Chapitre 1

Politique de sécurité et analyse de risques

1.1 Analyse de risques Ebios : généralités

Exercice 1 : Bien supports et menaces génériques (*[Age10a, Chapitres 1, 2, 4]*)

1. Classer les bien supports suivants selon les catégories : *matériels (MAT), logiciels (LOG), canaux informatiques et de téléphonie (RSX), personnes (PER), supports papier (PAP), canaux interpersonnels (CAN), locaux (LOC)* :
   — fibre optique
   — document imprimé
   — cartouche de sauvegarde
   — commutateur téléphonique
   — assistant personnel (PDA)
   — SGBD Oracle
   — discussions de couloir
   — salle de réunion
   — Linux
   — client de courrier électronique
   — poste de travail
   — salle de conférence
   — ligne téléphonique
2. Proposer des exemples d'impacts génériques : sur le fonctionnement, les humains, les biens. Quels autres impacts ne rentrent pas dans les catégories précédentes ?
3. Pour les catégories LOG et CAN précentes, proposer des menaces génériques en précisant le(s) critère(s) de sécurité concernés et les vulnérabilités exploitables. Par exemple pour PER on proposerait "Dissipation de l'activité d'une personne" par l'exploitation du temps de travail, du blocage de l'accès d'une personne ou l'exploitation d'une personne en dehors de ses prérogatives. Cette menace porte atteinte à la disponibilité de la personne et sera efficace sur les sujets à la dissipation.

Exercice 2 : Évaluation des risques (*[Age10c, p. 62]*)

L'action 4.1.1. de la méthode Ebios « Analyser les risques » consiste à mettre en évidence l'ensemble des risques qui pèsent réellement sur le périmètre de l'étude et à déterminer leur gravité et leur vraisemblance, une première fois sans tenir compte des mesures de sécurité existantes, et une seconde fois en les prenant en compte. On fait ainsi le lien entre les événements redoutés et les scénarios de menaces, c'est-à-dire entre ce que l'organisme craint et ce à quoi il est exposé.

1. Connaissant les résultats produits par les étapes précédentes de la méthode, expliquer comment identifier les risques.

1.2 Analyse de risques Ebios : cas d'étude UCBL

Description du cas La Direction du Système d'Information (DSI) de l'UCBL désire mettre en place une Politique de Sécurité du Système d'Information (PSSI). La complexité du SI impose d'utiliser une méthode pour recenser et classifier exactement ce qu'il faut sécuriser. La méthode Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) est retenue pour conduire cette étude et aboutir à la définition de la PSSI. Parmi les services de l'UCBL, notons celui des *finances*, en charge de la comptabilité, de la gestion des budgets, des marchés et des payes. Les services financiers s'appuient sur le logiciel SIFAC (Système d'Information, Financier Analytique et Comptable) hébergé sur un serveur du bâtiment Braconnier. Notons que l'activité services financiers n'est pas régulière, en effet, ces services sont particulièrement sollicités chaque fin de mois pour les payes et de façon intense aux mois de novembre et de début décembre avec la clôture de l'exercice budgétaire.

Exercice 3 : Étude du contexte ($[Age10a,\ Age10c]$)

1. Les sources de menaces au sens Ebios sont les sources non humaines (code malveillant, phénomène naturel, catastrophe naturelle ou sanitaire, activité animale, événement interne) ou humaines. Les humaines sont décomposées en interne/externe, avec/sans intention de nuire et selon leur capacité (faibles, importantes, illimitées). Indiquer quelles sont les sources de menaces qui peuvent raisonnablement être écartées du contexte de l'étude.
2. Donner des exemples de sources de menaces pour les types de sources de menaces suivants :
   1. Source humaine interne, sans intention de nuire, avec de faibles capacités ;
   2. Source humaine interne, sans intention de nuire, avec des capacités illimitées ;
   3. Source humaine externe, sans intention de nuire, avec de faibles capacités ;
   4. Source humaine externe, malveillante, avec de faibles capacités ;
   5. Événement interne.
3. Quels sont les critères traditionnels de la sécurité ? La DSI souhaite ajouter le critère de *traçabilité* dans le périmètre de son étude. Proposer une définition de ce critère et justifier l'inclusion de ce nouveau critère dans le contexte.

Exercice 4 : Détermination des objectifs de sécurité ($[Age10a,\ Age10c]$)

Dans le module d'étude des risques Ebios, les risques intolérables du service des finances sont :
— risque lié à l'arrêt de SIFAC en période de clôture ;
— risque lié l'usurpation d'identité sur la messagerie électronique ;

1. Quelles sont, en général, les différentes possibilités de traitement des risques ? Lesquelles sont envisageables dans le contexte de l'étude ?
2. Proposer des mesures de sécurité pour *réduire* les risques.

