Énoncé détaillé du devoir

Objectif

Ce travail aura comme objectif de mettre en pratique les notions vues en classe concernant la modélisation de menaces selon la méthode STRIDE.

Étapes de réalisation

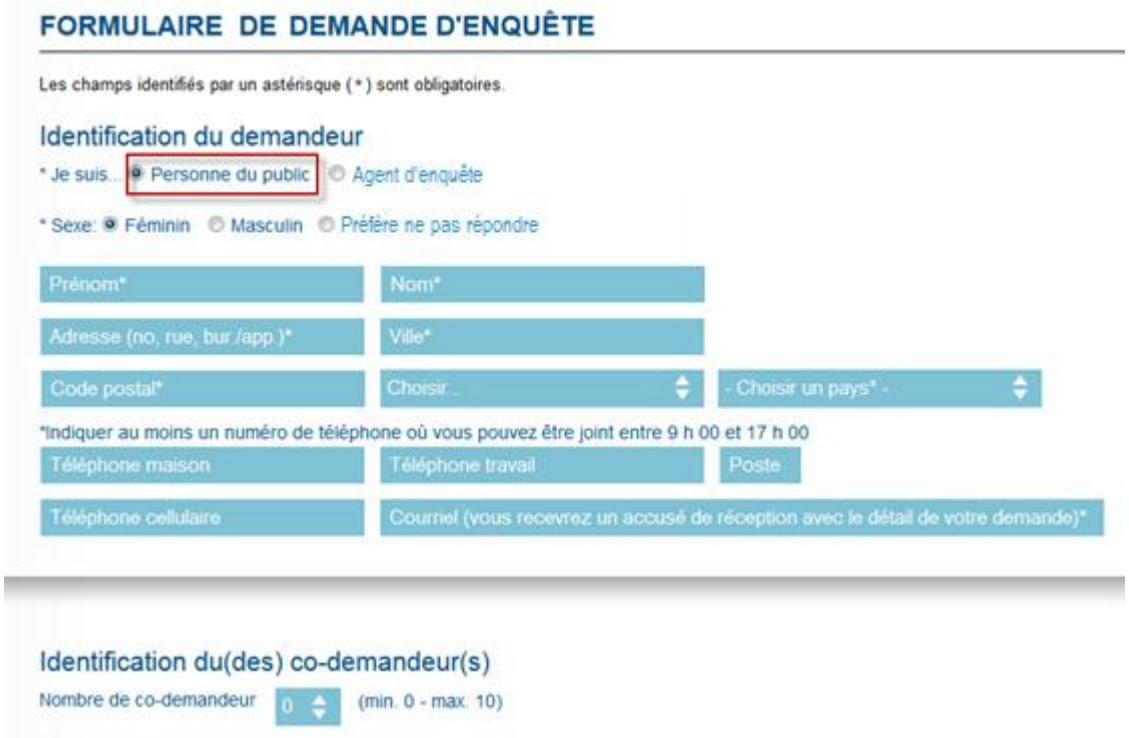
Voici un bref résumé de la problématique.

Une entreprise dans le domaine des assurances automobile et habitation a rendu disponible un site web pour ses clients dans le but de leur permettre d'ouvrir un dossier à la suite d'un incident.

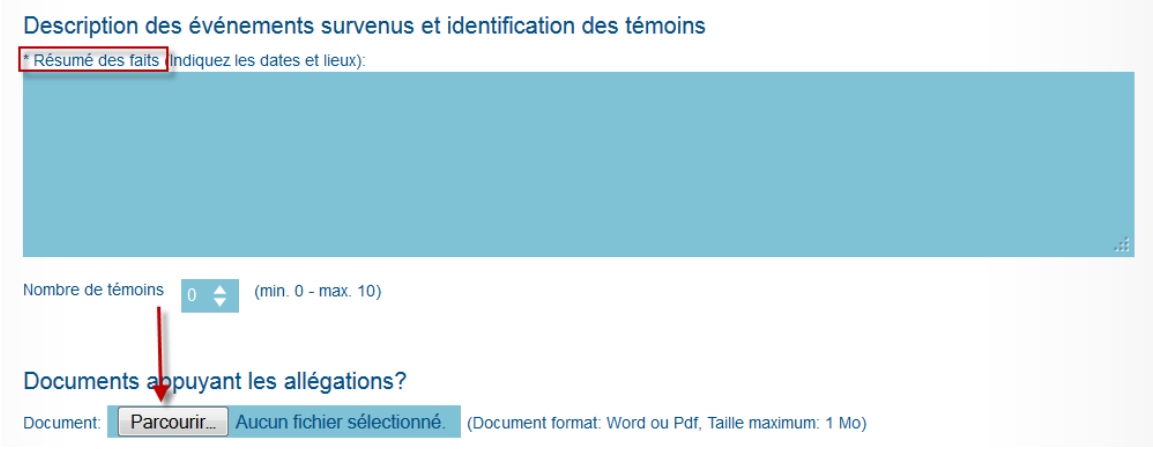
Le site permet à un client détenteur d'une police d'assurance de s'inscrire, de remplir le formulaire et de décrire l'incident afin de procéder au traitement du dossier.

