REPUBLIQUE DE COTE D'IVOIRE

Union-Discipline -Travail

Ministère de l'Économie Numérique
et de la Poste

École Supérieure Africaine des Technologies
de l'Information et de la Communication

Année académique : 2018-2019

MASTER1 SITW

MANAGEMENT DU RISQUES : CAS D'ETUDE LES OPERATEURS MOBILE

Réaliser par

DIE THIERRY DUVAL

SIRI ABOUBAKAR

SOUMAHORO BAKARY

SOMMAIRE

LISTES DES FIGURES

LISTES DES TABLEAUX

INTRODUCTION

Le **management du risque** est la discipline qui s'attache à identifier, évaluer et prioriser les risques relatifs aux activités d'une organisation, quelles que soient la nature ou l'origine de ces risques, pour les traiter méthodiquement de manière coordonnée et économique, de manière à réduire et contrôler la probabilité des événements redoutés, et réduire l'impact éventuel de ces événements. Afin d'aider à rédiger les expressions des besoins de sécurité et à identifier des objectifs de sécurité, ce document présente les différents ateliers de la méthode ebios appliquée à un cas pratique tels que :

- Recenser les valeurs métiers et les biens supports de l'organisation
- Identifier les sources de risques (SR) et les objectifs visés (OV)
- Enumérer l'écosystème et les chemins d'attaque
- Identifier les menaces et les vulnérabilités
- Donner les mesures de sécurités

PARTIE I :
PHASE THEORIQUE

Nous avons essentiellement cinq ateliers que nous allons tenter d'expliquer tout au long du document.

I. ATELIER 1

I.1 Valeur métiers

Les valeurs métiers d'une entreprise représentent les biens essentiels de celui-ci, sans ces biens l'entreprise ne fonctionnerait pas.

Exemple de biens essentiels des opérateurs nous avons l'accès internet, le sms, etc.

I.2 Biens supports

Les biens supports représentent les grandes catégories de composants d'un système d'information sur lesquels reposent les biens essentiels et/ou les mesures de sécurité. Ces biens supports peuvent être soit des systèmes informatiques et de téléphonie (Des matériels, des logiciels, des canaux informatiques et de téléphonie), soit des organisations (Des personnes, des support papiers, des canaux interpersonnel), soit les locaux qui hébergent les autres biens supports et fournissent les ressources.

II. ATELIER 2

II.1 Sources de risque

Les sources de menaces représentent une typologie des choses ou personnes à l'origine des risques. Ces sources peuvent être humaines ou non humaines. Les sources humaines ont un caractère intentionnel ou accidentel mais aussi des sources humaines agissant délibérément (des personnes physiques ou morales malintentionnées), par contre d'autre sources peuvent être non humaines à caractère intentionnel ou accidentel comme les phénomènes naturels mais aussi des sources non humaines agissant délibérément comme les codes malveillants d'origine inconnue.

II.2 Objectifs visés

L'objectif visé par une source de risque peut aller au-delà du seul périmètre de l'objet de l'étude. Dans ce cas, ce dernier est susceptible de servir d'intermédiaire pour atteindre l'OV ou de subir des impacts collatéraux du fait de son exposition au risque.

III. ATELIER 3

III.1 Ecosystème

L'écosystème comprend l'ensemble des parties prenantes qui gravitent autour de l'objet de l'étude et concourent à la réalisation de ses missions (partenaires, sous-traitants, filiales, etc.). De plus en plus de modes opératoires d'attaque exploitent les maillons les plus vulnérables de cet écosystème pour atteindre leur objectif (exemple : atteinte à la disponibilité d'un service en

attaquant le fournisseur de service en nuage, piège de la chaîne logistique d'approvisionnement de serveurs facilitant l'exfiltration de données sensibles).

III.2 Chemins d'attaques

Ils comprennent l'ensembles des canaux utiliser pour nuire au bon fonctionnement de l'organisation.

