BUT R5.CYBER.12
(Analyse de risques)

Jean-Marc Pouchoulon

Octobre 2023

1 Environnement du TP et notation.

1.1 Objectifs du TP:

En sécurité des systèmes d'informations, les techniciens pensent en général Firewall, IPS/IDS, antivirus ... C'est une activité importante, mais sans savoir ce qu'il faut protéger ces mesures techniques n'ont pas de sens.

L'objectif de ce TD/TP est de vous montrer comment définir ce qui est important à protéger : les biens ou actifs du système d'information. Il va s'agir pour vous d'acquérir un mode de raisonnement sur l'analyse de risques.

L'analyse de risque permet de faire le lien entre le terrain et les "généraux" de l'entreprise. Il fera avancer la sécurité dans votre entreprise. Ce n'est pas à l'informaticien mais au décideur de haut niveau de trancher entre *l'acceptation , la réduction, la délégation et la supression* des risques que vous aurez mis en évidence.

EBIOS Risk Manager est la méthode d'analyse de risques recommandée par l'A.N.S.S.I. (version précédée par EBIOS 2010). C'est celle que vous utiliserez durant ces TD/TP. Mais il en existe beaucoup d'autres.

1.2 Organisation, recommandations et notation du TP.

Il peut vous être explicitement demandé de faire valider votre travail au cours du TP par l'enseignant au fur et à mesure de votre avancement. Tous les travaux sont à déposer sur l'ENT de l'IUT. Un travail doit être enregistré avec les noms des personnes dans le nom du fichier, et l'intitulé du fichier doit être clair (par ex: TP_EBIOS_Etudiant1_Etudiantn). Les délais sont parfois et exceptionnellement négociables, mais une fois fixés doivent être respectés sous peine d'une note nulle.

L'objectif de cette séance est de vous former à "penser risques". .

2 Exercices sur la gestion des risques

2.1 Analyse d'un risque autour d'un cycliste

On se propose d'analyser simplement les risques auxquels s'expose un cycliste sans protection sur la route.

1. Quel est le bien essentiel à protéger ?
2. Quel est la vulnérabilité principale affectant le bien essentiel à protéger ?
3. Quel est la menace ?
4. Quels sont les impacts de cette menace sur le bien essentiel ?
5. Quel est la vraisemblance de ce scénario de risques ?
6. Quel peut être le scénario d'exploitation de la vulnérabilité par le risque ?
7. Quelle est la mesure de réduction du risque qui peut être adoptée ?

8. Refaites un check du risque et des scénarios de menaces en affinant l'analyse (prenez le cas d'un cycliste roulant à plus de 30 Km /heure et sujet à des chocs plus importants ?
9. Quelle mesure pouvez vous proposer pour réduire ce risque ?

2.2 Biens essentiels et biens supports

1. Classez les biens supports suivant selon les catégories issues de la méthode EBIOS 2010 : matériels (MAT), logiciels (LOG), canaux informatiques et de téléphonie (RSX), personnes (PER), supports papier (PAP), canaux interpersonnels (CAN), locaux (LOC) :
   - La fibre optique
   - Le document imprimé
   - Les bandes de sauvegarde
   - L'autocom
   - Un smartphone
   - Le SGBD Mysql
   - Les discussions de couloir
   - Le système d'exploitation Linux
   - client de courrier électronique
   - Le poste de travail
   - La salle de conférence
   - La ligne téléphonique
   - Un étudiant
2. Parmi les biens suivants quels sont les biens essentiels et les biens supports ?
   - Le serveur supportant l'application SCODOC.
   - Les notes des étudiants.
   - Le dossier d'entrée en licence.
   - Le directeur de la licence MRIT si l'étude de risque porte sur l'ouverture de la licence.
   - Les salles de réunion visio de l'IUT
   - L'enseignement des langues
   - Un téléphone professionnel
   - Un carnet d'adresse électronique.
3. Dans le cas d'un tunnel routier quels sont les biens essentiels et les biens supports ?

2.3 Analyse de risque simplifiée sur une évaluation écrite

1. Quel est l'événement redouté pour un enseignant sur une évaluation écrite ?
2. Quel est le bien essentiel ?
3. Quels sont les critères de sécurité concernés (DICT) ?
4. Quels sont les impacts de haut niveau ?
5. Quel est le bien support ?
6. Quelle est la menace ?
7. Quelles sont les vulnérabilités essentielles du bien support ?
8. Quels sont les scenarii de menaces et leurs probabilités d'occurence?
9. Quel est le risque ?
10. Quelles sont les mesures de sécurité à prendre pour limiter ce risque ?

3 Etude de risques sur la vulnérabilité des données d'un chercheur en déplacement.

3.1 Le contexte

Un chercheur est amené à se déplacer 60 jours par à l'étranger pour participer à des conférences . Il voyage avec son ordinateur portable (un lenovo sous windows 10 sans chiffrement). L'ordinateur contient ses articles , des documents de travail et ses messages. Il peut communiquer avec sa base au travers d'une liaison VPN. Il ne se déplace que dans des pays ou le nombre d'enlèvement de personnes est nul, mais sous des latitudes tropicales (fèvre jaune mortelle, dengue, malaria..). Il continue à travailler pendant ses déplacements et communique avec son laboratoire et d'autres entités amies de part le monde. Un laboratoire dépend pour son financement des brevets issus de la recherche. Les chercheurs de ce laboratoire sont en lien avec l'industrie et des processus secrets de fabrication "hi-tech". La plupart encadrent des équipes et ont un besoin permanent de communications.

