ISMS,
IS 27007	ISMS *auditor guidelines*,
IS 27011	ISM *guidelines for telecommunications* (ITU-T X.1051)
IS 27013	*Guidance on the integrated implementation of ISO/IEC 20000 part 1 and ISO/IEC 27001*,
IS 27014	*Information security governance framework,*
TR 27015	ISMS *for financial and insurance services sectors,*
IS 27016	ISM *organizational economics,*
IS 27017	*Cloud computing security and privacy management system.*

II – Gestion des risques

Normes en sécurité de l'information (3/4)

Normes techniques en élaboration au WG4

Dix sont actuellement en préparation. Certaines reprennent des documents déjà existants.

ISO/CEI 27031 ***Guidelines for ICT readiness for business continuity***,
ISO/CEI 27032 *Guidelines for cybersecurity*,
ISO/CEI 27033 *Network Security*,
ISO/CEI 27034 *Application security*,
ISO/CEI 27035 ***Information security incident management***,
ISO/CEI 27036 ***Information security for supplier relationships***,
ISO/CEI 27037 *Guidelines for identification, collection, acquisition and preservation of digital evidence,*
ISO/CEI 27038 *Specifications for digital redaction,*
ISO/CEI 27039 *Selection, deployment, and operation of intrusion detection and prevention systems (IDPS),*
ISO/CEI 27040 *Storage security,*
ISO/CEI 27050 *E-dicsovery.*

II – Gestion des risques

Normes en sécurité de l'information (4/4)

Quelques normes du WG3 :

IS 21827:2006 : Plus connue sous l'acronyme SSE/CMM (*Systems Security Engineering / Capability Maturity Model*), cette norme analyse la maturité de la sécurité avec une approche qualité.

IS 15408 (Critères Communs). Correspond surtout à l'évaluation et à la certification des produits et des systèmes. Des développements complémentaires sont à mentionner :

IS 19790 sur la certification des produits de cryptologie,

IS 19791 sur la certification des systèmes opérationnels,

IS 19792 sur la certification des produits de biométrie.

II – Gestion des risques

Autres approches

L'analyse des risques en sécurité de l'information conduit en entreprise à deux démarches classiques :

La **cartographie des risques** qui est une approche "***top-down***" dans laquelle des décideurs assistés d'experts évaluent les probabilités et les impacts des risques pour établir une cartographie. Une attention particulière est portée aux risques majeurs.

La connaissance de la **sinistralité**, démarche "***bottom-up***" qui permet, par une remontée efficace des incidents et une analyse appropriée, de mieux appréhender la réalité des incidents survenus.

Ces deux démarches se "croisent" pour une détermination efficace des mesures à prendre.

II – Gestion des risques

Audits intrusifs

Ces audits consistent à tester les **vulnérabilités** et le **niveau de sécurité** des **configurations** d'une architecture. Ils exigent une grande maîtrise au niveau des clauses contractuelles comme à celui de l'exécution. De nombreux points sont à considérer parmi lesquels :

- Définition rigoureuse des **conditions d'intervention** (périmètre traité incluant les cibles et l'environnement, confidentialité des informations).
- Expertise technique élevée (compréhension de l'architecture et de l'environnement applicatif, connaissance des **vulnérabilités exploitables**, intervention en **contexte opérationnel**).
- Capacités d'analyse pour évaluer les faiblesses et proposer des améliorations en tenant compte de la **politique de sécurité** et de la **culture d'entreprise**.

III – Architecture de sécurité (7498-2)

La norme ISO 7498-2 JTC1/SC21

Vocabulaire relatif à la sécurité,

Services et **mécanisme**s de sécurité,

Relations entre les services et les mécanismes de sécurité,

Positionnement des services et des mécanismes,

Fonctions d'**administration** de la sécurité.

III - Architecture de sécurité (7498-2)

Risques

On distingue trois types de risques à prendre en compte dans un système de traitement de l'information :
Modification, altération ou destruction de l'information,
Compromission de l'information,
Interruption de service.

Ces risques conduisent à prendre des mesures de **protection** ou de **prévention** portant sur les informations, les services de communication et de traitement de données, les équipements et les intervenants en cause.

III - Architecture de sécurité (7498-2)

Menaces

Accidentelles ou intentionnelles,

D'origine interne ou externe.

