

Secteur Tertiaire Informatique
Filière « Etude et développement »

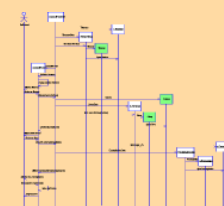
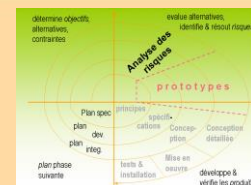
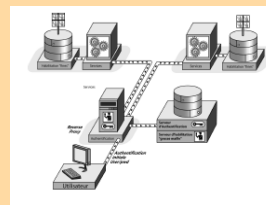
Séquence « Période d'intégration »

Sensibiliser à la sécurité informatique

Apprentissage

Mise en situation

Evaluation



Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

Version	Date	Auteur(s)	Action(s)
1	20/04/16	Lécu Régis	Création du document
2	27/04/16	C. Perrachon	Modifications de forme : suppression ligne blanche après les titres (pour tous les niveaux). Autres modifications en mode révision

TABLE DES MATIERES

Table des matières	3
1. Introduction à la Cyber sécurité	5
1.1 Les enjeux de la sécurité des SI.....	5
1.2 Les besoins de sécurité.....	9
1.3 Notions de vulnérabilité, menace, attaque.....	12
1.4 Panorama de quelques menaces.....	14
1.5 Le droit des TIC et l'organisation de la cybersécurité en France	16
1.6 La Cyber Sécurité : un domaine en pleine évolution.....	18
2. La démarche CYBERDU dans la formation CDI.....	18

Objectifs

A l'issue de la séance, le stagiaire sera capable d'identifier :

- Les risques informatiques classiques
- Les concepts de sécurité informatique : critères DICP, notions de vulnérabilité, menace et attaque
- L'importance de la sécurité dans le développement informatique
- L'intégration de la démarche sécurité dans la formation CDI, selon les préconisations du projet CyberEdu

Pré requis

Aucun : la séance part de la vie courante et de l'actualité, pour dégager progressivement les concepts courants de la sécurité informatique.

Elle fait partie de la séquence d'intégration à la formation CDI :

- La réflexion sur la sécurité informatique peut aider le stagiaire à mieux appréhender le métier de développeur, au même titre que les séances « *S'approprier les objectifs de la formation et repérer son futur environnement professionnel* » et « *Repérer les risques liés à l'exercice du métier et sensibiliser au développement durable* ».
- Elle comporte de nombreuses recherches sur Internet, qui peuvent être conduites en groupe et participer à la constitution du groupe en présentiel.

Méthodologie

Ce document peut être utilisé en présentiel ou à distance.

Chaque slide est accompagné d'un guide de lecture qui précise le vocabulaire technique, et propose des recherches complémentaires, avec des liens sur wikipedia.

Mode d'emploi

Symboles utilisés :



Renvoie à des supports de cours, des livres ou à la documentation en ligne constructeur.



Propose des exercices ou des mises en situation pratiques.



Point important qui mérite d'être souligné !

Ressources

Document du projet CyberEdu : [CyberEdu_module_1_notions_de_base.pdf](#)

1. INTRODUCTION A LA CYBER SECURITE

Cette introduction s'appuie sur le document du projet CyberEdu :

[CyberEdu_module_1_notions_de_base.pdf](#)

Si vous êtes en formation présentielle, ce document sera présenté par le formateur, qui répondra à vos questions. L'exposé pourra être suivi d'une discussion, car la plupart des points sont très concrets et demandent peu de connaissances techniques.

Ce document est suffisamment clair pour que vous puissiez le suivre en autonomie, en suivant le guide de lecture proposé dans ce document et en faisant des recherches complémentaires sur Internet.

Dans les deux cas, ce document vous guidera dans votre découverte de la Cyber Sécurité et son premier principe : *pour être efficace, une politique de sécurité informatique doit se penser à l'échelle de l'entreprise et prendre en compte tous ses aspects.*

1.1 LES ENJEUX DE LA SECURITE DES SI

Si vous découvrez ce chapitre en autonomie, suivre ce



Guide de lecture

a) Préambule

(p. 5)

Bien distinguer le Système d'Information de l'entreprise (SI) d'un système informatique particulier et son système d'exploitation :

- le SI est global à l'entreprise et rassemble toutes ses ressources et ses flux d'informations, y compris les informations non informatisées.
- nous verrons par la suite dans d'autres séquences comment définir de façon systémique un SI avec les méthodes Merise et UML. Une méthode systémique ne se réduit pas à l'informatique : c'est une approche organisationnelle qui prend en compte tous les processus de l'entreprise.
- le SI présente une large surface d'exposition aux attaques, qu'il faudra prendre en compte globalement dans une approche sécurité.

Une bonne politique de sécurité informatique exige donc elle-même une méthode systémique. Même si la sécurité des logiciels occupe une place importante dans la sécurité de l'entreprise, elle n'est jamais suffisante.

