République de Côte d'Ivoire

Ministère de l'Economie Numérique et de la Poste

ESATIC
ECOLE SUPÉRIEURE AFRICAINE DES TIC

Année Académique : 2018-2019

Analyse de risques : cas d'une Assurance

Sécurité des systèmes d'informations

Enseignant: M. Mamadou NAON

Classe : Master 1 SITW

Réalisé par:

BOSSON Wilfried Mathieu

KONAN Kouadio Samuel

TRAORE Zéla Tahiré

SOMMAIRE

Introduction

Les compagnies d'assurance permettent à des individus ou des investisseurs d'éliminer certains risques. Les clients transfèrent donc leurs risques assurables à une compagnie d'assurance qui elle, en revanche, doit les gérer efficacement afin d'éviter des scénarios catastrophiques qui pourraient mettre en péril la situation financière de l'entreprise et par le fait même de maintenir sa profitabilité. De ce fait, ces compagnies tentent de bien quantifier le risque qu'ils assurent afin de déterminer la prime, qui accumulée avec toutes les primes des assurés, servira à compenser les indemnités qu'elle devra faire lorsque l'événement assuré se produira.

Cependant, dans le cadre de ses opérations, une des tâches les plus importantes d'une compagnie d'assurance est de gérer efficacement les risques auxquels elle s'expose en assurant des clients. Dès lors, il importe de s'interroger sur les risques susceptibles de menacer ces compagnies et si possible comment y remédier.

Pour répondre à cette préoccupation majeure, nous analyserons les risques suivant la méthode **Ebios Risk Manager** qui permettra d'apprécier les risques numériques et d'identifier les mesures de sécurité à mettre en œuvre pour les maitriser.

Suite à cette problématique, notre exposé se présentera sous les axes suivants :

Dans la première partie, il sera question de présenter une compagnie d'assurance de manière générale afin de ressortir les différentes missions qui lui sont assignées. Ensuite, nous analyserons les risques d'une compagnie d'assurance afin de déterminer les valeurs métiers et biens supports. Enfin, dans la troisième partie, nous présenterons des mesures de sécurité pour protéger cette compagnie contre les risques.

I- Description d'une société d'assurance

Une société d'assurance fournit une prestation lorsqu'un événement indépendant de la volonté d'un assuré survient. Cela peut concerner la santé, la vie, le travail, des biens ou encore des habitations, etc. Ainsi, les missions d'une société d'assurance sont de créer des produits d'assurance pour les assurés mais aussi d'en assurer la gestion et la vente finale. Un contrat d'assurance est signé entre la société d'assurance et l'assuré, décrivant les droits et obligations de chaque partie.

La prestation est le plus souvent financière et est destinée à un individu, une association ou une entreprise. Pour obtenir cette prestation, l'assuré doit verser une cotisation ou une prime tous les mois. Ce versement peut être fixe ou variable.

Types d'assurances

Il existe **deux grandes catégories** d'assurances : celles qui couvrent une personne physique et celles qui couvrent les biens. Mais, il est également possible de souscrire plusieurs assurances dans un même contrat. On parle alors de « multirisques ».

1- L'assurance de personnes

Une assurance de personnes a pour objet de couvrir les **risques relatifs aux individus** comme les accidents corporels, la maladie, le décès ou encore l'invalidité.
On distingue la prévoyance (garantie emprunteur, indemnités journalières, rente éducation…) et la santé laquelle est subdivisée en deux catégories bien distinctes : la garantie obligatoire (Sécurité sociale) et la garantie complémentaire (mutuelle, assureurs…).
L'assurance de personnes peut être souscrite soit à titre individuel soit à titre collectif. Certains contrats permettent la constitution et le versement d'une épargne sous forme de capital ou de rente. C'est notamment le cas d'une assurance vie.

2- L'assurance des dommages

L'assurance des dommages permet d'obtenir une **indemnisation en cas de sinistre**.
Elle regroupe à la fois la protection de **responsabilité** (responsabilité civile, responsabilité civile familiale ou responsabilité professionnelle) et celle de **biens** (dommages causés au véhicule, protection des biens meubles ou immeubles).