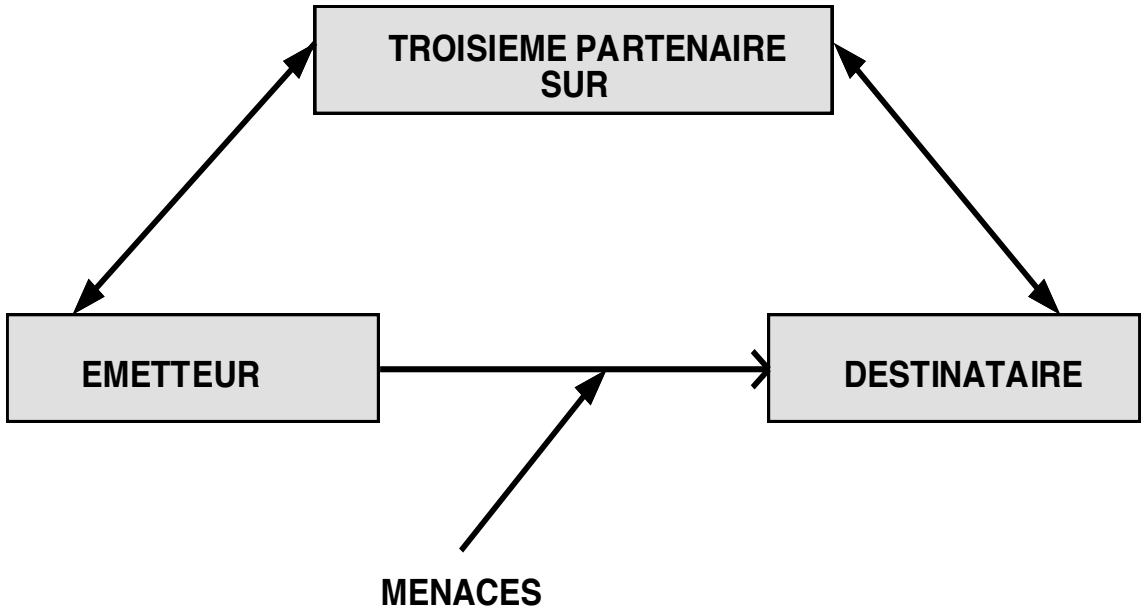
Techniquement, on distingue aussi :

Menaces passives : elles ne modifient pas le contenu de l'information et portent essentiellement sur la confidentialité.

Menaces actives : elles modifient le contenu de l'information ou le comportement des systèmes de traitement (**brouillage** des communications, **modification** des données transmises ou résidentes, **pénétration** du système, **destruction** physique ou logique)

III - Architecture de sécurité (7498-2)

Besoins de sécurité



Pour l'**émetteur** :

Le message doit parvenir au bon destinataire (**authentification**),

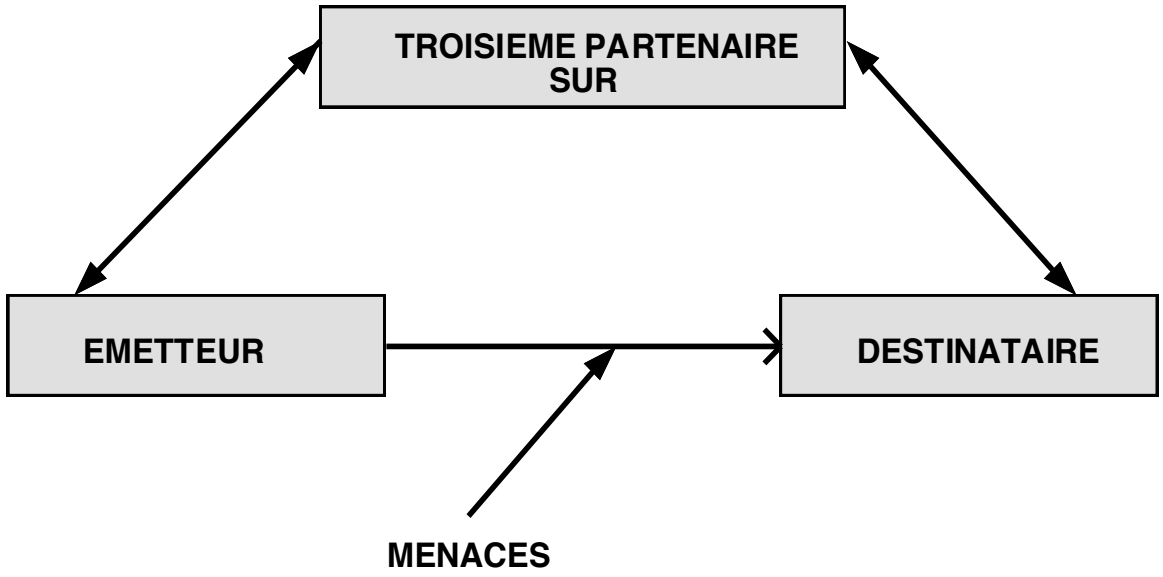
Le message ne doit être compris que par son destinataire (**confidentialité**),

