Université d'Alger1
Faculté des sciences
Département informatique

Série TD 5

Gestion des risques
EBIOS

Exercice 1.

Indiquez dans le tableau ci-dessous quel est le terme (utilisé dans la méthode EBIOS) qui correspond le plus à chacun des exemples suivants :

Service d'annulation de réservations en ligne, Serveur, partenaire, se venger d'un organisme, indisponibilité d'un service, équipe en charge du projet, concurrents, générer une crise sanitaire, employés vengeurs
local technique, données à caractère personnel, modification illégitime du seuil de température haute d'un processus industriel, services étatiques, espionnage industriel, client, administrateurs, résultats de travaux de recherche, services étatiques, hacktivistes, divulgation de données, phase de déploiement d'un projet, prestataire, dispositif de vidéo protection, diffuser un message idéologique, informations clients, réseau de téléphonie, savoir-faire en conception de pièces industriel., service de supervision, passerelle d'interconnexion, modification d'une base de données, Voler des informations à des fins lucratives, département de recherche& développement.

Valeurs métiers	
Bien supports	
Partie prenante	
Evènement redouté	
Source de risque	
Objectifs visés par une source de risque	

Exercice 2.

Indiquer pour chaque élément dans le tableau ci-dessous, s'il est utile pour estimer la gravité ou la vraisemblance.

Importance de la valeur métier considéré	
Expositions aux menaces considérées	
Existence de vulnérabilité	
Facilité d'exploitation des vulnérabilités	
Capacité et motivation des sources de risque	
Nombre d'impacts identifié	

Exercice 3.

Identifiez la valeur métier, le bien support, l'évènement redouté (avec l'objectif de sécurité altéré et l'impact de ce dernier) ainsi que la source du risque et l'objectif visé liés à chacun des exemples suivants :

1- Un site de e-commerce se dispose d'une base de données clients, présente sur un serveur de son parc informatique et contenant les informations bancaires de ces derniers. Un utilisateur externe a pu accéder à la BD des clients à travers le réseau.

2- Un adolescent de quinze ans a en effet été interpellé pour s'être introduit dans le système informatique de son collège dans le but de modifier ses résultats scolaires. Dépité de n'avoir pu atteindre ce but, le collégien a saturé le système informatique en expédiant plus de 40 000 courriels, manoeuvre qui a provoqué une indisponibilité pendant quatre jours.

3- Des escrocs sont parvenus à convaincre un directeur financier d'une entreprise que la direction lui ordonnait de verser d'importantes sommes sur un compte tiers.

4- Un raid surprise a dû être annulé avant-hier à cause d'un soldat israélien qui avait mis à jour son statut Facebook pour indiquer "mercredi nous nettoyons Qatanah, et jeudi, si dieu le veut, nous rentrons à la maison". Le soldat a depuis été relevé de son poste de combat.

Exercice 4.
Lisez l'énoncer suivant puis répondez aux questions.

La société @RCHIMED est un bureau d'ingénierie en architecture qui réalise des plans d'usines ou d'immeubles avec l'établissement préalable de devis. Sa structure organisationnelle est fonctionnelle avec une direction, un service commercial, un bureau d'études, un service comptabilité et un service de gestion de site internet.

Dans le bureau d'étude, la société élabore des plans d'exécution pour ses professionnels, des calculs de résistance de structure et matériaux (le calcule se base sur des paramètres techniques de calcule) et propose des maquettes virtuelles pour ses clients. Ces activités reposent sur un dossier technique du projet qui définit les normes et les procédures en vigueur. 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 présentées 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 (des ordinateurs pour le design et d'autres pour le calcul et la création), le service commercial 2 ordinateurs portables, le service comptabilité 1 ordinateur, et le service de gestion de site Internet 1 ordinateur.

Le cabinet a acquis les logiciels ARC+ pour le maquettage virtuel, SIFRA pour le travail à partir de tablettes graphiques et SPOT pour les calculs de résistance des matériaux. Le bureau d'études possède également un outil de présentation assisté par ordinateur (PAO) appelé Pagemaker. Tous les services sont équipés d'une suite bureautique. Les ordinateurs du bureau d'étude sont équipés de MAC OS X, le reste du cabinet est équipé de Windows XP.