Par exemple, en cas d'accident de la route, elle garantit entre autres l'indemnisation des dommages subis par la voiture et s'avère donc nécessaire même si, dans la plupart des cas, elle n'est pas obligatoire. C'est notamment le cas de la prévoyance.

On distingue deux niveaux de garanties dommages : la garantie dommages collisions (permettant à un assuré de bénéficier d'une indemnisation en cas d'accident responsable avec la présence d'un tiers identifiable) et la garantie dommages tous accidents (permettant à un assuré de bénéficier d'une indemnisation en cas d'accident responsable même en l'absence de tiers).

Ainsi notre étude sera menée suivant un cas général des assurances.

II- Analyse des risques avec EBIOS RM

EBIOS Risk Manager est la méthode d'appréciation de traitement des risques numériques publiée par l'Agence nationale de la sécurité et des systèmes d'information (ANSSI) avec le soutien du Club EBIOS.

Cette méthode permet d'apprécier les risques numériques et d'identifier les mesures de sécurité à mettre en œuvre pour les maitriser. Elle permet aussi de valider le niveau de risque acceptable et de s'inscrire à plus long terme dans une démarche d'amélioration continue. Enfin, cette méthode permet de faire émerger les ressources et arguments utiles à la communication et à la prise de décision au sein de l'organisation et vis-à-vis de ses partenaires.

1- Identification des valeurs métiers

Les valeurs métiers représentent le patrimoine informationnel qu'une source de risque aurait intérêt à attaquer pour atteindre ses objectifs. Dans notre cas d'assurance, nous nous limiterons à 4 valeurs métiers.

- **Police d'assurance :** c'est un document contractuel qui fixe les conditions d'engagements de l'assureur à l'égard de l'assuré ou d'un groupe d'assurés. Elle se compose des conditions générales propres à la compagnie d'assurance pour un risque ou un ensemble de risques considéré et est complétée par les conditions particulières qui se rapportent à la situation de l'assuré.

- **Remboursement** : Il s'agit du processus grâce auquel les assurés perçoivent ce qui doit leur revenir après qu'ils aient été victime d'un sinistre ou d'un problème de santé. Il faudra un rendez-vous afin de régler le remboursement

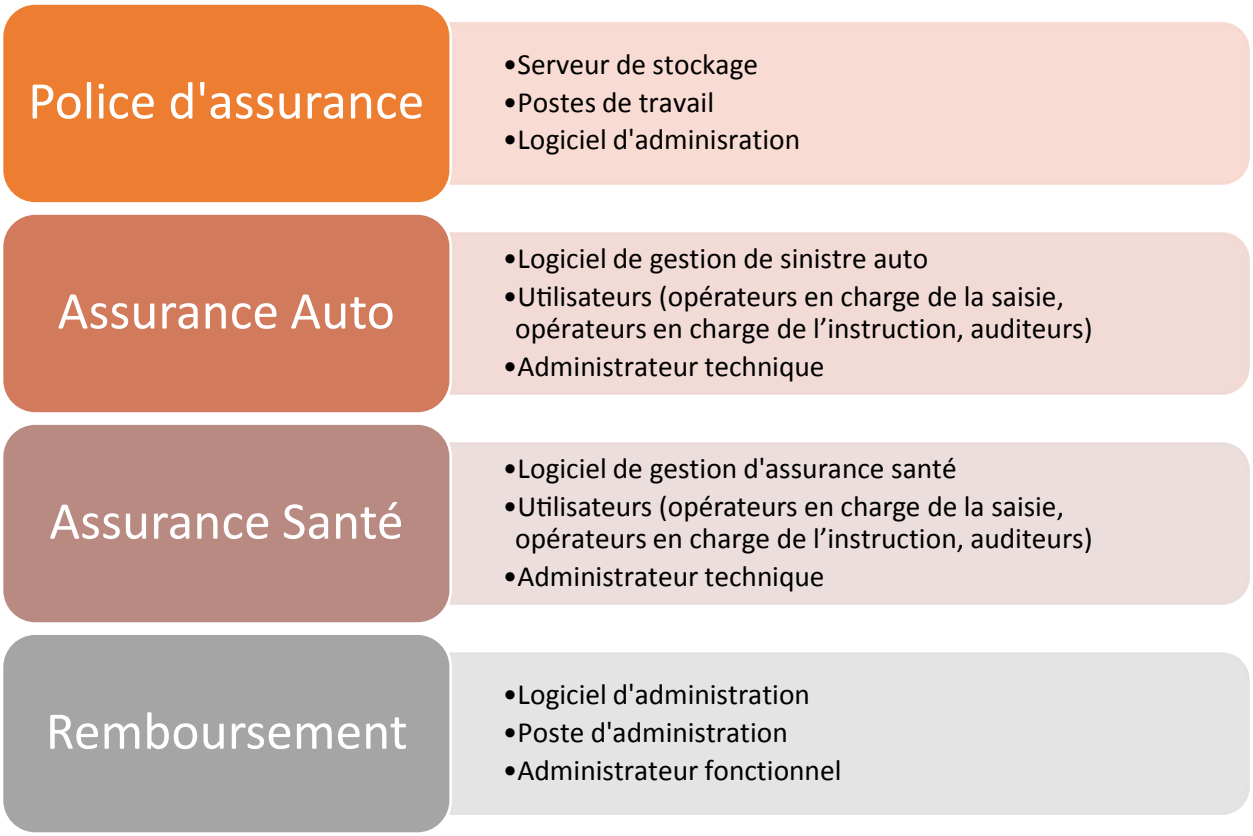
- **Assurance santé** : Processus grâce auquel les assurés reçoivent des compensations sur leur consultation médicale et sur leurs ordonnances médicales. Il est question ici pour les assurés de se rendre dans centres de santés prenant notre assurance en charge. Ils pourront de ce fait payer le pourcentage qu'il leur ait dû d'après la police d'assurance.