(p. 6)

Pour parvenir à un bon niveau de sécurité, il faudra éviter de mettre des œillères et protéger TOUS les « actifs » de l'entreprise. La norme ISO/IEC 27005 de gestion des risques distingue deux types d'actifs : primordiaux ou supports. Voir https://fr.wikipedia.org/wiki/ISO/CEI_27005.

Les « *actifs primordiaux* » se rapportent au savoir faire et à l'activité de l'entreprise :

- processus métiers : quels sont les procédés de fabrication, les activités spécifiques au métier de l'entreprise, qui pourraient être visés par des attaques informatiques, et dont la perte, divulgation ou arrêt ruinerait l'entreprise ou nuiraient énormément à son activité ?

Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

- informations sensibles : brevets, secrets industriels dont la divulgation nuirait énormément à l'activité.

Ces actifs primordiaux sont donc des biens immatériels indispensables à la survie de l'entreprise. Mais ils sont nécessairement liés à des « *actifs supports* » : différents sites géographiques pour une grande entreprise, le personnel, les matériels utilisés.

Chacun de ces actifs supports peut présenter des vulnérabilités qui vont permettre de s'attaquer aux actifs primordiaux supportés et compromettre le fonctionnement de l'entreprise.

Une bonne politique de sécurité doit donc évaluer tous les composants du SI : réseau, sauvegardes, sorties papier et leur destruction, éducation du personnel à la sécurité.

Donnons quelques exemples.

Les *hackers* ou utilisateurs malveillants attaqueront toujours les composants les plus fragiles du SI, qui ne sont pas nécessairement les systèmes ou les applications informatiques :

- Réseau : il ne sert pas à grand-chose de mettre en œuvre une méthode d'authentification par nom d'utilisateur et mot de passe, si les mots de passe sont envoyés en clair sur le réseau et peuvent être facilement interceptés par un utilisateur malveillant, équipé d'un logiciel espion.
- Mauvaise utilisation des supports papier : à quoi bon encrypter les données sensibles dans des bases de données sécurisées si ces données sont accessibles sur des supports papier ?
 - L'approche sécurité rejoint sur ce point les préoccupations environnementales : il faut limiter au maximum l'utilisation du papier.
 - Pour les supports papier indispensables, il faut protéger leur accès et les détruire après usage (broyeur).
- Education du personnel à la sécurité : il est souvent plus facile de baser une attaque sur la crédulité des personnes que sur une véritable faille informatique. Par exemple, se faire passer pour un collègue au téléphone, et demander les mots de passe système, que l'on a prétendument oubliés, en intervenant sur un site distant.

b) Les enjeux

(p. 7) « *Réduire* » les risques à un niveau acceptable pour « *limiter leurs impacts* », et non pas les éliminer. Un deuxième principe de sécurité informatique : il ne peut pas y avoir de risque zéro.

Une politique de sécurité bien conduite doit chiffrer les risques, définir le niveau d'acceptabilité en fonction du domaine de l'entreprise (défense, site de vente internationale, petite association peu connue) et proportionner les moyens de défense au niveau voulu.

(p. 7) On ne peut mener une politique de sécurité efficace sans la participation et l'implication de tous les salariés : développeurs informatiques, exploitants, équipe réseau, et tous les utilisateurs.

Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

La politique de sécurité doit donc être proportionnée et réaliste pour ne pas gêner les utilisateurs et les salariés de l'entreprise (« *obstruction* »). « Trop de lois tuent la loi » s'applique en sécurité informatique : il ne faut pas dégoûter les utilisateurs en multipliant les interdictions, mais les convaincre du bien-fondé d'un petit nombre de règles que tous vont appliquer. Il ne peut y avoir ni qualité ni sécurité sans l'adhésion du groupe.

Quelques exemples pour convaincre les salariés de l'importance de la politique de sécurité de l'entreprise :

- Le fichier RH (ressources humaines) est-il protégé avec des autorisations différentes pour que des informations essentielles ne soient pas connues de tous ? Tout le monde peut avoir besoin de connaître l'étage et le téléphone de son interlocuteur, mais dans les pays latins, personne n'apprécie que son salaire soit divulgué publiquement ;
- Confidentialité des mails professionnels qui sont aussi souvent utilisés comme mails personnels.

(p. 8) « *Impacts juridiques et réglementaires* » :

- une entreprise peut être rendue responsable des préjudices causés à ses clients, suite à la « compromission » de ses fichiers clients : démarche abusive, escroquerie avec usurpation d'identité.
- la loi évolue dans le sens d'une double responsabilité : en premier celle de l'attaquant mais aussi en second celle de l'entreprise qui n'a pas su parer l'attaque, par son incompetence.