Le message reçu doit être identique au message émis (**intégrité**),

Le destinataire ne doit pas pouvoir nier avoir reçu le message (**non-répudiation**).

III - Architecture de sécurité (7498-2)

Besoins de sécurité



Pour le **destinataire** :

Être sûr de l'identité de l'émetteur (**authentification**),

Aucun tiers ne doit avoir pris connaissance du message (**confidentialité**),

Le message reçu doit être identique au message émis (**intégrité**),

L'émetteur ne doit pas pouvoir nier avoir émis le message (**non-répudiation**),

Seuls des émetteurs autorisés peuvent envoyer des messages (**contrôle d'accès)**

III - Architecture de sécurité (7498-2)

Services de sécurité

Authentification : mode avec ou sans dialogue.
Contrôle d'accès : protège contre l'usage non autorisé de ressources accessibles via le réseau. Il peut s'appliquer à divers types d'accès (usage de ressources de communication ; lecture, écriture ou destruction d'informations ; exécution d'une ressource de traitement)
Confidentialité des données : mode avec ou sans dialogue. La confidentialité peut être à champ sélectif. Elle peut aussi porter sur le flux de trafic.
Intégrité des données : mode avec ou sans dialogue. L'intégrité peut être à champ sélectif.
Non-répudiation : elle peut porter sur l'émetteur ou le destinataire.

III - Architecture de sécurité (7498-2)

Mécanismes de sécurité

Chiffrement,

Signature numérique,

Contrôle d'accès,

Intégrité des données,

Échange d'authentification,

Notarisation.

III - Architecture de sécurité (7498-2)

Chiffrement

Le chiffrement permet de transformer des données en clair en des données non intelligibles pour ceux qui n'ont pas à les connaître.

Le message chiffré est appelé un **cryptogramme**.

L'opération permettant au(x) destinataire(s) de reconstituer le message est le **déchiffrement**.

L'opération consistant à essayer de déterminer le message en clair à partir du cryptogramme sans information sur l'algorithme de chiffrement est le **décryptement**.

III - Architecture de sécurité (7498-2)

Chiffrement

On distingue en général deux types d'algorithmes inversibles :

Symétriques (ou à clés secrètes) : la connaissance de la clé de chiffrement entraîne celle de la clé de déchiffrement.

Asymétriques (ou à clés publiques) : la connaissance de la clé de chiffrement n'entraîne pas celle de la clé de déchiffrement.

La **gestion des clés** est un élément fondamental de la sécurité des systèmes d'information.

III - Architecture de sécurité (7498-2)

Signature numérique

Les mécanismes de signature numérique recouvrent deux procédures :
La signature d'une unité de données,
La vérification de la signature d'une unité de données.

La signature ne doit pouvoir être produite que grâce à une information connue du seul signataire.
La vérification ne doit pas permettre de retrouver cette information secrète.
La vérification doit pouvoir prouver que seul le détenteur de l'information secrète a pu procéder à la signature.
La validité juridique de la signature électronique évolue (Loi du 13 mars 2000, décrets 2001-272 du 30 mars 2001 et 2002-535 du 18 avril 2002,…)

III - Architecture de sécurité (7498-2)

Contrôle d'accès

Les mécanismes contrôlant l'accès d'une entité à une ressource peuvent utiliser :

- l'identité authentifiée de l'entité,
- une information sur l'entité,
- un élément appartenant à cette entité,
- une liste de droits d'accès,
- des "étiquettes" de sécurité spécifiant des niveaux de sensibilité.

Ces mécanismes dépendent de la politique de contrôle d'accès choisie :

Sécurité discrétionnaire : l'utilisateur définit les droits d'accès aux informations dont il a la responsabilité.