- **Assurance auto** : il s'agit ici de s'occuper de tout ce qui concerne les sinistres dont peuvent être sujet un automobile. L'assuré devra envoyer l'ensemble des preuves prouvant que son véhicule a été victime de sinistre dans l'optique que l'assureur puisse couvrir la réparation.

- **Assurance habitation** : il s'agit ici de s'occuper de tout ce qui concerne les sinistres dont peuvent être sujet son habitation. L'assuré devra envoyer l'ensemble des preuves prouvant que son véhicule a été victime de sinistre dans l'optique que l'assureur puisse couvrir la réparation.

2- Identification des biens supports

Les biens supports sont relatifs à chaque valeur métier. Il s'agit des éléments du système d'information sur lesquels les valeurs métiers reposent. Pour cela, on s'appuie sur la cartographie du système d'information de l'organisme.



3- Identification des sources de risque

Cette étape vise à répondre à la question suivante : qui ou quoi pourrait porter atteinte aux missions et valeurs métier identifies dans l'atelier 1, et dans quels buts ?

Types de sources de menaces	Retenu ou non	Exemple
Source humaine interne, malveillante, avec de faibles capacités	Oui	Employé malveillant
Source humaine interne, malveillante, avec des capacités importantes	Oui	
Source humaine interne, malveillante, avec des capacités illimitées	Oui	Administrateur malveillant
Source humaine externe, malveillante, avec de faibles capacités	Non	
Source humaine externe, malveillante, avec des capacités importantes	Oui	Pirate, Concurrent
Source humaine externe, malveillante, avec des capacités illimitées	Non	
Source humaine interne, sans intention de nuire, avec de faibles capacités	Oui	Employé peu sérieux
Source humaine interne, sans intention de nuire, avec des capacités importantes	Oui	
Source humaine interne, sans intention de nuire, avec des capacités illimitées	Oui	Administrateur peu sérieux
Source humaine externe, sans intention de nuire, avec de faibles capacités	Non	
Source humaine externe, sans intention de nuire, avec des capacités importantes	Non	

Source humaine externe, sans intention de nuire, avec des capacités illimitées	Non	
Code malveillant d'origine inconnue	Non	
Phénomène naturel	Oui	Panne de matériel
Catastrophe naturelle ou sanitaire	Oui	Inondation, Tempête, Tremblement de terre
Activité animale	Non	
Évènement interne	Oui	Faille dans l'application
Évènement externe	Oui	Mauvaise gestion du prestataire, Décision de justice

4- Identification des scénarios stratégiques

D'abord définissons une échelle de niveaux de gravité :

1 Négligeable	2 Limitée	3 Importante	4 Critique
La société surmontera les impacts sans aucune difficulté	La société surmontera les impacts malgré quelques difficultés	La société surmontera les impacts avec de sérieuses difficultés	La société surmontera les impacts avec de très sérieuses difficultés et sur une très longue période

Les scénarios stratégiques sont un ensemble d'évènement ou encore d'attaque pouvant utiliser une source de risque pour atteindre son objectif.