« *Impacts sur l'image et la réputation, impacts financiers* »

- cas classique d'une entreprise spécialisée dans la sécurité informatique, qui voit son site Web attaqué (défacé ou défiguré) : le Logo altéré avec un humour hacker, le PDG avec des oreilles d'âne. Ce qui paraît être une blague de potache peut avoir des conséquences terribles sur la vie de l'entreprise : perte de crédibilité, départ des clients, effondrement boursier.

« *Impacts organisationnels* »

- L'attaque par « déni de service » consiste à empêcher totalement le fonctionnement d'un serveur ou le ralentir fortement, pour arrêter son activité normale.
- Cette attaque classique a un fort impact organisationnel, puisque l'entreprise ne peut plus être contactée par ses clients, ses fournisseurs, voire ses sites distants.
- Exemple : le déni de service par les *anonymous* contre les banques qui avaient retiré leur crédit à *WikiLeaks*.

c) Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

(p. 9) Pour lutter efficacement, il faut connaître son adversaire. En sécurité informatique, il faut abandonner l'image du bidouilleur enthousiaste, presque sympathique, qui conduit des attaques empiriques au cas par cas.

Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

Comme décrit dans le slide, les attaquants sont aujourd'hui, majoritairement, des organisations bien structurées : états, entreprises concurrentes, organisations terroristes, services secrets.

La rumeur selon laquelle les virus sont souvent écrits et propagés par les fabricants d'antivirus est bien sûr exagérée, mais elle a un fond de vérité : elle rappelle la complexité, la technicité des menaces informatiques actuelles, et elle est plus près de la vérité que l'image du bidouilleur.

L'« *hacktiviste* » infiltre des systèmes informatiques ou des organisations en mettant ses compétences au service de ses convictions politiques, par des opérations coup de poing technologiques : piratages, détournements de serveurs, remplacement de pages d'accueil par des tracts. Exemple : les « anonymous ».



Pour approfondir : <https://fr.wikipedia.org/wiki/Hacktivisme>

(p. 10)

« *botnet* » : réseau de *bot*, ou machine zombie. Ce sont des machines qui peuvent être contrôlées à distance à l'insu de leur utilisateur et détournées de leur utilisation normale.

Elles peuvent alors servir à différentes activités illicites :

- utilisées comme serveur, elles peuvent stocker et mettre en ligne des contenus illégaux.
- un *botnet* de grande taille permet de réaliser des dénis de service, en envoyant de nombreuses requêtes à un serveur web, pour l'occuper à 100% et lui interdire de répondre à ses véritables utilisateurs.



Pour approfondir : <https://fr.wikipedia.org/wiki/Botnet>

d) La nouvelle économie de la cybercriminalité

(p. 11-12)

Il ne faut pas tomber dans la théorie du complot en pensant qu'il y a une organisation unique responsable de toutes les attaques et les malversations sur Internet !

Mais il y a effectivement une « *économie* » des actions malveillantes, avec une connexion entre différents systèmes de délinquance : un numéro de carte peut être volé par un *keylogger* (logiciel espion qui enregistre toutes les saisies ou les envoie à un serveur), et stocké dans une base de données. Il sera ensuite mis en vente sur des sites illégaux pour une somme modique, et permettra d'effectuer des achats illégaux, de jouer sur des sites en ligne.

Avec Internet, ce type de fraude s'est globalisé et il n'est pas toujours évident pour la victime d'une cyber-attaque d'obtenir réparation, voire parfois de savoir qu'elle a été attaquée.

e) Les impacts de la cybercriminalité sur la vie privée

(p. 13)

Le « *cyber-harcèlement* » (« *cyber-bullying* »), est une forme de harcèlement conduite par divers canaux numériques : création de faux profils, rumeurs infondées, messages d'insulte.



Pour approfondir : <https://fr.wikipedia.org/wiki/Cyberharcèlement>



Avez-vous déjà été victime d'une attaque sur Internet et dans quelles conditions : virus, utilisation frauduleuse de votre carte bancaire, revente de vos coordonnées bancaires et utilisation frauduleuse répétée, usurpation d'identité, cyber-harcèlement ?

Les impacts de la cybercriminalité sur les infrastructures critiques

(p. 14)

La cybercriminalité ne se limite pas aux attaques individuelles et à l'informatique de gestion : elle peut s'attaquer à des automates industriels et aux systèmes de contrôle et de supervision dans les usines, les barrages, les centrales nucléaires.

Elle devient donc un risque majeur pour de nombreuses installations (classées OIV « Opérateur d'Importance Vitale » pour la nation).



Exemple : le virus « Stuxnet », virus complexe qui a été conçu pour s'attaquer à des systèmes industriels spécifiques (les centrifugeuses dans les centrales nucléaires iraniennes).