Exemple :

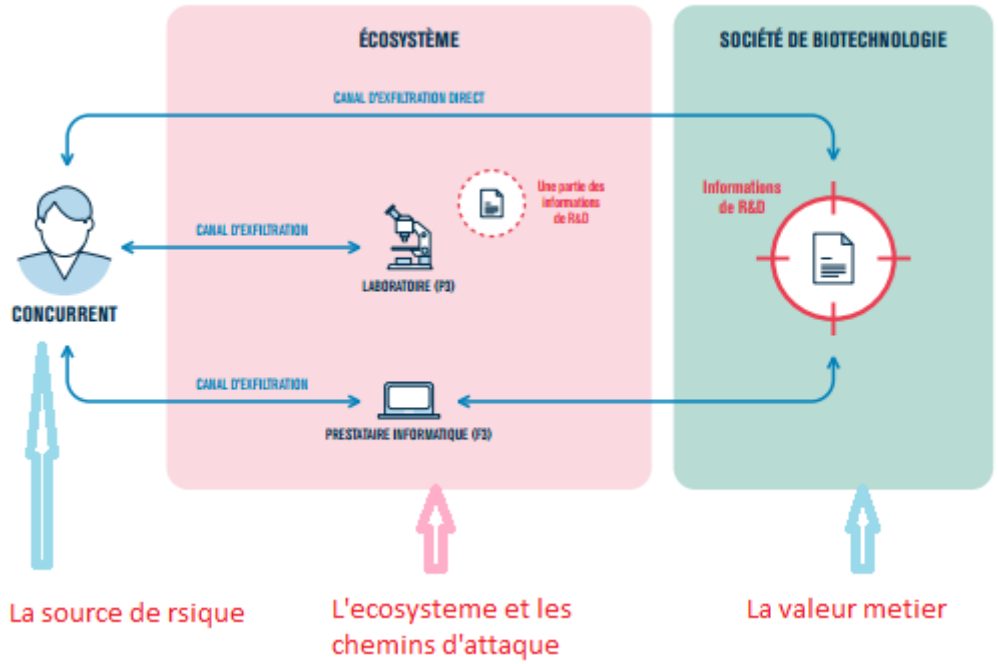

Figure 1: l'écosystème et les chemins d'attaque

IV. ATELIER 4

Les menaces représentent les incidents ou les sinistres types qui peuvent affecter les biens supports et la sécurité des biens essentiels et susceptibles d'affecter la confidentialité, l'intégrité et la disponibilité.

Exemple de menace nous avons : les détournements d'usagers, la modification, l'espionnage etc.

V. ATELIER 5

Cette phase consiste à donner les mesures de sécurités contre les menaces retenues à l'atelier précèdent.

Les fonctions de sécurité

-Authentification
-Signature électronique
- Confidentialité
- Horodatage
- Accusé d’enregistrement et de réception
- Qualification
- Infrastructures de gestion de clés (IGC)
- Politique de sécurité de l'information
- Organisation de la sécurité de l’information
- Gestion des biens
- Sécurité liée aux ressources humaines
- Avant le recrutement
- Pendant la durée du contrat
- Fin ou modification de contrat
- Sécurité physique et environnementale
o Zones sécurisées
o Voies d’eau
o Incendies
- Gestion de l'exploitation et des télécommunications
o Procédures et responsabilités liées à l’exploitation
o Gestion de la prestation de service par un tiers
o Planification et acceptation du système
- Protection contre les codes malveillant et mobile
- Sauvegarde
- Gestion de la sécurité des réseaux
- Manipulation des supports
- Échange des informations
- Surveillance
- Contrôle d’accès aux réseaux, systèmes, serveurs, machines, applications, fichiers, …
- Acquisition, développement et maintenance des systèmes d’information
o Exigences de sécurité applicables aux systèmes d’information
o Mesures cryptographiques
o Sécurité en matière de développement et d’assistance technique
o Gestion des vulnérabilités techniques
- Gestion des incidents liés à la sécurité de l’information
- Gestion du plan de continuité de l'activité
- Conformité avec les exigences légales, les audits.

PARTIE II :

CAS D'ETUDE DES OPERATEURS MOBILE

La **téléphonie mobile en Côte d'Ivoire** est un secteur en évolution. Il y a trois opérateurs : Orange, MTN et Moov. La couverture varie. Dans grandes parties d'Abidjan il y a même une couverture 4G. L'offre de service de téléphonie mobile et d'accès internet mobile d'orange est de 12 406 555 abonnés, ceux de MTN est de 9 059 773 abonnés et ceux de Moov est de 5 984 922 abonnés. Vue l'importance de ces différentes valeurs pour ces opérateurs, l'analyse de risque de ces valeurs seront les bienvenues. Nous effectuerons l'analyse de risque des opérateurs mobile avec la méthode ebios.

VI. Les valeurs métiers et biens supports

Le tableau ci-dessous contient les différents biens essentiels, les biens supports, la description de ces biens ainsi que les entités ou personnes reliées à ces biens.