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.

Question 1 : Donner des exemples de sources de menaces à prendre en compte dans l'étude pour chacun des types de sources de menaces suivants :

Source humaine interne, sans intention de nuire, avec de faibles capacités ;	
Source humaine interne, sans intention de nuire, avec des capacités illimitées ;	
Source humaine externe, malveillante, avec des capacités importantes ;	
Source humaine externe, malveillante, avec de faibles capacités	
Source humaine externe, sans intention de nuire, avec des capacités importantes	
Source humaine externe, sans intention de nuire, avec de faibles capacités ;	
Événement interne.	
Type général	

Question 2 : Identifier 3 processus (métiers) essentiels du cabinet et pour chacun les informations essentielles concernées ?

Processus métiers essentiels	Informations essentielles conercnées

Question 3 : Classer les bien supports de la société suivants selon les catégories : *Matériels (MAT), logiciels (LOG), canaux informatiques et de téléphonie (RSX), personnes (PER), supports papier (PAP), canaux interpersonnels (CAN),*
Locaux (LOC) :

Réseau interne,
Sous réseau Ethernet,
Sous réseau Wifi,
Ligne téléphonique
Système de l'hébergeur (Internet et pour courrier électronique),
Hébergeur (pour courrier papier),
Internet (pour des accès distants et le courrier électronique),

Partenaire (cotraitants bâtiment, clients…).
Salle de conférence
Poste de travail
Utilisateurs interne
partenaitres (cotraintants, clients, ..ETC)
Administrateurs informatique
Outil de messagerie
Suite bureautique
MAC OS X
Windows XP
Imprimante
ARC+ (pour visualisation) LOG
Spot (calcul de résistance) LOG
Pagemaker (PAO)
Système de l'hébergeur ()
Système de l'hébergeur
Internet

Question 4 : Identifiez les bien supports liés au bureau d'étude.

Question 5 : Pour les activités de création de plans et de calculs de structures, identifier les événements redoutés selon les 3 critères de sécurité disponibilité, intégrité, confidentialité en précisant pour chacun quelques impacts possibles.

Besoin de sécurité	ER	Impact	Gravité
Disponibilité			
intégrité			
confidentialité			

NB. Proposez une évaluation de la gravité de chaque ER selon l'échelle suivante :

- Niveaux de l'échelle	- Description détaillée de l'échelle
- Négligeable	- @RCHIMED surmontera les impacts sans aucune difficulté.
- Limitée	- @RCHIMED surmontera les impacts malgré quelques difficultés.
- Importante	- @RCHIMED surmontera les impacts avec de sérieuses difficultés.
- Critique	- @RCHIMED ne surmontera pas les impacts (sa survie est menacée).

Question 6 : Pour le risque lié à l'altération de plans ou de calculs de structures, détaillez les sources et la vraisemblance des menaces donnée dans le tableau suivant :

La menace	Source de menace	vraisemblance
Menaces sur le réseau Ethernet causant une altération		
Menaces sur le sous réseau		

Ethernet causant une altération		
Menaces sur l'organisation d'@RCHIMED causant une altération		
Menaces sur un partenaire causant une altération		

NB. Pour l'évaluation de la vraisemblance, on utilisera l'échelle suivante :

- Niveaux de l'échelle	- Description détaillée de l'échelle
- Minime	- Cela ne devrait pas se (re)produire
- Significative	- Cela pourrait se (re)produire.
- Forte	- Cela devrait se (re)produire un jour ou l'autre.
- Maximale	- Cela va certainement se (re)produire prochainement.

Question 7 : Au terme de la conduite de la méthode, le risque lié à l'altération de plans ou de calculs de structures a été identifié comme étant un risque intolérable.

Citer quelques mesures de sécurité à considérer dans cette étude pour réduire ce risque.