1.3 Analyse de risques Ebios : cas d'étude @RCHIMED

Description du cas La société @RCHIMED est un bureau d'ingénierie en architecture. Cette PME toulonnaise est constituée d'une douzaine de personnes.

La société @RCHIMED réalise des plans d'usines ou d'immeubles avec l'établissement préalable de devis. Pour cela, elle calcule des structures, élabore des plans techniques pour ses architectes et

propose des maquettes virtuelles pour ses clients. Le suivi des constructions est aussi assuré par le cabinet, qui met à jour les plans et calculs si des modifications sont nécessaires.

Le cabinet d'architecture bâti sa réputation grâce à des solutions architecturales originales basées sur des techniques innovantes. Cette société concourt pour de grands projets nationaux ou internationaux ; elle s'appuie pour cela sur son système informatique qui lui permet de réagir extrêmement rapidement aux appels d'offre ou aux demandes des clients.

Elle attache également une importance extrême à la qualité des documents remis et plus précisément aux maquettes virtuelles (visualisations 3D) qui permettent de donner à ses clients une idée précise et concrète de la solution proposée. Dans un contexte de rude concurrence, rapidité, précision et originalité des travaux sont des composantes essentielles de son activité.

Par ailleurs, elle a créé son site Internet sur lequel sont présentés les informations concernant la société et des exemples de devis et de maquettes virtuelles.

L'informatique de la société est reliée par un réseau wifi et le bureau d'études dispose d'un réseau local de type Ethernet. Le site Internet est hébergé sur un serveur externe. Le bureau d'étude possède 7 ordinateurs, le service commercial 2 ordinateurs portables, le service comptabilité 1 ordinateur, et le service de gestion de site Internet 1 ordinateur.

Sécurité du système d'information Il n'y a pas de principes généraux, ni de politique de sécurité, seulement les quelques règles suivantes :

- le contrôle d'accès se fait par identifiant /mot de passe ;
- principe de sauvegarde de tout fichier ;
- chaque ingénieur est responsable du fichier qu'il traite, les fichiers sont sauvegardés sur des disques USB stockés dans une armoire fermant à clé, située dans le bureau d'études ;
- parallèlement, les documents papiers sont rangés dans une armoire forte du service commercial ;
- en ce qui concerne la maintenance, un contrat a été établi avec les fournisseurs de logiciels avec intervention sous 4 heures.

Conjoncture La mise en réseau des systèmes informatiques s'est effectuée avec succès et a permis de réduire encore plus les délais de réalisation des travaux. L'entreprise doit maintenant répondre au souhait de la majorité des clients qui est de correspondre directement avec le bureau d'étude via Internet pour transmettre tous les types de documents (dossiers techniques, devis, appel d'offre, messages...).

L'entreprise a dernièrement perdu un marché : la rénovation de la mairie de Draguignan. Lors de la présentation des projets, il est apparu de curieuses similitudes entre la maquette virtuelle d'@RCHIMED et la proposition d'un concurrent de Nice. Le directeur d'@RCHIMED soupçonne une compromission du projet qu'il avait présenté. Il a maintenant des craintes sur la confidentialité de certains projets.

D'autre part, de plus en plus de contrats pour lesquels @ARCHIMED souhaite se positionner sont conditionné par la capacité du cabinet à assurer la confidentialité relative aux aspects techniques du projet. Par exemple, L'appel d'offre pour la rénovation de certaines installations de la marine nationale de l'arsenal de Toulon entre dans ce cadre.

Compte tenu de son volume et de sa disposition, la société travaille de façon très ouverte. Cependant, les experts du bureau d'études sont les seuls à pouvoir accéder aux logiciels les plus performants de conception et de maquettage. Ces experts ont par ailleurs bénéficié d'une formation à la manipulation de ces outils. Chacun est conscient de ces responsabilités financières, civiles et pénales associées à l'usage des informations qu'il manipule : dossier client, données nominatives...

Le choix d'une étude de sécurité s'impose donc pour, d'une part, déterminer les conditions qui permettent l'ouverture du système informatique vers l'extérieur et d'autre part pour déterminer les mesures de sécurité nécessaires à la protection des projets sensibles.

Exercice 5 : étude du contexte (*[Age10b, p. 15, p.18]*)

1. Donner des exemples de sources de menaces à prendre en compte dans l'étude pour les types de sources de menaces suivants :
   1. Source humaine interne, sans intention de nuire, avec de faibles capacités ;
   2. Source humaine interne, sans intention de nuire, avec des capacités illimitées ;
   3. Source humaine externe, malveillante, avec des capacités importantes ;
   4. Source humaine externe, malveillante, avec des capacités illimitée ;
   5. Source humaine externe, sans intention de nuire, avec de faibles capacités ;
   6. Événement interne.
2. Identifier 3 processus (métiers) essentiels du cabinet. Quelles sont les informations essentielles concernées ?