Valeurs métiers	Mobile Money	Accès internet	SMS	USSD
Description	Le mobile money sert à effectuer les transactions monétaire (retraire et dépôt) et en ligne (payement de facture, les achats en ligne)	L'accès internet nécessite *un réseau *un satellite	Le système de messagerie sert à envoyer et recevoir des messages, à alerter, à faire des pubs	USSD est un type de messagerie plus rapide permettant de : *consulter un compte *souscrire à un service
Entités ou Personnes	Les opérateurs mobiles, les banques, l'ARTCI	Les partenaire Commerciaux, Les entreprises	Les particuliers, Les entreprises	Les particuliers

Biens supports	-Systèmes de base de données (SQL server, oracle), -Poste de travail -Serveur LDAP	-Machine, switch, routeur, -Ordinateur central -Logiciel réseau -Téléphone mobile -Serveur DNS, serveur DHCP -Câble réseau	Service SNMTP -Serveur POP -Téléphone mobile -Ordinateur -Carte mémoire, Disque dur	-Box -Téléphone mobile -Ordinateur -Serveur de messagerie instantané
Description	Ces serveurs permettent d'emmagasiner les données des comptes des utilisateurs	Ces différents matériels permettent d'accéder aux pages web, d'attribuer des bandes passantes aux utilisateurs et de stocker les données des utilisateurs	Ces équipements ont pour rôle d'envoyer des informations, de stocker les données et d'administrer les informations des utilisateurs	Les composants cités plus haut permettent de stocker les messages marketing, les pubs et les informations des utilisateurs
Entités ou Personnes	Business solutions analyste	-Installateurs de réseaux -Stagiaire en recrutement	-Chef projet technique -Stagiaire en recrutement	-Business Manager F/H -Personne charger des projets marketing

Tableau 1:Valeurs métiers et biens supports

VII. Les sources de risque et les objectifs visés

Dans cette partie, nous allons donner les sources de risque, les objectifs visés par les attaquants ainsi que la pertinence de ces risques.

Source de risque humaine interne/externe	Les objectifs visés	La pertinence des menaces
Les collaborateurs malveillants	Test d'intrusion sur le système informatique	Faible
Concurrent	Voler les informations	Elevé
Ancien employé désirant se venger d'un licenciement	Saboter l'activité de l'organisation	Moyen
Un prestataire	Offrir des services à l'organisme	Faible
Hacker	Rendre les services indisponibles, pirater les comptes mobiles money	Elevé
Développeur	Créer des solutions d'automatisation des tâches	Faible
Source de risque non humaine	**Les objectifs visés**	**La pertinence des menaces**
Virus informatique	Modifier le fonctionnement normal des systèmes	Moyen
Phénomène géologique	Détruire les locaux de l'entreprise	Moyen

Tableau 2:les sources de risques et les objectifs visés

VIII. L'écosystème et les chemins d'attaque

Pour ce fait nous allons déterminer les parties prenantes externe de l'écosystème de l'entreprise.

Catégories	Les parties prenantes
Client	Les agences de service mobile money
	La population
	Les détenteurs de cabine téléphonie
Prestataire	Les fournisseurs de la bande passante
	Prestataire informatique
Partenaire	Régulateur

Tableau 3: les parties prenantes

Ces différentes parties prenantes constituent en quelques sortes un chemin d'accès aux biens essentiels de l'entreprise c'est-à-dire ces différentes sources de risque passe par ces chemins pour atteindre ces valeurs.

Nous ainsi ce tableau ci-dessous

Source se risque	Objectif visés	Chemins d'attaque stratégique	La pertinence
Virus informatique	Modifier le fonctionnement normal des systèmes	Un virus modifie le fonctionnement des systèmes, en partant d'un prestataire informatique	Elevé
Concurrent	Voler les informations	Un concurrent vole les informations en créant un canal d'exfiltration de données : * Portant directement sur le système d'information * Passant par le prestataire informatique	Moyen
Hacker	Rendre les services indisponibles, pirater les comptes mobiles money	Un hacktiviste rend les services indisponibles, en provoquant un arrêt du fonctionnement des différents serveur du département technique et du business solutions analyste partant d'un prestataire informatique	Elevé

Tableau 4: les chemins d'attaque

IX. Les menaces reliées aux biens supports

Les menaces représentent les incidents ou les sinistres types qui peuvent affecter les biens supports.