Les grandes lignes :

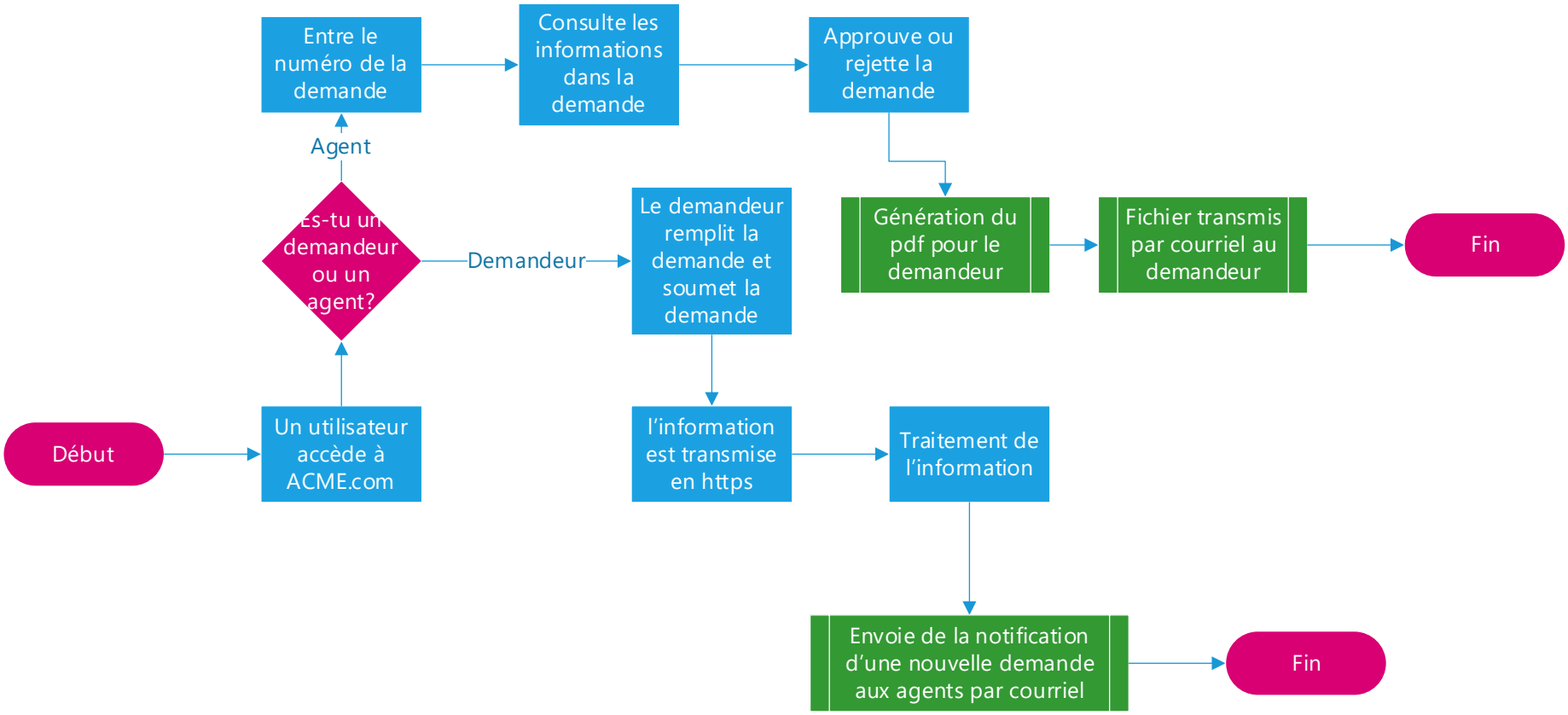
1. Le site ACME.com permet aux détenteurs d'une police d'assurance d'ouvrir une demande ainsi qu'aux agents d'enquête pour les sinistres de consulter un dossier.



