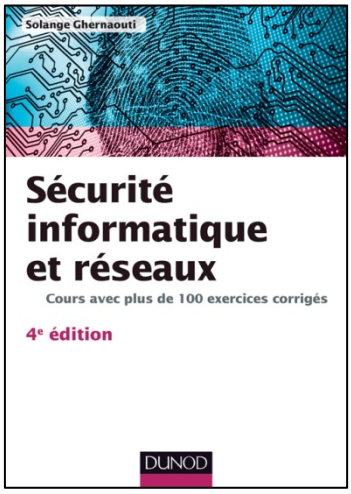

SECURITE INFORMATIQUE ET RESEAUX

CHAPITRE 1

Exercice 1.12

Définir la notion d'intégrité des données ainsi que les objectifs du contrôle d'intégrité.

L'intégrité est l'état d'une chose qui est demeurée intacte. Pour ce qui concerne des données, l'objectif du contrôle d'intégrité est de vérifier qu'elles n'ont pas été altérées tant de façon intentionnelle qu'accidentelle.

Exercice 1.13

Quelles relations existent entre les critères d'intégrité et de confidentialité ?

La confidentialité des données est le maintien du secret des informations. L'information n'a pas été modifiée de manière non autorisée (intégrité), l'information n'est pas compréhensible par des personnes non autorisées (confidentialité). Les critères d'intégrité et de confidentialité sont complémentaires, lorsqu'ils sont réalisés par des fonctions *ad hoc* de sécurité, ils permettent de développer la confiance dans la véracité de l'information.

Exercice 1.14

Dans quelle mesure la notion de qualité des données est-elle liée à celle de sécurité ?

La qualité est généralement une caractéristique d'excellence, reflétant une valeur, une compétence. Dans la mesure où des données possèdent un certain degré de sécurité et satisfont des exigences de disponibilité, d'intégrité ou de confidentialité, elles possèdent un degré intrinsèque de qualité et elles permettent d'offrir des services de qualité.
En respectant les critères de sécurité, la satisfaction d'exigences de la qualité comme la justesse et la fiabilité, peut être réalisée.

Exercice 1.15

Parmi les critères de sécurité suivants, lequel n'est pas adapté à un système d'information ?

A) Confidentialité B) Intégrité C) Insolvabilité D) Non-répudiation

Réponse C

Exercice 1.16

Dans quelle mesure peut-on considérer des principes d'éthique comme faisant partie d'une démarche de sécurité informatique ?

Le dictionnaire Le petit Robert nous rappelle que « *l'éthique est la science de la morale, l'art de diriger la conduite* ». Les qualités morales des acteurs qui conçoivent, gèrent, mettent en place, utilisent les systèmes informatiques sont nécessaires pour assurer les critères techniques de sécurité. On ne peut assurer l'intégrité ou la confidentialité des données par exemple, si les personnes qui sont habilitées à les manipuler ne sont pas intègres, ou sont malveillantes. L'humain est toujours le maillon faible de la chaîne sécuritaire mais il peut être également producteur de sécurité à condition qu'il respecte une certaine éthique compatible avec les valeurs de sécurité de l'environnement dans lequel il opère.

CHAPITRE 2

Exercice 2.16

Sur quels principes se fonde la réalisation d'attaques informatiques ?

La réalisation d'attaques informatiques se fonde sur le leurre, le détournement, l'usage abusif des technologies, la manipulation d'information, l'exploitation des failles et vulnérabilités, l'usurpation d'identités et de paramètres de connexion d'ayants droit.

Exercice 2.17

Quelle est la place de la maîtrise de la cybercriminalité dans une démarche de cybersécurité ?

Il est nécessaire de renforcer la cybersécurité pour diminuer les vulnérabilités des environnements à protéger contre des cyberattaques, diminuer les opportunités de réaliser des malveillances, dissuader les attaquants potentiels.
Bien sécuriser un environnement suppose que l'on connaisse les menaces contre lesquelles on souhaite se prémunir, l'origine des menaces, les auteurs de malveillance, leurs boîtes à outils, leurs savoir-faire opérationnels afin de mettre en place des mesures de sécurité adaptées. La maîtrise de la cybercriminalité, contribue par une approche interdisciplinaire, à contribuer à la réalisation de la cybersécurité.