Sécurité par mandat : l'autorisation d'accès dépend des droits du demandeur, du niveau de sensibilité des informations et d'attributs spécifiques.

III - Architecture de sécurité (7498-2)

Intégrité des données

Les mécanismes d'intégrité mettent en jeu deux processus :

L'entité **émettrice** ajoute à l'unité de données une information supplémentaire fonction de cette unité.

L'entité **réceptrice** vérifie l'intégrité de l'unité de données reçue en calculant, à partir de celle-ci, une information correspondant à celle transmise par l'entité émettrice et en comparant le résultat obtenu à cette dernière.

III - Architecture de sécurité (7498-2)

Échange d'authentification

L'authentification d'une entité homologue peut faire intervenir ce que cette entité :
- est,
- possède,
- connaît.

Les procédures choisies utilisent souvent des techniques cryptographiques auxquelles peuvent être associés :
- horodatage avec horloges synchronisées,
- protocoles à deux ou trois échanges (selon que l'authentification est unilatérale ou mutuelle).

III - Architecture de sécurité (7498-2)

Notarisation

Ce mécanisme est associé au service de non-répudiation.

Il fait intervenir **un tiers** (troisième partenaire sûr, souvent appelé **notaire** par analogie fonctionnelle).

Il garantit certaines informations associées aux données échangées entre l'entité émettrice et l'entité réceptrice comme l'intégrité des données, leur origine, l'heure d'émission, l'heure de réception…

III - Architecture de sécurité (7498-2)

Quelques remarques

- De la sécurité informatique à la sécurité de l'information.
- Journalisation (enregistrement des événements, exploitation des informations, aspect probant)
- Sécurité physique.
- Confiance dans les personnes.
- Logiciels et matériels sûrs : évaluation, validation, vérification, preuves formelles…
- Méthodes d'évaluation de la sécurité : EBIOS, MEHARI,
- Certifications de produits ou de systèmes (Livre Orange, ITSEC, Critères Communs, CSPN), extension aux organisations ou aux personnes (ISO/IEC 27001)
- Existence d'autres critères que D,I,C (comme pérennité, authenticité)

IV - Authentification

Comment s'authentifier ?

Par ce que l'on sait (mot de passe)

Par ce que l'on a (carte, jeton)

Par ce que l'on est (données biométriques)

On peut aussi distinguer

Principe logique (mot de passe, carte, jeton)
Principe physique (données biométriques)

IV - Authentification

Authentification par ce que l'on sait (mot de passe)

Dépend beaucoup de l'**implémentation.**
Possibilité de **génération automatique** de mots de passe (alternative aux difficultés de mémorisation)
Existence de variantes (réponses préétablies à des questions)
La **difficulté à mémoriser** est une source classique de failles (compromission par manque de précautions)
Problèmes d'utilisation sur les **réseaux** (interception et cascade)
Compromission difficile à détecter.

IV - Authentification

Remarques sur les mots de passe

Durée de validité, modalités de **changement.**

Choix trivial (longueur, composition). Utiliser un mécanisme de composition simple, facile à mémoriser et difficile à compromettre.

Stockage (éviter que l'on puisse accéder aux mots de passe ou les reconstituer)

Traitement des erreurs (éviter la reconstitution des mots de passe à partir des enregistrements d'erreurs)

Capacité croissante des attaquants, conséquence sur la **longueur minimum** des mots de passe.

IV - Authentification

Authentification par ce que l'on a

Nombreux dispositifs (badges, carte Secur ID, Activ card, bouchons, dongles, cartes à mémoire) faciles à transporter.

Peut poser des problèmes de généralisation (nécessité d'une **interface**)

Attention au risque de n'authentifier que le dispositif détenu, prévoir un protocole correct (**authentifier le possesseur**)

Compromission limitée et facile à détecter (sauf copie)

Coût intermédiaire entre mot de passe et dispositif biométrique.

IV - Authentification

Authentification par ce que l'on est

Quasiment **impossible à transmettre** à un tiers, à la différence des cas précédents.

Difficile à imiter ou à contourner en raison de la complexité des caractéristiques biologiques retenues.

La variabilité des caractéristiques biologiques et l'environnement peuvent conduire à recourir à des facteurs de tolérance limitant l'efficacité du mécanisme.