2. L'assuré peut par la suite joindre des fichiers pour appuyer la demande.



3. L'assuré transmet ensuite le formulaire complété via un canal https à la compagnie d'assurance.
4. On peut considérer que l'entreprise stocke l'information reçue dans des serveurs de BD et utilise une architecture de type 3 tiers.
5. La demande une fois complétée est envoyée à l'agent
6. Après un certain délai, habituellement d'au plus trois journées ouvrables, l'assuré reçoit par courriel, un fichier PDF contenant un statut de sa demande.
7. Ce fichier PDF est en pièce jointe et le courriel contient des informations confidentielles. Il contient les informations suivantes :
    a. Un suivi de la demande
    b. Nom, prénom, adresse, numéro de police, numéro de permis de conduire, date de l'incident, l'historique des réclamations, etc.
8. Un agent d'enquête peut aussi voir le statut de la demande à partir du même site.
9. Voici un aperçu du processus :



Livrables

Un rapport contenant les sections suivantes :
1. État de la situation : introduction, hypothèses, etc.
2. Un DFD (Data flow diagram)
3. Vecteurs d'attaque possibles (STRIDE)
4. Niveau de risque
5. Pistes de solutions et recommandations proposées

NB :

1. Un rapport individuel (ou par groupe de max 3).
2. Le rapport en format WORD ou pdf

Réponses détaillées

Table des matières

Introduction :

La réalisation des différentes tâches au sein d'une organisation requiert généralement l'exploitation de données diverses à l'intérieur d'un système d'information informatisé.

Or, il se trouve que ce système est le plus souvent exposé à des défaillances techniques (panne), des intrusions des logiciels malveillants ou tout simplement des défauts de manipulation. Les données collectées, stockées et échangées au sein du réseau d'entreprise sont pourtant confidentielles. Ce qui impose donc aux entreprises de garantir un contrôle de leur infrastructure.

Un réseau d'entreprise fait intervenir plusieurs composants qui assurent la communication et l'échange de données entre les différents acteurs à l'interne comme à l'externe. Sécuriser ce réseau revient donc à optimiser l'état et le fonctionnement de ses composants afin de se prémunir des attaques informatiques et des incidents liés à un mauvais usage dans le but de protéger les données.

ACME étant une entreprise exerçant dans le domaine des assurances automobile et habitation, elle est tenue de respecter les lois des pays où elle exerce ces activités à savoir la loi 25 pour Québec (Loi sur la protection des renseignements personnels LQ 2021, c 25) et rendre un service disponible 24h/24 tous les jours de l'année.

En considérant que l'entreprise stocke l'information reçue dans des serveurs de BD et utilise une architecture de type 3 tiers, cette architecture doit respecter les trois notions en matière de sécurité à savoir le DIC.

Disponibilité : l'accès aux ressources du système d'information doit être permanent et sans faille durant les plages d'utilisation prévues. Les services et ressources sont accessibles rapidement et régulièrement.

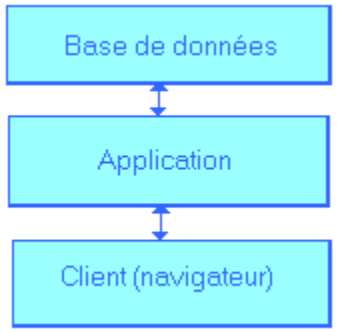
Intégrité : les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante.

Confidentialité : seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

D'autres aspects peuvent aussi être considérés comme des objectifs de la sécurité des systèmes d'information, tels que : la traçabilité (ou « preuve »), la non-répudiation et l'authentification.

Pour répondre à ces exigences, notre rapport comportera une mise en contexte avec de hypothèses, nous ressortirons un Data flow Diagram, identifier, identifierons les vecteurs d'attaques possibles en nous basant sur la modélisation de menaces selon la méthode STRIDE pour enfin évaluer le niveau de risque et proposer des solutions et recommandations .