Pour approfondir : <https://fr.wikipedia.org/wiki/Stuxnet>

g) Quelques exemples d'attaques



Rechercher des exemples d'attaques récentes :

<http://www.zataz.com/les-50-attaques-informatiques-qui-ont-marque-le-web-francais-en-2015/#axzz44N2Qibjd>

1.2 LES BESOINS DE SECURITE

Nous sommes partis de l'actualité, de la description des utilisateurs malveillants, de leur motivation et des attaques qui constituent la partie la plus visible dans le domaine de la sécurité informatique.

Nous allons maintenant nous rapprocher de notre métier, **le développement informatique sécurisé**, en classant ces attaques selon ce qu'elles mettent en danger, le type de risque encouru, et lui associer le « besoin de sécurité » qui lui correspond.

Toutes les techniques de sécurisation du logiciel que nous aborderons dans cette formation se rapportent à l'un ou plusieurs de ces critères.

Si vous découvrez ce chapitre en autonomie, suivre ce



Guide de lecture

a) Introduction aux critères DIC

(p. 23)

Remarquons que les trois critères se rapportent d'une manière ou d'une autre à l'accès aux données. En cas d'attaque sur la :

Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

- **Disponibilité** : l'accès est tout simplement rendu impossible pour tous les utilisateurs, ou pour les utilisateurs autorisés.
- **Intégrité** : l'accès en écriture est rendu possible pour des utilisateurs non autorisés, ce qui va permettre une « compromission » des données (incohérence ou incomplétude des données).
- **Confidentialité** : l'accès en lecture est rendu possible pour des utilisateurs non autorisés, ce qui va permettre une divulgation de données confidentielles.

b) Besoin de sécurité : Preuve

(p. 24)

Les trois premiers critères sont des besoins de sécurité essentiels. Le quatrième critère, la **Preuve**, est une mesure de la sécurité d'un système :

- **La traçabilité** : on peut savoir par des fichiers d'historique, ce qui a été fait sur le système (fichiers créés, supprimés ou modifiés, accès aux bases de données, création d'un compte utilisateur, modification d'un mot de passe).
- **L'authentification** : les utilisateurs doivent se faire connaître avant de pouvoir utiliser le système informatique (par un compte avec un mot de passe, une carte de service, l'empreinte digitale).

Le mécanisme d'authentification est indispensable à la défense de la Confidentialité et de l'Intégrité d'un système : une fois authentifié, l'utilisateur ne reçoit que les permissions nécessaires en lecture et en écriture, sur les ressources auxquelles il a droit.

- **L'imputabilité** : en croisant les deux premiers critères (traçabilité et authentification), on peut toujours savoir qui a fait une action, dont il sera tenu pour responsable.

Le critère de Preuve est indispensable pour qu'un système informatique ait une valeur juridique :

- je valide une commande sur Internet.
- je signe un contrat électronique, sans document papier.

En suis-je responsable, est-ce vraiment moi qui ai effectué cette action, un autre utilisateur du système sous sa propre identité ou un autre utilisateur qui a usurpé mon identité ?

b) Différences entre sûreté et sécurité

(p. 26)

Dans le contexte du développement logiciel :

- La « **sûreté** » d'un logiciel : il est bien conçu, bien codé et fonctionne comme prévu dans son cahier des charges, dans des conditions normales d'utilisation.

Par exemple, un logiciel de mesures sera dit « fiable » s'il assure une continuité de service, sans interruption. Il est « intègre », si le système n'est pas soumis à des perturbations qui faussent ses mesures.

- La « *sécurité* » d'un logiciel : sa capacité à résister à des utilisateurs et des actions malveillantes. Par exemple, pour le logiciel de mesures : est-on sûr que les mesures proviennent des capteurs ? Peut-on introduire des fausses mesures dans le dispositif ?

Sur le schéma à droite, on remarque que trois propriétés sont communes à la sûreté et à la sécurité, avec des nuances : Disponibilité, Intégrité, Confidentialité.

La maintenabilité (possibilité de « maintenir » le logiciel en fonctionnement après sa livraison) et la fiabilité sont propres au langage de la sûreté.

c) Exemple d'évaluation DICP

Le développeur informatique ne doit pas chercher à tout faire lui-même, particulièrement dans le domaine de la sécurité. Mais il doit pouvoir collaborer avec d'autres métiers, et tenir compte des résultats qui lui sont fournis.

Un auditeur en sécurité informatique peut évaluer les besoins en sécurité d'une entreprise, d'un service, d'un système ou d'un logiciel, existant ou à réaliser, selon les critères DICP.

Comme il n'est pas possible de tout sécuriser à 100%, et que le développement du logiciel doit être adapté au niveau de risque acceptable, le développeur s'appuiera sur l'analyse de risque pour adapter au mieux le logiciel.