Problèmes d'**acceptation** de la part des utilisateurs (empreintes rétiniennes, vie privée).

Coût élevé (sécurité de haut niveau).

Authentification ou identification ?

IV - Authentification

Authentification mixte

Il est possible d'utiliser plusieurs mécanismes :

- lecteur de badge et empreintes digitales,

- utilisation de dispositifs différents selon la sensibilité des informations ou l'utilisateur (sans compter l'aspect secours)

Emplacement des dispositifs et ergonomie.

V – Éléments à retenir

Quelques affaires anciennes connues :

Ver Internet : 2 novembre 1988, 6000 ordinateurs atteints, dégâts évalués à 15 millions de dollars, condamnation "modérée" (10 000 dollars d'amende, 400 heures de service communautaire)

***Stalking the wily hacker* (C. Stoll) :** Com. of the ACM, Vol 31, N°5 - Mai 1988, espionnage international.

Affaires CCC (Chaos Computer Club) : *The wily hacker*, réseau SPAN (1987)

V – Éléments à retenir

Évolution (1/2) :

Attaques par DOS et DDOS : Possibilité apparue courant 1999, largement exploitée depuis (*botnets*)

Virus, vers, Chevaux de Troie : Apparus dès le milieu des années 80. Le rapport "*IBM Global Business Security Index*" d'août 2005 indique **237 millions d'attaques** virales et informatiques dans le monde durant le **premier semestre** (Cyber criminalité - E. Filiol, P. Richard - Dunod 2008).

Développement du ***phishing*** (sites bancaires) et des ***ransomwares***.

Données personnelles, vie privée : *phishing*, réseaux sociaux, moyens de paiement.

V – Éléments à retenir

Évolution (2/2) :

Attaques ciblées : Industriels, structures gouvernementales.

Attaques SCADA (S*upervisory Control and Data Acquisition)* : Ciblent des systèmes industriels (Stuxnet).

Cyberattaques stratégiques : Estonie en 2007, Georgie en 2008.

PRISM, Snowden.

Marchandisation de la délinquance, **banalisation** des moyens.

V – Éléments à retenir

- Application du principe du **moindre privilège.**

- Le remède ne doit pas être pire que le mal.

- Défenses au niveau des **systèmes terminaux**, pas seulement du réseau.

- Circulation des informations permettant de limiter les **vulnérabilités**.

- **Gestion de crise, PC** à constituer (niveau national, grands organismes, etc.)

- Améliorer la **prise en compte** de la sécurité (concepteurs, fournisseurs, utilisateurs, *stakeholders*,…).

V - Éléments à retenir

- Exploitation banale de **failles connues**, déjà publiées. Importance des mises à jour et des procédures associées.

- La **veille** en matière de **sécurité** est un outil de plus en plus indispensable. Elle est à mettre en place au sein d'une entité en conformité avec la politique de sécurité globale, en s'appuyant sur un outil collaboratif et sur une organisation efficaces.

- Le développement de certaines attaques peut conduire à la remise en cause de procédures existantes (*ransomwares* et sauvegarde par exemple).

- Retour à la normale : Pour garantir un retour à la normale exempt de risques consécutifs aux intrusions, il faudrait reconfigurer tous les systèmes à partir des éléments de référence et recertifier chaque utilisateur. C'est très complexe, surtout si l'on prend en compte des contraintes banales de service (continuité du service, modalités de gestion,...). Quid s'il reste des Chevaux de Troie (les intrus attendent parfois des mois avant d'utiliser les chevaux de Troie déposés) ?

V – Éléments à retenir

Cas de la journalisation

Diversité des sources (réseaux, serveurs, applications)
Granularité des enregistrements (outils d'analyse, volumes à traiter, seuils de réaction)
Choix des supports physiques.
Protection des éléments de sécurité, risque de désactivation des programmes d'audit.
Traitement en temps réel, en temps différé, conditions de stockage, droits d'accès.
Obligations réglementaires, aspects contractuels.

VI – La sécurité informatique et le droit

Quatre aspects sont présentés :

Loi sur la **fraude informatique**

Loi et directives relatives au **droit d'auteur**

Loi "**Informatique et Libertés**"

Réglementation sur le **chiffrement**

VI - Fraude informatique (1/5)

Loi 88-19 du 5 janvier 1988, modifiée dans le Code Pénal entré en vigueur le 1 mars 1994.