Voir (nbre points) de chaque question dans la Grille de correction en annexe B

Section 1		
Questions :	Réponses et copies écrans des différentes étapes	
Question 1 : État de la situation : Hypothèses ou autres constats pertinents, etc.	Mise en contexte ACME exerce dans le domaine des assurances automobile et habitation, elle utiles le site web ACME.com pour échanger les informations des clients, architecture SI est du type trois-tiers. Les infrastructures de ACME sont essentiellement (des serveurs de BD, d'applications, des équipements de réseautique,) et des employés. Utilisation de site Web (un canal https) pour accès clients et enquêteurs Utilisation de fichier PDF ACME échange les données en internes et en externes (clients et agent d'enquêtes) Délai de traitement trois jours maximum Généralité : Présentation de l'architecture trois-tiers L'architecture de ACME est une architecture trois tiers, elle est divisée en trois niveaux : Niveau de présentation, Niveau de l'application ; Niveau de base de données. Ce modèle divise l'application en trois couches logicielles :  Base de données : les données à stocker définitivement. Application (ou middleware) : le traitement logique et applicatif des données. Client (navigateur) : l'affichage et la présentation des données qui constitue le dialogue avec le client. Source : https://fr.wikipedia.org/wiki/Architecture_trois_tiers Chaque couche communique avec les couches voisines immédiates. Dans ce modèle, on interdit qu'une couche communique avec une couche plus basse que le niveau inférieur immédiat et plus haut que le niveau supérieur immédiat. Les couches communiquent entre elles via un modèle d'échange et proposent des ensembles de services. Chaque niveau a un rôle bien défini et évolue sans imposer des changements aux autres couches.	

L’architecture 3 niveaux permet :

L'hétérogénéité des plates-formes (Windows, Linux, etc. ...) ;

D’améliorer la sécurité des données, en supprimant le lien entre le client et les bases de données ;

Une meilleure répartition de la charge entre différents serveurs d'applications.

Définitions des trois niveaux

Premier niveau – Présentation

C’est la partie interactive et visible de l'application pour les clients. Cette interface est représentée en HTML pour être utilisée par un navigateur web (Internet Explorer, Edge ou Chrome).

Ce niveau envoie les requêtes du client à destination au niveau de l’application, et en retour lui présente les informations renvoyées par l’application.

Deuxième niveau – Application

C’est la partie fonctionnelle de l'application, celle qui implémente la logique, elle décrit les opérations que l'application effectue sur les données en fonction des requêtes des clients envoyées de la couche de présentation.

Elle offre des services applicatifs à la couche de présentation. Pour offrir ces services, elle utilise les données du système de base de données, accessibles via le niveau inférieur. En retour, elle renvoie à la couche de présentation les résultats des données traitées.

Cette couche inclue le middleware open source utilise pour les données clients

Troisième niveau – Base de données

C’est la partie qui gère l'accès aux données de la base de données. Ces données sont transparentes et le niveau de l’application accède à ces données de manière uniforme (couplage faible).

Cette couche inclut les données des détenteurs des donnes des clients et agents enquêteurs dans une base de données dédiée et une autre base de données qui inclue les sauvegardes.

Enjeux :

ACME étant une société d’assurance qui traite les demandes de ces clients via son site internet ACME.com, elle doit respecter certaines exigences tel que :