Exemple du site Web statique :

- **Disponibilité et Intégrité**: ce sont ses atouts majeurs. Un site perd une bonne partie de ses visiteurs à chaque indisponibilité. Et c'est encore pire s'il est « défacé » avec des faux produits, des prix erronés.
- **Confidentialité et preuve** : faible, puisqu'il est par nature public et que l'utilisateur ne fait que consulter les informations. C'est bien sûr très différent pour un site dynamique de commerce en ligne, où il faut garantir la confidentialité de l'achat et sa preuve juridique (validation de la carte bancaire).

d) Mécanisme de sécurité pour atteindre les besoins DICP

Les outils de sécurité (à gauche) sont maintenant connus de la plupart des utilisateurs informatiques. Ils sont complémentaires et tous nécessaires à la sécurité informatique : il ne suffit pas d'installer un anti-virus pour que le système devienne invulnérable !

Quelques commentaires pour comprendre le lien entre ces outils et les critères DICP :

Anti-virus :

- **Disponibilité** : un virus informatique peut, en détruisant des fichiers ou la totalité du système, rendre celui-ci indisponible
- **Intégrité** : il peut compromettre les données, par des écritures dans des fichiers ou en base de données

Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

- **Confidentialité** : certains virus nuisent à la confidentialité, en communiquant à votre insu les données à des utilisateurs malveillants (« chevaux de Troie », *back door*, porte dérobée),



Pour approfondir [http://fr.wikipedia.org/wiki/Porte dérobée](http://fr.wikipedia.org/wiki/Porte_d%C3%A9rob%C3%A9e)

Cryptographie :

Le « chiffrement » des données (par exemple dans une liaison *https*) interdit l'accès aux utilisateurs qui ne possèdent pas les clés de « déchiffrement », et contribue donc à la **confidentialité** et à l'**intégrité** des données.



Pour approfondir <https://fr.wikipedia.org/wiki/Chiffrement>

Pare-feu (*firewall*) :

L'anti-virus protège le système contre une attaque directe d'un logiciel malveillant. Le chiffrement protège les données. Le pare-feu filtre les accès réseau au système : il participe à la **Disponibilité** et à la **Confidentialité** du système, puisqu'on ne peut attaquer ou connaître ce à quoi on n'a pas accès.

Contrôle d'accès logique :

Exemple : l'onglet « sécurité » de l'explorateur Windows, permet d'attribuer des autorisations en lecture, écriture, exécution aux différents utilisateurs ou groupes d'utilisateurs de votre système.

Sécurité physique des équipements et locaux :

Il est plus difficile de protéger un système d'un utilisateur malveillant qui travaille en local sur le système, que d'un utilisateur distant : d'où l'importance de la protection physique des locaux dans la politique de sécurité de l'entreprise.

1.3 NOTIONS DE VULNERABILITE, MENACE, ATTAQUE

Les critères **DICP** définissent ce qui est attendu d'un système informatique sécurisé. Ce sont les faiblesses (**vulnérabilités, failles**) dans un ou plusieurs de ces critères, exploitées par des utilisateurs ou du code malveillants (**menaces**) qui vont permettre les **attaques**.

Si vous découvrez ce chapitre en autonomie, suivre ce



Guide de lecture

Un exemple non informatique, pour définir le vocabulaire :

- La vulnérabilité : un volet non fermé, une serrure bas de gamme
- La menace : le voleur
- L'attaque : le cambriolage où le voleur va exploiter les accès les moins protégés.

Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

En informatique comme dans la vie courante, il n'y a jamais de sécurité parfaite et on ne peut que retarder l'attaquant : la meilleure serrure ne résiste que quelques minutes à un vrai cambrioleur. Mais elle décourage les débutants et le gain de temps permettra peut-être une intervention externe, pour faire échouer le cambriolage.

a) Notion de vulnérabilité

(p. 32)

Le développement informatique est au centre de la sécurité informatique, parce qu'il intervient dans toutes les phases où peuvent se glisser des vulnérabilités :

- Au départ, on comprend mal la demande du client et l'environnement du logiciel et on conçoit mal le logiciel : par exemple, en envoyant les mots de passe en clair dans un lieu public, en wifi.
- Dans la phase de réalisation (codage ou programmation), on ne prévoit pas certains bugs qui vont permettre une exploitation malveillante du logiciel.
- Dans la phase de configuration du logiciel et d'installation chez le client : on peut réduire à néant la sécurité d'un logiciel bien conçu et bien codé, en définissant des mots de passe faibles (trop courts et pas assez diversifiés).

b) Notion de menace

(p. 33)

Une bibliothèque de quartier a les mêmes vulnérabilités qu'une grande banque : portes, fenêtres. Mais il n'est pas nécessaire de la sécuriser de la même manière !

- Dans l'analyse de risque d'une entreprise ou d'une application, la recherche des menaces est donc un deuxième point d'entrée. Comme il est en général impossible d'éliminer toutes les vulnérabilités, il faut dimensionner correctement la stratégie de sécurité, en se posant les questions :
 - Par qui peut-on être attaqué et dans quelles conditions ?
 - Qu'est-ce qui rend cette attaque vraisemblable ?
- A noter, la diversité des menaces : humaine, logicielle, interne ou externe.