Source de risques	Objectifs visés	Chemins d'attaque stratégiques	Gravité
Employé	Modifier ou supprimer des données de déclarations de sinistre des assurés en vue d'avoir des pots de vins ou vengeance si l'employé est malveillant ou par mégarde s'il est peu sérieux	Deux chemins possibles : 1. S'attaquer au serveur de stockage des polices d'assurance, en usant de ses accès afin de modifier les données du serveur.	3 Importante

		2. s'attaquer au logiciel d'assurance afin de modifier leur état d'assurance	
Administrateur	Supprimer, modifier les données de déclarations de sinistre des clients ou/et des autres employés afin de soutirer de l'argent aux clients, faire porter le chapeau de ses agissements à un autre employé ou couvrir un employé malveillant	Effectuer grâce à ses propres accès. L'admin va altérer les informations dans les serveurs de stockages, les logiciels d'assurance et de remboursement en utilisant ses accès puis supprimer les logs ou en utilisant l'usurpation d'identité	4 Critique
Concurrent	Voler des informations en espionnant les données de déclaration de sinistre contenues dans les différents serveurs de la société	Deux chemins possibles : - En créant un canal d'exfiltration des données de déclarations de sinistre - Portant sur le système d'information des politiques d'assurances (serveurs de stockages) - Base de données des logiciels de gestion de sinistre	3 Importante

Pirate	- Divulguer des données de déclaration de sinsitre	Trois chemins possibles : En se créant un accès aux données de déclarations de sinistre via : - le système d'information des politiques d'assurances (serveurs de stockages) - Base de données des logiciels de gestion de sinistre (Attaque de type Man in The Middle)	4 Critique
	- Altérer les données de déclaration de sinistre		3 Importante
	- Rendre indisponible les données de déclaration de sinistre	Attaque DDoS/DoS sur les logiciels et les serveurs	2 Limitée

III- Mesure de sécurité contre les risques

Maintenant déterminons les mesures de sécurité à utiliser face aux risques rencontrés par rapport au scénarios stratégiques énumérés.

N	Thème ISO 27002	Description	Risques solutionnés
1	**10.5.1 Sauvegarde des informations** Et **10.7 Manipulation des supports** Et **11.2 Gestion de L'accès Utilisateur**	Dans les situations où la confidentialité a une importance, il convient de protéger les sauvegardes en les chiffrant. Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de biens et l'interruption des activités de l'organisme.	Vol d'informations

		Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations).	
2	**10.7 Manipulation des supports** Et **11.2 Gestion de L'accès Utilisateur**	Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de biens et l'interruption des activités de l'organisme. Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations).	Divulgation d'informations
3	**11.4 Contrôle d'accès au réseau**	Empêcher les accès non autorisés aux services disponibles sur le réseau.	Attaque DoS/ DDoS
4	**10.7 Manipulation des supports** Et **11.2 Gestion de L'accès Utilisateur**	Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de biens et l'interruption des activités de l'organisme. Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations).	Altération d'informations
5	**10.10 Surveillance**	Protection des équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés. Analyser les journaux à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte.	Attaque DoS/DDoS, altération de l'information, divulgation d'informations

Conclusion

Au terme de notre étude il convient de retenir dans un premier temps que l'ensemble des valeurs métiers des assurances est relié directement à des données des clients (souvent à caractère personnelles). Ensuite il faut ajouter à ce point le fait que l'ensembles des risques liés aux activités des sociétés d'assurance concernent la divulgation, le vol, l'altération des données et le fait que l'accès aux données constitue un service dont la disponibilité est menacée par certaines attaques de dénis de service.

Ainsi pour assurer la sécurité du système d'information il faut se concentrer sur les données transitant sur l'ensemble du système d'information. Il faut donc appliquer les mesures de sécurité énoncée plus haut.

Table des matières