Exercice 2.18

Pourquoi qualifie-t-on un virus de « polymorphe » ?

Un virus polymorphe est un virus qui change de signature (d'apparence) à chaque infection, ce qui rend sa détection difficile.

Exercice 2.19

Quels sont les points communs entre un virus, un cheval de Troie, une bombe logique et un logiciel espion ?

Il s'agit de logiciels malveillants dont la charge et le mode de réalisation varient en fonction de la finalité.
Un cheval de Troie ne se duplique pas, tandis que la réplication caractérise un virus. Une bombe logique est un virus dont la charge malveillante se déclenche à une date ou selon un événement particulier.

Exercice 2.20

Parmi les infrastructures qui composent un système d'information laquelle ne peut être concernée par une cyberattaque ?

A) Matérielle B) Réseau C) Logicielle D) Exploitation E) Structurelle

Réponse E

Exercice 2.21

Parmi les trois propositions suivantes, laquelle correspond le mieux à la définition d'une infraction informatique telle qu'établie par l'OCDE ?

A) « *Tout comportement illégal, immoral ou non autorisé qui implique la transmission et/ou le traitement automatique de données.* »

B) « *Tout comportement illégal qui implique l'usage de l'informatique et des télécommunications*. »

C) « *Tout comportement illégal, immoral ou non autorisé qui n'implique pas la transmission et/ou le traitement automatique de données*. »

Réponse A

Exercice 2.22

Parmi les attaques informatiques suivantes quelle est celle qui peut être qualifiée d'attaque passive ?

A) Modification B) Interception C) Fabrication D) Interruption E) Destruction

Réponse B

CHAPITRE 3

Exercice 3.18

Quels sont les facteurs et les acteurs qui contribuent à déterminer le niveau de protection des ressources informatiques d'une organisation ?

Les **principaux facteurs** sont :
– L'importance, la valeur de la ressource à protéger par rapport au métier et besoin de l'organisation.
– Le niveau de dépendance de l'organisation à la ressource considérée (il peut s'agir de processus, de fonctions, de personnes…).
– Le fait qu'une ressource puisse être soumise à une réglementation particulière (contraintes légales).
– Les contraintes financières.
– L'existence de personnes compétentes au sein de l'organisation pour prendre en charge cette tâche.

Les **principaux acteurs** sont les dirigeants de l'entreprise au niveau stratégique (*top manager*, comité de direction, conseil d'administration), la responsable sécurité au niveau opérationnel ainsi que les responsables métier et les propriétaires des ressources.

Exercice 3.18

Expliquer comment le concept de « séparation des tâches » contribue à la sécurité informatique d'une organisation.

En matière de sécurité informatique, la séparation des tâches contribue à prévenir des fraudes d'origine interne dues à des pouvoirs excessifs accordés à une même personne qui s'avère être malhonnête (notion de moindre privilège).

Exercice 3.19

Pourquoi pour une organisation, la stratégie de sécurité de l'information est fonction de la stratégie générale de celle-ci ?

Au sein d'une organisation, la sécurité de l'information a pour finalité de lui permettre de réaliser sa mission dans de bonnes conditions (les informations à partir desquelles les décisions sont prises sont disponibles, intègres et parfois confidentielles lorsqu'il s'agit d'informations stratégiques). La sécurité de l'information lui permet d'être compétitive, elle répond donc directement aux besoins de sa stratégie générale.
La sécurité ne doit pas être perçue comme un frein à la bonne marche de l'organisation mais doit constituer un levier de réalisation de ses objectifs tels que spécifiés dans la stratégie générale. Une sécurité de l'information cohérente constitue un avantage compétitif.

Exercice 3.20

Parmi les propositions suivantes quelle est celle qui correspond le mieux au besoin de gérer la sécurité ?

A) Traiter la sécurité comme une exigence du business.

B) Appréhender et traiter la sécurité comme un processus continu.

C) Appréhender et traiter la sécurité comme un processus discontinu.

D) Appréhender et traiter la sécurité comme un processus connu.