- Gravité élevée
- Gravité moyen
- Gravité faible

Biens supports	Menaces	Menace sur les critères de sécurité
Système de base de données	Modification du logiciel	*Disponibilité *Intégrité *Confidentialité
	Détournement de l'usage prévu par le logiciel	*Disponibilité *Intégrité *Confidentialité
Poste de travail	Espionnage d'une machine	*Confidentialité
	Dépassement des limites de fonctionnement d'une machine	*Disponibilité
Serveur	Détournement de l'usage prévu par le serveur	*Disponibilité *Intégrité *Confidentialité
	Perte d'un serveur	*Disponibilité *Confidentialité
Les supports de transmission	Attaque du milieu sur un support de transmission informatique ou de téléphonie	*Disponibilité *Intégrité
	Saturation, modification, dégradation, disparition d'un support de transmission informatique ou de téléphonie	*Disponibilité

Tableau 5: les menaces

X. Mesure de sécurité

R1 : Disponibilité

R2 : Intégrité

R3 : Confidentialité

MESURE DE SECURITE	SENARIO DE RISQUE ASSOCIES	RESPONSABLE	FREINS ET DIFFICULTES DE MISE EN ŒUVRE	COUT / COMPLEXITE	ECHEANCE	STATUT
GOUVERNANCE						
Revoie et approuve la politique de sécurité de l'information	R1, R2, R3	DSI		+	2 mois	En cours
Contrôle l'efficacité de la mise en œuvre de la politique de sécurité de l'information	R1, R2, R3	Ingénier sécurité, DSI	Mesures cryptographiques	++	4 mois	Terminé
Fournir les ressources nécessaires à la sécurité de l'information	R2	Installateurs de réseaux		+	3 mois	Terminé
PROTECTION						
Contrôle d'accès aux réseaux, systèmes, serveurs, machines, applications, fichiers	R1, R3	Installateurs de réseaux		+	3 mois	En cours

Gestion des incidents liés à la sécurité de l'information	R1, R3	Chef projet technique	Gestion des vulnérabilités techniques	++	5 mois	A lancer
Protection contre les codes malveillant	R1, R2, R3	Ingénieurs sécurité		+++	3 mois	A lancer
DEFENSE						
Surveillance des programmes visant à maintenir à niveau la sensibilisation à la sécurité de L'information	R1, R2	Ingénieurs sécurité, DSI		+++	6 mois	En cours
RESILIENCE						
Gestion du plan de continuité de l'activité de sécurité	R1, R2, R3	Ingénieurs sécurité, DSI		+++	6 mois	En cours

Tableau 6: les mesures de sécurité

CONCLUSION

Le management du risque, notamment le suivi des risques, doit s'appuyer sur des **indicateurs de pilotage** pour assurer par exemple le maintien en condition de sécurité. Ces indicateurs permettent de vérifier l'efficacité des mesures prises et leur adaptation à l'état de la menace. Une fois ces indicateurs listés, définissez ou affinez le processus d'amélioration continue de la sécurité et la gouvernance afférente (organisation, rôles et responsabilités, comités associés). Il est recommandé de constituer un **comité de pilotage** se réunissant tous les six mois pour aborder cette montée en puissance ou tous les douze mois en rythme de croisière afin d'assurer un suivi des indicateurs, de l'avancement du PACS et de l'évolution des risques. La mise à jour de l'étude des risques se réalise dans le respect des cycles stratégique et opérationnel prévus. En cas d'événements importants susceptibles de remettre en cause la pertinence des scénarios (émergence d'une nouvelle menace, évolution significative de l'écosystème ou de l'objet de l'étude, etc.), ceux-ci feront l'objet d'une mise à jour au juste niveau.

TABLE DES MATIERES

BIBLIOGRAPHIE

https://fr.wikipedia.org/wiki/Gestion_des_risques (la date est : 01/07/2019 à 21h06)

https://fr.wikipedia.org/wiki/T%C3%A9l%C3%A9phonie_mobile_en_C%C3%B4te_d%27Ivoire (la date est : 02/07/2019 à 10h36)

https://www.irisa.fr/prive/Bernard.Cousin/Cours/messagerie.2P.pdf (la date est : 04/07/2019 à 14h28)

https://www.google.com/search?source=hp&ei=Z2QfXZ4qkr9S5L-4oA0&q=20170328_AMSN_Annexe+3_Base-de-connaissances-guide-methode-gestion-risques_v8_NP&oq=20170328_AMSN_Annexe+3_Base-de-connaissances-guide-methode-gestion-risques_v8_NP&gs_l=psy-ab.3...692.692..1605...0.0..0.279.536.2-2.....0....2j1..gws-wiz.....0.0HtDUGS8Ywo (la date est : 01/07/2019 à 21h06)