3.2 Mini étude de risques

1. Quel est le bien essentiel (c'est un processus) ?
2. Quelles sont les biens supports ?
3. A votre sens donnez les deux évènements les plus redoutés par les métiers. Quels en sont les impacts prévisibles (échelle de 1 à 4 du plus faible au plus fort) ?
4. Pour deux des biens supports principaux, donnez leurs vulnérabilités et les menaces possibles.
5. Donnez quelques scenarii de menaces. Quel est la probabilité de ces scenarii ?
6. Exprimez en Français les risques (exploitation d'une vulnérabilité d'un bien support par une menace et donnant lieu à un impact).
7. Proposez des mesures pour réduire les risques.

4 Début d'étude "Ebios Risk Manager" sur l'IUT de Béziers

4.1 Atelier 1: cadrage et socle de sécurité

Il vous est demandé de décrire :

1. La mission principale de l'IUT.
2. Les valeurs métiers associées à cette mission.
3. Les personnes responsables de ces valeurs métiers.
4. Les biens supports associés et les personnes responsables de ces biens supports.
   - Logiciels EDT (ADE) et Apogée (scolarité), CRI de l'université de Montpellier
   - Serveurs Moodle, Apogée, pstage, PC fixes et portables, github, registry, dns, nextcloud, réseau de campus, wifi, firewall, services CRI Montpellier
   - Serveurs scodoc , Apogée
5. d'identifier les évènements redoutés.
   - Corruption du processus d'évaluation (triche et modifications des notes) entraînant la perte de conscience professionnelle des étudiants et des enseignants.
   - Perte de données (notes, cours)
   - Arrêt du réseau (panne), indisponibilité des services de l'IUT.
6. Les impacts associés aux évènements redoutés et la gravité retenue (significative, grave , critique).

4.2 Atelier 2 : Sources de risques et objectifs visés par ces sources de risques

1. Pour chaque évènement redouté, identifier les sources de risques et les objectifs visés par ces sources de risques. Vous donnerez aussi pour chaque source de risque les motivations à atteindre ces objectifs et ses ressources. Sélectionnez les couples source de risque/objectif visé les plus importants.

5 Etude détaillée de risques sur un examen national

5.1 Présentation du cas

L'Examen classant National est un examen qui permet de classer les étudiants de médecine en vue de l'internat. C'est un examen national informatisé.

Votre travail est de réaliser une étude de risques sur ce projet par groupe de deux.

C'est un projet réel qui a fait l'objet d'une présentation aux journées systèmes et réseaux de 2015. Vous aurez pour support la vidéo issue des JRES: `https://video.umontpellier.fr/video/19083-retoursjressurebosexam`
Les supports (présentation et article) sont sur Moodle.

En vu de réduire les risques le guide d'hygiène informatique de l'ANSSI ou la norme ISO 27002 sont vos amis:

— `http://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/guide_hygiene_informatique_anssi.pdf`

Après avoir visionné la vidéo et lu l'article vous pouvez commencer l'étude de risques. Vous avez une feuille de calcul sur l'ENT pour vous aider à remplir les différentes rubriques. Vous la rendrez sur Moodle à la fin de l'étude .

5.2 Etude du contexte

1. Qu'est-ce qui est à l'origine de l'étude (motif, événement...) ?
2. Quel est l'objectif de l'étude (son but et les livrables attendus) ?
3. Comment organisez le travail (actions, rôles, charges...) ?
4. Que sait-on du contexte (externe et interne) ?
5. Qui assure les rôles de MOA (Définition des besoins) et de MOE (hébergement, qualification et l'intégration)
6. Comment les risques sont-ils gérés actuellement ?
7. Quelles sont les limites du périmètre étudié ?
8. Qui doit participer à l'étude ?
9. Quels sont les référentiels applicables (cherchez sur internet on le trouve) ?
10. Quelles sont les contraintes qui pourraient impacter l'étude ?
11. Contre quels types de menaces décide-t-on de se protéger ?
12. Quelles sont les mesures de sécurité existantes ?

5.3 Etude des biens essentiels et des biens supports

Lister les biens essentiels et les biens supports. Réalisez un tableau rattachant à chaque bien support les biens essentiels qui lui sont rattachés.

5.4 Etudiez les évènements redoutés

Les événements redoutés sont obtenus par interview des "métiers". Extrayez-les de la vidéo ou de l'article et imaginez ce que vous pourriez redouter en tant que responsable du département de médecine.

Sur le classeur de calcul le premier onglet est dédié aux échelles (impact et vraisemblance). Dans le cas d'un étude réelle, l'établissement de ces échelles serait de votre responsabilité mais elles vous sont données ici.

5.5 Listez les menaces

Pour celà vous vous servirez du document "EBIOS-2-Bases-de-connaissances" et de l'annexe C de la norme iso 27005 et du document `https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-2-BasesDeConnaissances-2010-pdf`.

5.6 Listez les vulnérabilités

Vous pouvez vous inspirer du guide de sécurisation de l'informatique industrielle et de l'annexe D de la norme iso 27005.

5.8 Réunissez les évènements redoutés et les scénarii de menaces pour analyser les risques

5.9 Prenez la place du décideur et traiter les risques

Acceptez,refusez,réduisez,transmettez les risques...