Réponse B

Exercice 3.20

Parmi les assertions suivantes quelle est celle qui ne caractérise pas la sécurité informatique d'une organisation ?

A) Une vision à long terme

B) Un mal nécessaire

C) Un compromis

D) Du bon sens

Réponses B

Exercice 3.21

Quels sont les principes de base à prendre en compte dans la démarche sécuritaire d'une organisation ?

Les principes de base d'une démarche sécuritaire sont les principes de : vocabulaire, de volonté directoriale, financier, de cohérence, de simplicité et d'universalité, de dynamicité, de continuum, d'évaluation, de contrôle et d'adaptation.

CHAPITRE 4

Exercice 4.16

Quels sont les éléments constitutifs d'une politique de sécurité ?

Les principaux éléments constitutifs sont : le champ d'application de la politique, les responsabilités, les procédures d'implémentation et de contrôle.

Exercice 4.17

Qu'apporte la notion de « gouvernance de la sécurité » par rapport à celle de « management de la sécurité » ?

La principale différence entre la gouvernance et le management de la sécurité réside dans la finalité de ces deux tâches. Le « management de la sécurité » répond à la question du « Comment réaliser la sécurité aux niveaux opérationnel et stratégique ». En revanche, la

« gouvernance » répond au besoin de pouvoir diriger et contrôler la manière dont la sécurité est réalisée.

Exercice 4.18

Comment se définit un risque résiduel ? Que signifie-t-il dans un contexte de maîtrise des risques informatiques ?

Un risque résiduel est le risque qui persiste malgré les mesures de sécurité prises par une organisation pour les mettre sous contrôle (ex. : tremblement de terre). Un risque résiduel peut faire l'objet selon sa nature, sa probabilité d'occurrence et ses impacts d'une assurance ou de mesures de continuité des affaires par exemple.

Exercice 4.19

Laquelle des propositions suivantes ne concerne pas une politique de sécurité ?

A) Simple et compréhensible

B) Aisément réalisable

C) Facilement maintenable

D) Vérifiable et contrôlable

E) Approuvée par l'ensemble du personnel

Réponse E

Exercice 4.20

Parmi les propositions suivantes, laquelle ne devrait pas faire partie d'une politique de sécurité de l'information ?

A) Politique de gestion de crise

B) Politique de gestion des ressources humaines

C) Politique de contrôle d'accès

D) Politique de sensibilisation

E) Politique de gestion des incidents

Réponse B

Exercice 4.21

Parmi les normes ISO suivantes, laquelle propose un code de bonnes pratiques d'un système de management de la sécurité de l'information ?

A) ISO 27011

B) ISO 27002

C) ISO 27007

D) ISO 27004

E) ISO 27001

Réponse B

Exercice 4.22

Parmi les normes ISO suivantes, laquelle définit les exigences de sécurité d'un système de management de la sécurité de l'information ?

A) ISO 29999

B) ISO 29977

C) ISO 27277

D) ISO 27999

E) ISO 27001

Réponse E

Exercice 4.18

Parmi les propositions suivantes, laquelle correspond à l'acronyme « PDCA » ?

A) PREPARE – DO – CHECK - ACT

B) PLANIFIER – DURCIR – CONTINUER – ARRÊTER

C) PLAN – DO – CHECK – ACT

D) PLAN – DO – CHECK – ARREST

Réponse C

CHAPITRE 5

Exercice 5.14

Quels services de sécurité, une fonction dite « *one-way function* » permet-elle de réaliser ? Citer un nom de « *one-way function* ».

Une fonction dite « *one-way function* » ou fonction de « *hashage* » ou encore fonction « *digest* » comme MD5 ou SHA, permet de réaliser un service de contrôle d'intégrité.

Exercice 5.15

Quels services de sécurité la stéganographie permet-elle de réaliser ? Qui de manière générale utilise la stéganographie ?

La stéganographie est une application particulière du chiffrement qui permet de dissimuler une information dans une autre. Cela contribue à réaliser la confidentialité de l'information masquée. Toute personne souhaitant communiquer des informations de manière discrète, voir confidentielle utilise ce type de service, notamment pour des communications relatives à des actions criminelles ou terroristes. Par ailleurs, les techniques de tatouage électronique de document reposent sur des principes stéganographiques.