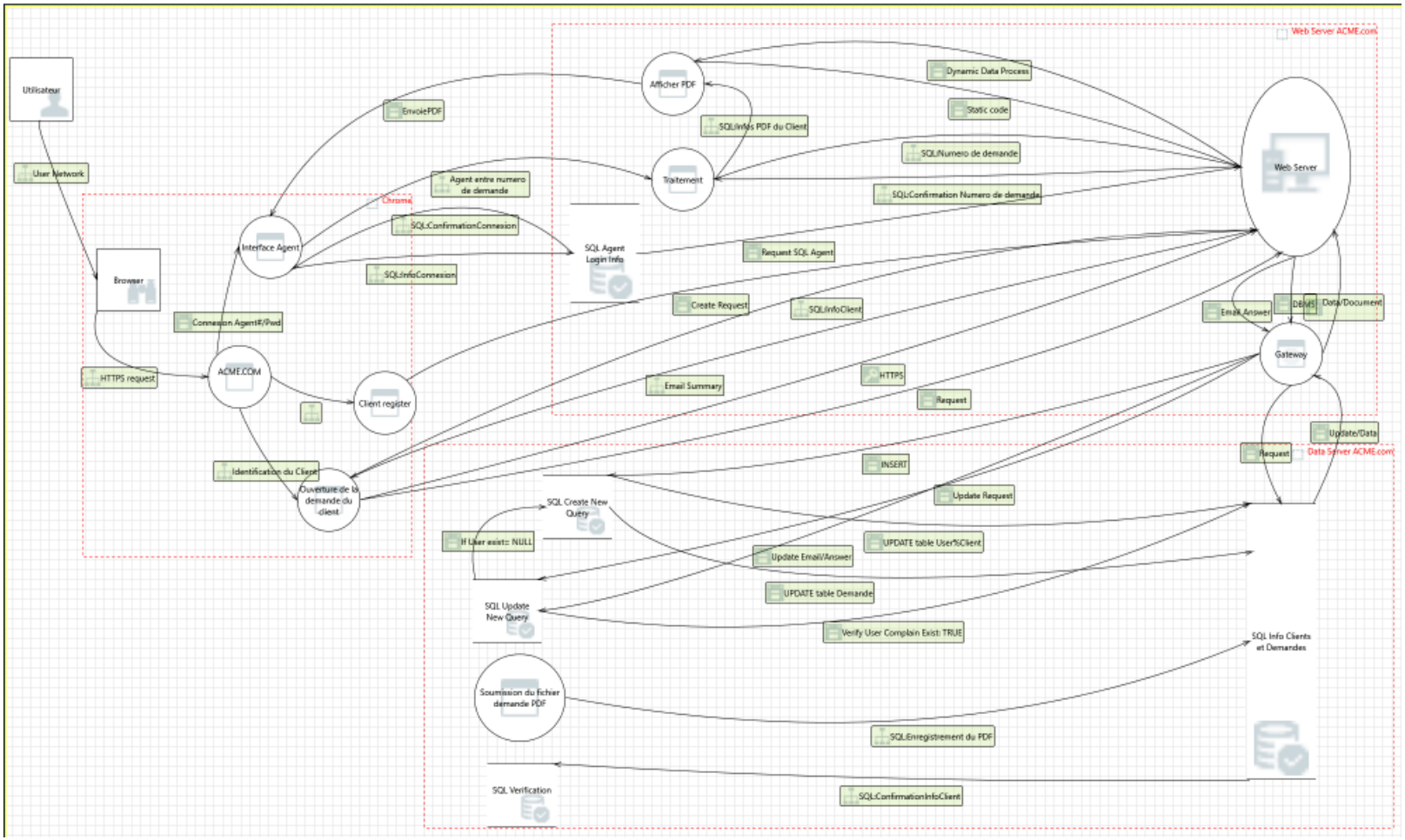
- Maintenir le service disponible 24/7, tous les jours de l’année

-La protection des données : ACME est responsable de protection des données personnelles de ces clients, de ces employés, des agences partenaires d’affaires, de son organisation.

-Assurer la protection de ces infrastructures physiques, matérielles et applicatifs, en effet ACME se doit d’assurer la sécurité des applications de son système informatique, la sécurité physique de ses infrastructures

-Veiller au respect des contrats clients et fournisseurs

	- Des exigences à respecter par les parties prenantes (employés, clients internes et externes, entreprise d'enquête), respect des délais de traitement, suivi et payement des réclamations -Rester crédible, et garder son image de marque. **Hypothèses** ACME peut faire face à divers scénarios dont les suivants : - Des vols ou fuites de données (en interne comme à l'externe) - Des indisponibilités du service suite à une panne (logicielle ou physique), ou une cyberattaque (déni de service, hameçonnage…) -Des usurpations d'identités des clients, des fraudes -Des vulnérabilités applicatifs, du a des patches non appliqués -Des infection par un virus -Des systèmes et application désuètes -Des risque de pertes financières et dégradation de l'image de l'entreprise NB : Certaines hypothèses apparaitront dans Le STRIDE, nous nous en servirons pour évaluer les risques et trouver des pistes de solution
Question 2 : **Un DFD (Data flow diagram)**	**Le data flow diagramme doit répondre à quelques fonctions dont :** 1.Connexion au système, accès via internet avec un lien https 2.Creation de compte (Nom, not de passe, plage de naissance…) 3. ouverture de session (identifiant, mot de passe, numéro de police…) 4.Type de Requêtes (Soumission, réclamation, suivi) 5.Enregistrements / modification de données 6.Consultation de la base de données, Informations clients, (numéro de police, type de demande, historiques, contrat…) 7.Accuser de réception (courriel et numéro de la demande) 8. Fermeture de session En tenant compte de l'architecture trois-tiers, nous pouvons en ressortir le Data flow diagram (DFD) suivant



Data Flow Diagram de ACME

Question 3 :
Vecteurs d'attaque possibles (STRIDE)