Articles 323-1 à 323-7.

Concerne les atteintes aux **systèmes de traitement automatisé des données** (notion qu'elle définit).

Cette loi crée des **incriminations nouvelles spécifiques** à ces systèmes.

VI – Fraude informatique (2/5)

STAD (Système de traitement automatisé de données)

Tout ensemble composé :

- d'une ou plusieurs entités de traitement,
- de mémoires,
- de logiciels,
- d'organes d'entrées et de sorties,
- de liaisons,
- de données,

(- de systèmes de sécurisation)

VI - Fraude informatique (3/5)

Incriminations envisagées

- Accès ou maintien frauduleux dans un système,
- Actes visant à fausser et entraver le fonctionnement du système,
- Intervention sur les données : modification, suppression, introduction,...
- Participation à un groupement ou à une entente en vue de se livrer à un ou plusieurs des délits ci-dessus,
- Tentative pour les délits ci-dessus.

VI – Fraude informatique (4/5)

Peines prévues (1/2)

- **Accès ou maintien frauduleux :** 2 ans et 30 000 € ou 3 ans et 45 000 € si suppression ou altération des données ou si altération du fonctionnement du système **(323-1)**
- **Actions visant à fausser ou à entraver ... :** 5 ans d'emprisonnement et 75 000 € d'amende **(323-2)**
- **Intervention sur les données :** 5 ans d'emprisonnement et 75 000 € d'amende **(323.3)**
- **Participation à un groupement ... :** peines prévues en 323-1 à 323- 3 ou la plus sévère d'entre elles **(323-4)**
- **Tentative ... :** peines prévues en 323-1 à 323-3 ou la plus sévère d'entre elles **(323-7)**

Aggravation dans certains cas.

VI – Fraude informatique (5/5)

Peines prévues

- Personnes physiques :

Peines complémentaires d'interdiction des droits civiques, civils et de famille (5 ans), de l'exercice d'une fonction publique ; confiscation de la chose qui a servi à ou était destinée à commettre l'infraction, ou de la chose qui en a résulté **(323-5)**

- Personnes morales :

Taux de l'amende quintuple de celui des personnes physiques ; interdiction pour 5 ans ou plus d'exercer une ou plusieurs activités professionnelles ou sociales ; confiscation de la chose qui a servi à ou était destinée à commettre l'infraction ou de la chose qui en a résulté **(323-6)**

VI – Droit d'auteur (1/3)

- Loi 85-660 du 3 juillet 1985.

- Directive communautaire 91-250 du 14 mai 1991.

- Loi 94-361 du 10 mai 1994 sur la mise en oeuvre de la directive précitée.

- Concerne la protection des programmes d'ordinateur au titre du droit d'auteur.

VI – Droit d'auteur (2/3)

Protection des programmes d'ordinateur

- Ils sont assimilés à des **oeuvres littéraires,**

- La protection s'étend sur 70 ans,

- Les **droits patrimoniaux** sont exercés par l'employeur,

- Les auteurs sont des personnes physiques ou morales,

- La **décompilation** est **autorisée** seulement en vue de l'**interopérabilité**.

VI – Droit d'auteur (3/3)

A la requête de tout auteur ou d'un ayant-droit, les commissaires de police sont tenus d'opérer une **saisie description** du logiciel contrefaisant, laquelle peut se concrétiser par une copie.

La **saisie contrefaçon** est exécutée en vertu d'une ordonnance rendue sur requête par le Président du Tribunal de Grande Instance. Il autorise, s'il y a lieu, la saisie réelle.

Au Pénal (article L.335 du CPI), la **contrefaçon de logiciel** est punie de **3 ans d'emprisonnement** et de **300 000 € d'amende, 5 ans et 500 000 €** si commise en bande organisée.

VI – Loi Informatique et Libertés (1/4)

Loi 78-17 du 6 janvier 1978 (modifiée en 1988, 1992, 1994, 1999, 2000, 2003, **2004,** 2006, 2009)

Article 2 : sont réputées **personnelles** au sens de la présente loi les **informations** qui permettent**,** sous quelque forme que ce soit, directement ou non, **l'identification** des personnes physiques auxquelles elles s'appliquent.

Article 11 : La **CNIL** (Commission Nationale de l'Informatique et des Libertés), ses missions, sa composition.