Exercice 5.16

Quels critères de sécurité la cryptographie ne permet pas de réaliser ?

La cryptographie ne permet pas d'obtenir la disponibilité des ressources, tandis que les critères d'intégrité, de confidentialité, et d'authentification peuvent être réalisés par la mise en œuvre du chiffrement.

Exercice 5.17

Lequel de ces algorithmes de chiffrement est qualifié d'asymétrique ?

A) DES

B) AES

C) RSA

D) BB 84

Réponse C

CHAPITRE 6

Exercice 6.16

Pourquoi le protocole IPSec fonctionne en mode connecté ?

Parce que pour pouvoir authentifier deux entités communicantes il faut qu'elles soient en relation et que ces dernières s'accordent sur les mécanismes de sécurité à utiliser lors de leurs échanges de données. Le service d'authentification d'un émetteur et d'un récepteur qu'offre la mise en œuvre du protocole IPSec ne peut se réaliser qu'en mode connecté. De plus, l'établissement d'une association de sécurité IPSec permet de négocier le contexte de sécurité à utiliser lors de l'échange.

Exercice 6.17

Pourquoi la gestion des identités (*Identitiy Managment*) est devenue une fonction cruciale pour la sécurité du système d'information des organisations ?

La gestion des identités permet de réaliser le contrôle d'accès aux ressources d'un système d'information, qui est une fonction cruciale de la sécurité.

Exercice 6.18

Parmi les solutions existantes de mécanisme de contrôle d'accès basé sur de la biométrie, qu'elle est généralement la plus mal acceptée par les utilisateurs ? Pourquoi ?

Des mécanismes biométriques de contrôle d'accès basé sur l'empreinte de la rétine ou de l'iris sont jugés très intrusifs par les utilisateurs et sont souvent encore le plus souvent mal acceptés de ces derniers.

Exercice 6.19

Quel protocole permet de créer un réseau privé virtuel, VPN (*Virtual Private Network*) ?

Le protocole IPSec.

Exercice 6.20

Quels sont pour une organisation, les principaux risques introduits par l'usage de solutions de *cloud computing* ?

Les principaux risques sont notamment liés à la perte de contrôle des données par leurs propriétaires, une plus grande dépendance de ces derniers à la disponibilité du réseau de télécommunication pour y accéder, à la localisation des données dans des pays tiers qui ne permet pas forcément une sécurité juridique (telle que celle qui pourrait exister dans le pays ou l'entreprise propriétaire des données est implantée), une certaine difficulté à faire réaliser des audits de sécurité, etc.

CHAPITRE 7

Exercice 7.11

Est-ce qu'une cellule peut faire l'objet d'une protection périmétrique ?

Non. La notion de protection périmétrique fait référence à des mesures de sécurité architecturales de cloisonnement d'environnement. Il est impossible de protéger, séparer physiquement une cellule de transmission.

Exercice 7.12

Quels sont les services de sécurité offerts par un réseau UMTS ?

Les services de sécurité offerts sont la confidentialité de l'identité de l'abonné, l'authentification mutuelle, la confidentialité et l'intégrité des données de l'utilisateur et de signalisation.

Exercice 7.13

Définir la notion d'authentification mutuelle dans un réseau cellulaire.

L'authentification est qualifiée de mutuelle dans la mesure où le service de sécurité mis en œuvre permet à la fois d'authentifier l'abonné au réseau mobile et le point d'accès au réseau.

CHAPITRE 8

Exercice 8.12

Pourquoi, dans un réseau d'entreprise, il est recommandé de créer des zones démilitarisées (*DMZ*), à quels besoins cela répond-il ?

Des zones démilitarisées permettent de réaliser une sécurité périmétrique en isolant certains environnements informatiques afin de mieux les protéger, d'en contrôler l'accès et la sortie. Cela permet également d'éviter la propagation d'actions non autorisées ou de logiciels malveillants.

Exercice 8.13

Est-ce qu'un système pare-feu protège contre des attaques par déni de service ?

Non pas directement, il peut être l'objet d'attaque en déni de service mais il peut contribuer à offrir des fonctions de répartition de charge des systèmes dont il contrôle l'accès.