Un système d'information sécurisé est organisé comme un château fort avec des fossés et un donjon. Il est prévu pour se défendre contre un attaquant extérieur, et il est plus vulnérable contre une menace interne (le « *stagiaire malintentionné* »).

c) Notion d'attaque

(p. 34 et 35)

La sécurité logicielle va donc consister à réduire autant que possible les vulnérabilités du système d'information. Ce qui est tolérable va dépendre du contexte et des scénarios d'attaque possibles.

d-f) Exemple de vulnérabilité

(p. 36 à 38)

Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

A retenir de l'exemple, différence entre bug et vulnérabilité :

- dans la plupart des bugs, le logiciel plante, sort en exception, n'est plus fonctionnel ;
- il y a vulnérabilité, si suite à un bug ou une action intentionnelle de l'utilisateur malveillant, le logiciel continue à fonctionner de façon non conforme à son cahier des charges, ce qui permet une « exploitation » du bug.
- dans l'exemple, le logiciel VNC ne plante pas, mais il ne contrôle pas la cohérence des échanges avec l'utilisateur, et valide la connexion même si le mot de passe n'est pas fourni.

1.4 PANORAMA DE QUELQUES MENACES

Ce chapitre analyse quelques menaces type. Les exemples sont choisis pour illustrer la diversité des menaces et des attaquants.

Si vous découvrez ce chapitre en autonomie, suivre ce



Guide de lecture

a) Sources potentielles de menace

(p. 40)

Un schéma pour lutter contre les idées reçues. A noter :

- Le *hacker* ou « *cyber-délinquant* » individuel est au bas de l'échelle des menaces, car il est à l'extérieur de l'entreprise et a relativement peu de connaissances et de ressources techniques pour mener à bien ses attaques ;
- Le « *personnel interne* » a un accès plus direct aux ressources de l'entreprise, et constitue une menace plus importante ;
- Les « *états* » sont des menaces importantes, car ils ont des ressources techniques considérables et une motivation (espionnage militaire ou industriel).

c) Hameçonnage & ingénierie sociale

(p. 42 à 44)

Ces deux attaques visent le même objectif : récupérer des données confidentielles, à des fins d'escroquerie ou de prise de contrôle du système d'information.

Mais :

- Le « *phishing* » ou Hameçonnage comporte toujours une partie technique. Il faut construire un faux site Web qui se fait passer pour le vrai, et qui va capturer l'identifiant et le mot de passe.



Pour approfondir <http://fr.wikipedia.org/wiki/Hameçonnage>

- « *L'ingénierie sociale* » n'a pas nécessairement de partie technique. C'est une version moderne de l'arnaque, qui peut réussir avec des scénarios très simples : on peut

Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

appeler l'ingénieur système, en se faisant passer pour un collègue en clientèle qui a oublié le mot de passe système.



Pour approfondir

[http://fr.wikipedia.org/wiki/Ingénierie_sociale_\(sécurité_de_l'information\)](http://fr.wikipedia.org/wiki/Ingénierie_sociale_(sécurité_de_l'information))

d) Déroulement d'une attaque avancée :

(p. 45 à 48)

A noter : une attaque est d'autant plus grave qu'elle comporte une possibilité d'escalade : dans l'exemple, on commence par prendre le contrôle d'une « *machine cible* » qui va ensuite servir de « *tête de pont* », dans l'attaque avancée.

En contrôlant à distance la tête de pont, le hacker est vu comme un utilisateur normal de l'entreprise en interne (il est à l'intérieur du château fort) ce qui va permettre un autre type d'attaque plus technique vers les serveurs de l'entreprise, qui abritent les mots de passe des utilisateurs, etc.

Exemple :

L'attaque par ingénierie sociale peut être très efficace, en utilisant peu de techniques informatiques : une simple recherche sur Internet permet souvent de trouver les dates de naissance des *People*, leurs amis, le nom de leurs chiens et de répondre facilement aux questions de sécurité, qui permettent d'obtenir un nouveau mot de passe, en le déclarant perdu.

e) Fraude interne :

(p. 49)

- La plus dangereuse, car l'attaquant est déjà dans les murs et la plupart des dispositifs de défense sont ciblés pour des attaquants extérieurs.
- Il y a peu de publicité et de statistiques sur ce type d'attaque, car les entreprises n'en sont pas fières.
- Comme dans l'affaire Kerviel avec la Société Générale, les fraudes internes ont généralement des raisons complexes qui dépassent l'aspect informatique : procédures de contrôle insuffisantes ou mauvaise mise en œuvre de ces procédures.

f) Violation d'accès non autorisé : mot de passe faible

(p. 50)

C'est une attaque simple mais répandue, qui vise à la fois les entreprises et les individus.