Article 34 : Le **responsable du traitement** (de données personnelles) est tenu de prendre **toutes précautions utiles**, au regard de la nature des données et des risques présentés par le traitement, **pour préserver la sécurité des données** et notamment empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

VI – Loi Informatique et Libertés (2/4)

La **CNIL (1/2)**

Autorité administrative indépendante.

Créée par la loi du **6 janvier 1978**, réformée par la loi du **6 août 2004** qui transposait la directive européenne du 24 octobre 1995 (dir. 95/46/CE)

Elle se compose d'un collège de **17 personnalités** nommées pour 5ans :

- 4 parlementaires (2 députés, 2 sénateurs)
- 2 membres du Conseil économique, social et environnemental.
- 6 représentants des hautes juridictions (2 conseillers d'Etat, 2 conseillers à la Cour de Cassation, 2 conseillers à la Cour des Comptes)
- 5 personnalités qualifiées désignées par le Conseil des Ministres (3), le Président de l'Assemblée Nationale (1) et le Président du Sénat (1)

Trois directions (affaires juridiques, internationales et expertise ; relations avec les usagers et contrôle ; ressources humaines, financières et logistiques)

VI – Loi Informatique et Libertés (3/4)

La **CNIL (2/2)**

Cinq missions principales :

- Informer,
- Garantir le droit d'accès,
- Recenser les fichiers,
- Contrôler,
- Réglementer.

Les **Droits Informatique et Libertés :**

- Droit d'information,
- Droit d'accès,
- Droit de rectification et de radiation,
- Droit d'opposition,
- Droit d'accès indirect.

VI – Loi Informatique et Libertés (4/4)

Articles 226-16 à 226-22 du Code Pénal sur les atteintes aux droits de la personne résultant des fichiers et des traitements informatiques :

- 226-16 : respect des **formalités préalables** (5 ans d'emprisonnement et 300 000 € d'amende)

- 226-17 : obligation de **sécurité** (5 ans d'emprisonnement et 300 000 € d'amende)

- 226-18 : collecte et traitement illicites d'informations nominatives (5 ans d'emprisonnement et 300 000 € d'amende)

- 226-19 : stockage illicite d'informations nominatives (5 ans d'emprisonnement et 300 000 € d'amende)

- 226-20 : conservation de données au-delà de la durée prévue (5 ans d'emprisonnement et 300 000 € d'amende)

- 226-22 : divulgation d'informations nominatives (5 ans d'emprisonnement et 300 000 € d'amende, 3 ans et 100 000 € si par imprudence ou négligence)

VI – Règlement Général sur la Protection des Données – (UE) 2016/679

- La protection des personnes physiques à l'égard du traitement des données à caractère personnel
- Entre en vigueur le 25 Mai 2018
- Applicable aux fournisseurs de services numériques
- Pénalité pouvant atteindre 4% du chiffre d'affaires monde
- Des mesures organisationnelles, procédurales, et techniques qui devront être déployées de façon auditable.

VI - Chiffrement

1986 : tout moyen de cryptologie assimilé à une **arme de guerre** de deuxième catégorie. Dossier déposé au Ministère des PTE.

1990 (article 28 de la loi 90.1170 du 29 décembre) : notion d'"arme de guerre" supprimée ; **déclaration préalable** pour l'**authentification et l'intégrité** ; **autorisation préalable** pour le **chiffrement**. Dossier déposé au SCSSI.

1992 (28 décembre) : simplification des procédures sans modification de fond.

1996 : nouvelle réglementation, notion de **"tiers de confiance"**.

1998 : décrets complémentaires de la réglementation de 1996.

1999 : décrets autorisant les algorithmes dont les **clés ne dépassent pas 128 bits.**

2004 : LCEN, Loi 2004-575 du 27 juin 2004, **libéralisation**.

Autres pays : Chaque pays a ses propres lois. En outre, les règles de communication chiffrée entre deux pays varient selon les couples de pays considérés.

VII – Quelques références

Directive NIS : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

GDPR (UE) 2016/679 : http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1477991939126&uri=CELEX:32016R0679

ANSSI : http://www.ssi.gouv.fr/ (dont CERT France)

CNIL : http://www.cnil.fr/

Lois : http://www.legifrance.com/

CERT : http://www.cert.org/
http://www.auscert.org.au/

OSSIR : http://www.ossir.org/

CLUSIF : http://www.clusif.fr/