CHAPITRE 9

Exercice 9.16

Quels protocoles peuvent invoquer les services du protocole SSL (*Secure Sockets Layer*) ? Pour se réaliser de quel protocole SSL utilise-t-il les services ?

Des protocoles applicatifs comme les protocoles HTTP ou FTP par exemple, peuvent invoquer les services de sécurité offerts par SSL qui s'appuie pour sa réalisation sur le protocole TCP.

Exercice 9.17

À quel protocole le protocole TLS (*Transport Layer Security*) est-il équivalent ?

Le protocole TLS est équivalent à la version 3 du protocole SSL.

Exercice 9.18

Quels types d'algorithmes de chiffrement utilisent PGP (*Pretty Good Privacy*) ?

Les algorithmes de chiffrement mis en œuvre par PGP peuvent êtres divers et différents en fonction du type de service de sécurité à réaliser (authentification, intégrité ou confidentialité). Il peut s'agir de IDEA, MD5, RSA, Triple DES, Diffie-Hellman…

Exercice 9.19

À quoi correspond la solution 3-D Secure ?

Il s'agit d'une solution de sécurité qui a remplacé, la solution SET (*Secure Electronic Transaction*) afin de sécuriser les payements en ligne. Elle a été développée par Le Groupement des Cartes Bancaires « CB », Atos Origin, XIRING, Trusted Logic et Altasys.

Exercice 9.20

Pourquoi la gestion des droits numériques (DRM) est importante pour une organisation ?

Comme il est difficile de sécuriser des données qui sont hors des frontières traditionnelles du système d'information de l'entreprise du fait notamment de la mobilité, ou de l'usage du *cloud computing*, il est intéressant de pouvoir associer aux données des paramètres de sécurité qui régissent leur protection et le contrôle de leur usage indépendamment de leur localisation ou du support technique sur lequel elles se trouvent (notion de protection persistante).
La gestion des droits numériques contribue à assurer la protection d'un patrimoine numérique et répond en particulier au besoin de protection du droit d'auteur et de la propriété intellectuelle.

Exercice 9.21

Dans quelle mesure l'usage des réseaux sociaux classiques à des fins privées par des employés d'une entreprise peut générer des problèmes de sécurité pour celle-ci.

C'est souvent sur des réseaux sociaux que des informations sont récoltées par des criminels (notion de *social engineering*) ; ce qui leur permet de leurrer certains employés (notion de *spear phishing*) pour les amener à réaliser des actions qui conduisent le plus souvent à l'introduction de programmes malveillants ou à la prise de contrôle de systèmes constitutifs du système d'information de leur entreprise.

CHAPITRE 10

Exercice 10.15

Pourquoi la fonction de dimensionnement d'un réseau est-elle primordiale pour sa sécurité ?

Parce qu'elle contribue à la réalisation du critère de sécurité « disponibilité ».

Exercice 10.16

Pourquoi l'ajout dans un système d'information, d'entités matérielles ou logicielles peut poser des problèmes de sécurité ?

Parce que cela peut éventuellement, d'une part, introduire de nouvelles vulnérabilités et des menaces supplémentaires et, d'autre part, mettre à défaut les mesures de sécurité existantes.

Exercice 10.17

Quels sont les critères de sécurité qui correspondent le mieux à la notion de sûreté de fonctionnement ?

Ce sont les critères de disponibilité et intégrité.

Exercice 10.18

Comment la gestion opérationnelle d'un réseau peut contribuer à la sécurité d'un système d'information ?

La réalisation d'une politique de sécurité passe la mise en œuvre opérationnelle de mesures concrètes de sécurité. Ces dernières doivent faire l'objet d'une exploitation et d'une gestion efficaces, tâches qui relèvent de la gestion opérationnelle d'un réseau informatique.

La gestion opérationnelle d'un environnement informatique distribué comprend notamment toutes les fonctions qui permettent au réseau de fonctionner et d'offrir les services pour lequel il a été conçu, avec un bon niveau de performance et de qualité cela intègre notamment la disponibilité des ressources qui est un des critères de la sécurité informatique.