Une sécurité s'écroule s'il y a au moins un maillon faible : il ne sert à rien de bien concevoir et coder un logiciel avec une méthode d'authentification fiable, si à la fin l'administrateur choisit « abc » ou « toto » comme mot de passe système.

Le mot de passe suffit pour un usage domestique mais pas pour une banque ou une entreprise avec un besoin important en sécurité.

Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

Autres moyens :

- « *token USB* » : clé USB qui permet d'authentifier l'utilisateur de façon unique (par exemple, lors d'un accès distant vers son entreprise)
- « *one time password* » : mot de passe à usage unique, qui change à chaque nouvelle connexion. Ceci évite que le mot de passe soit capturé et réutilisé par un utilisateur malveillant.

Violation d'accès non autorisé : intrusion

(p.51)

« **Active Directory** » : c'est un produit Microsoft de type « Annuaire » (*directory*) qui regroupe les ordinateurs et les utilisateurs d'une entreprise dans un « domaine », pour permettre le partage des comptes utilisateurs entre les différentes machines.

La « **compromission** » d'un domaine signifie que certains comptes sont piratés et que des utilisateurs malveillants peuvent se connecter sur les postes de travail et/ou les serveurs du domaine.

Le « **cloisonnement** » des réseaux : comme rien n'est sûr à 100%, il est souhaitable d'isoler les différents réseaux de l'entreprise, pour limiter la propagation d'une attaque.

Par exemple, à l'AFPA, le réseau de formation sur lequel vous travaillez est indépendant du réseau de gestion de l'entreprise.

« **Test d'intrusion** » : simulation d'attaque réalisée par une équipe de spécialistes sécurité, pour mesurer l'efficacité d'une politique de sécurité interne.

h-i) Dénî de service et Botnet

(p.53 et 54)

Reprenons le scénario de l'attaque avancée :

- Le hacker, par une attaque de Hameçonnage ou d'ingénierie sociale, parvient à contrôler votre PC à distance, qui devient une « machine zombie » (*bot*)
- le réseau des Machines Zombies contrôlées par le hacker ou le groupe de hackers constitue un *botnet* qui pourra ensuite être utilisé pour lancer une attaque de type **DDoS** (*Distributed Denial of Service*, déni de service distribué).
- Toutes les machines zombies envoient des requêtes au serveur visé par le DDoS pour occuper la bande passante et lui interdire de répondre aux vraies requêtes.

1.5 LE DROIT DES TIC ET L'ORGANISATION DE LA CYBERSECURITE EN FRANCE

Ce chapitre organisationnel et juridique ne traite pas de notre métier de développeur informatique.

Il faut néanmoins le lire, car nous sommes concernés en tant que citoyens, utilisateurs informatiques et salariés d'entreprise. Quelques remarques :

a) Sur l'organisation de la sécurité en France

Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

(p.56 à 58)

La **Cyber Sécurité** est devenue un enjeu national, qui justifie d'introduire les concepts et la pratique de la sécurité dans toutes les formations informatiques, dont celles du développement informatique (projet **CyberEdu** conduit par l'**ANSSI, Association nationale de la sécurité des systèmes d'information**)

La Cyber Sécurité regroupe trois notions : la SSI (Sécurité des systèmes d'information), la **Cyber Défense** (aspect militaire, attaques étatiques), et la **Cyber Criminalité** (attaques d'individus, de mafia).

Pour être efficace, la Cyber Sécurité a besoin comme toutes les disciplines, de spécialistes, mais ceux-ci ne suffisent pas :

- les exemples précédents montrent qu'il suffit d'un maillon faible pour annuler toute une politique de sécurité ;
- il faut donc que chacun soit formé à la sécurité et participe à son niveau, dans la conception, le codage, le déploiement et l'exploitation des logiciels informatiques, dans l'installation et l'administration des systèmes et des réseaux.

b-c) Le droit des TIC (Technologie de l'information et de la communication)

(p. 59 et 60)

La pratique précède souvent la formalisation juridique.

Le droit des TIC est encore en train de se constituer, puisqu'il concerne un domaine complètement neuf.

Il procède souvent par analogie avec des situations non informatisées :

- par exemple, le vol d'un objet physique prive son propriétaire de son usage ;
- le vol de données, le téléchargement frauduleux de livres ou de films, est une atteinte à la propriété intellectuelle, où le propriétaire légitime est lésé sans être privé de son original.

d) La lutte contre la cybercriminalité en France

(p. 61 à 63)

A noter :

- L'importance de la condamnation pénale (2 à 5 ans) qui est souvent méconnue du public.
- La définition des délits qui n'est pas intuitive : accéder indument à un système d'information, sans nuire à l'entreprise, est passible de 2 ans de prison ferme.
- Le périmètre de la cybercriminalité qui concerne tous les STAD (Système de Traitement Automatisé de Données) : postes de travail et serveurs mais aussi téléphones, réseau téléphonique, réseau bancaire, disque dur, etc.

e) La CNIL

(p. 64 à 68)

Pour le dire de façon simple, la CNIL joue le rôle de contre-pouvoir : la Cyber Sécurité vise en général à protéger les systèmes informatiques contre des individus ou des organisations malveillantes.

Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

La CNIL défend le droit des individus face aux moyens informatiques : définition des données personnelles admissibles, procédures formalisées de déclaration de fichiers, droit à l'oubli sur Internet.

Cet aspect nous concerne d'abord comme citoyen, mais peut aussi avoir une incidence professionnelle : quelles données pouvons nous conserver sur un client ou un utilisateur ? Dans quelles limites, peut-on tracer une boîte aux lettres d'entreprise ? Tracer le travail d'un collaborateur en entreprise ? Ses recherches sur Internet ?



Pour approfondir <http://www.cnil.fr/>

1.6 LA CYBER SECURITE : UN DOMAINE EN PLEINE EVOLUTION

La Cyber Sécurité est un métier à part entière, mais c'est aussi une compétence utile pour tout développeur, qu'il faut entretenir, car elle évolue vite !

Parallèlement à l'apprentissage du métier de développeur dans la formation CDI, il est conseillé de s'intéresser à l'actualité de la sécurité informatique (attaques, vulnérabilités, menaces) en menant une veille technologique personnelle.

Quelques sites de référence, parmi ceux que nous utiliserons dans la formation CDI :

- L'ANSSI, organisme de référence français : <http://www.ssi.gouv.fr/>
- Le CERT, référence pour les alertes de sécurité : <http://www.cert.ssi.gouv.fr/>
- OWASP, référence pour le développement web : <https://www.owasp.org>

2. LA DEMARCHE CYBERDU DANS LA FORMATION CDI

Le chapitre précédent suffit à démontrer que pour être efficace, la sécurité informatique ne doit pas être réservée aux spécialistes :

- Elle doit être mise en œuvre par tous les professionnels qui interviennent dans le processus d'informatisation : développement, réseau, système.
- L'ensemble du personnel, y compris l'utilisateur de base, doit être sensibilisé à la sécurité informatique, pour éviter des attaques de type ingénierie sociale.

Le Projet **CyberEdu**, conduit par l'ANSSI, vise donc à professionnaliser tous les acteurs du processus informatique, dans le domaine de la sécurité, sans qu'ils deviennent pour autant de nouveaux experts en sécurité informatique. Chacun doit intégrer la sécurité dans son domaine d'activité.

Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »

Quelle est la place du développement dans la sécurité informatique ?

- La sécurité informatique ne se réduit pas au développement logiciel, puisque les vulnérabilités peuvent résulter spécifiquement de problèmes système ou réseau.
- Mais le développement logiciel sous toutes ses formes (logiciel de base, système d'exploitation, réseau, applications) occupe une place centrale dans la sécurité informatique, puisque toute vulnérabilité logicielle aura des conséquences à haut niveau.
- Pour rendre robuste un système informatique, il faut donc contrôler le processus de développement dans toutes ses phases : analyse, conception, codage, déploiement, maintenance.

En suivant les règles du projet **CyberEdu**, la formation « Concepteur Développeur Informatique » présentera et mettra en pratique les principes de la sécurité informatique dans toutes les phases du développement, et toutes les activités de la formation.

Faire un module de sécurité informatique (pour préparer un examen et passer à autre chose ?) ne sert à rien.

Cette séance de sensibilisation sert à lancer un chantier sécurité qui durera pendant toute la formation. Vous pourrez y participer par une veille technologique sur les principaux sites dédiés à la sécurité.

Il faut que la sécurité devienne une préoccupation normale du développeur :

- le plus souvent, cela demande peu de connaissances spécialisées, mais une attention soutenue pour bien développer.
- les critères du développement sécurisé rejoignent souvent les bonnes pratiques de développement objet et de qualité logicielle
- le développement sécurisé est avant tout un point de vue : notre logiciel fonctionne bien dans un cas normal, mais que se passerait-il si un utilisateur malveillant tentait intentionnellement des actions non prévues dans le cahier des charges ?



Pour en savoir plus sur le projet CyberEdu :

<http://www.ssi.gouv.fr/particulier/formation/cyberedu/>

CRÉDITS

OEUVRE COLLECTIVE DE L'AFPA

Sous le pilotage de la DIIP
et du centre sectoriel Tertiaire

EQUIPE DE CONCEPTION

Chantal PERRACHON – IF Neuilly-sur-Marne
Régis Lécu – Formateur AFPA Pont de Claix

Reproduction interdite

Article L 122-4 du code de la propriété intellectuelle.

« Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droits ou ayants cause est illicite. Il en est de même pour la traduction, l'adaptation ou la reproduction par un art ou un procédé quelconque. »

Sensibiliser à la sécurité informatique

Afpa © 2016 – Section Tertiaire Informatique – Filière « Etude et développement »