Exercice 6 : étude des événements redoutés (*[Age10b, p. 22]*)

Pour les activités de création de plans et de calculs de structures, évaluer les événements redoutés selon les 3 critères de sécurité disponibilité, intégrité, confidentialité. On utilisera les échelles suivantes :

— Disponibilité : *plus de 72h* $\preceq$ *entre 24 et 72h* $\preceq$ *entre 4 et 24h* $\preceq$ *moins de 4h*.
— Intégrité : *détectable* $\preceq$ *maîtrisé* $\preceq$ *intègre*.
— Confidentialité : *public* $\preceq$ *limité* $\preceq$ *réservé* $\preceq$ *privé*.
— Gravité : *négligeable* $\preceq$ *limitée* $\preceq$ *importante* $\preceq$ *critique*.

Evt.	Besoin	Source	Impacts	Gravité
Indisponibilité				
Altération				
Compromission				

Exercice 7 : étude des scénarios de menaces (*[Age10b, p. 24]*)

Détailler les sources et la vraisemblance des menaces portant sur le réseau wifi. On utilisera l'échelle de vraisemblance suivante : *minime* $\preceq$ *significative* $\preceq$ *forte* $\preceq$ *maximale*.

Menace	Source	Vraisemblance
Menaces sur le réseau wifi causant une indisponibilité		
Menaces sur le réseau wifi causant une altération		
Menaces sur le réseau wifi causant une compromission		

Exercice 8 : détermination des objectifs de sécurité (*[Age10b, p. 41 à 48]*)

Au terme de la conduite de la méthode, les risques intolérables identifiés sont :

— risque lié à l'altération d'un devis qui doit rester rigoureusement intègre ;
— risque lié à la compromission d'un devis au-delà du personnel et des partenaires ;
— risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres ;

— risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires.

Proposer des mesures de sécurité portant sur le bien support « serveurs logiciels du réseau interne » pour réduire ces risques. Quelles autres mesures fautdrait'il appliquer pour compléter les précédentes ?

1.4 Politique de sécurité

Exercice 9 : Critères non-fonctionnels des systèmes (*[GH11, ex. n° 1.1]*)

Remplir le tableau récapitulatif en identifiant pour chacune des capacités d'un système, les critères associés (*authenticité, auditabilité, intégrité, imputabilité, sûreté, exactitude, fiabilité, disponibilité, accessibilité, continuité, traçabilité, confidentialité*) et des exemples de mesures qui contribuent à les assurer.

Capacité	Critères	Mesures
Exécuter des actions		
Permettre l'accès aux entités autorisées		
Prouver les actions		

Exercice 10 : Rentabilité d'une politique de sécurité (*[AJO10, ex. n° 105]*)

Une entreprise remarque que, statistiquement, elle souffre chaque année de 5 infections virales et 3 défigurations de son site web. La remise en état après une infection coûte 2 jours de travail de l'administrateur, soit environ 2000 €. La remise en état du site web nécessite environ 500 €. On évalue la mise en place d'un produit d'antivirus ainsi qu'un système de protection pour le site web à environ 30.000 € par an.

1. À partir des données numériques précédentes, évaluer le retour sur investissement des mesures envisagées.
2. En quoi cette évaluation n'est pas adéquate, que faut'il prendre en compte d'autre ?

Exercice 11 : Niveau de sécurité (*[AJO10, ex. n° 104]*)

On appelle *security gap* la constatation que le niveau réel de sécurité d'un système d'information est toujours inférieur à celui estimé. De plus, cette différence de niveau tend à augmenter à mesure que le temps passe.

1. Donner deux raisons qui expliquent cette différence.
2. Décrire le genre de mesures à prendre pour éviter une baisse du niveau de sécurité.

Exercice 12 : Audit de sécurité (*[AJO10, ex. n° 106]*)

Une entreprise organise un appel d'offre pour faire auditer la sécurité de son réseau. Trois offres sont proposées :

1. un *audit conceptuel* : plans, schémas et configurations du réseau sont demandés. À partir de ces informations, l'expert estimera si le réseau est sûr ou non ;
2. un *scan de vulnérabilités* : à l'aide de sondes spécialisées placées à différents endroits du réseaux, l'expert découvrira automatiquement les vulnérabilités des équipements ;
3. un *test d'intrusion* : sans aucune information préalable, l'expert tentera de pénétrer le réseau de l'entreprise depuis Internet et de s'approprier des informations confidentielles.

Chaque audit est utile à sa manière. Pour chacun, décrire une situation qui en ferait l'usage approprié.