Spoofing

L'usurpation d'identité le fait qu'une machine ou un humain essaye de se faire passer pour une autre machine ou personne dans le but de les induire en erreur et gagner leur confiance pour ensuite leur voler des données sensibles ou utiliser des ressources informatiques dans le but de mener d'autres attaques. (Softwarelab.org, 2022)

Dans notre cas si on se fie à la méthode S.T.R.I.D.E, les risques à considérer sont :

- Qu'une machine\personne se fasse passer pour un agent d'assurance ou un détenteur d'assurance.
- Le DNS du site ACME.com pourrait être détourné vers un site frauduleux (faux formulaires)
- Usurpation de l'adresse IP, usurpation d'un serveur
- Détournement de courriel
- Usurpation du canal HTTPS
- Cheval de Troie dans le fichier PDF (peut cacher des maliciels dans le but de mener d'autres attaques)
- Les cybercriminels peuvent accéder au réseau local de l'entreprise en envoyant de fausses données ARP (Address Resolution Protocol). En associant leur adresse MAC à une adresse IP légitime, les pirates peuvent ainsi subtiliser des données sensibles.
- Des accès non autorisés peuvent être accordés à un attaquant qui se fait passer pour un client d'ACME

Tempering

La falsification de données est le fait d'accéder et de modifier voire même supprimer des ressources telles, l'information sensible, le code source sans en avoir l'autorisation (Owasp, 2022) dans notre cas il peut s'agir de :

- Modification des données clients (date de naissance, nom, adresse, NAS). Cela peut être fait par un attaquant n'ayant pas de lien direct avec ACME ou un client ayant une police d'assurance et qui chercherait à modifier dans son dossier de l'information afin d'en tirer avantage (modification de la prime à recevoir ou des biens assurés)
- Modification du formulaire de réclamation et des fichiers PDF
- Altération de la base de données du site.
- Injection de données dans la base de données SQL du site.
- Dommage physique serveur

- Un utilisateur malveillant envoie du code (script) exécutable (Menoth, 2018)
- Redirection de l'URL du site,
- Les demandes peuvent être interceptées par un attaquant et selon le type de données elles peuvent être utilisées pour attaquer d'autres parties du système ou simplement divulguer l'information menant à des violations de conformité.
- Des scriptes malveillants (XSS) pourraient être introduits par un attaquant.
- Un attaquant peut prendre le contrôle d'une passerelle dans le réseau.

Répudiation

La répudiation est le fait pour une personne de prétendre ne pas avoir fait une action. La personne peut prétendre ne pas avoir reçu ou envoyé certaines informations au cours d'une transaction ou communication à travers un réseau (Menoth, 2018). Dans notre cas il peut s'agir de :

- Un détenteur peut dire ne jamais avoir soumis de réclamation.
- Un agent peut dire ne jamais avoir consulté un formulaire, donc nier avoir accédé aux informations d'une personne.
- Un détenteur peut dire ne jamais avoir reçu le formulaire de confirmation PDF ou le courriel de confirmation.
- Un détenteur peut nier un sinistre dans le passé.
- Un agent peut dire ne jamais avoir reçu le formulaire du détenteur.
- Un agent pourrait faire croire qu'il a traité une réclamation alors que ça n'a jamais été fait.
- Un attaquant pourrait tenter de modifier les logs pour effacer ses traces.
- Un attaquant peut utiliser un faux courriel dans le but d'intercepter de l'information et faire en sorte qu'on ne puisse jamais remonter à lui.

Information disclosure

La divulgation d'information peut arriver de manière intentionnelle ou non intentionnelle, elle survient en général quand les processus de cryptages ou les mis par jours n'ont pas été suivi laissant ainsi des failles pouvant être exploitées pour accéder à de l'information sensible. Dans le cas de la divulgation d'information, le pirate accède à un système d'information ou une plateforme applicative spécifique dans le but d'y subtiliser de l'information sensible. Telles que la distribution de logiciels, les numéros de version et les niveaux de module de correction. Les informations collectées peuvent également comporter l'emplacement des fichiers de sauvegarde ou des fichiers temporaires (Portswiger,2022)

- Un détenteur/pirate pourrait tenter d'accéder au compte d'un autre détenteur et ainsi accéder à ses informations tels Nom, prénom, adresse, numéro de police, numéro de permis de conduire, date de l'incident, l'historique des réclamations, etc.
- Un pirate pourrait accéder à la base de données du site d'ACME
- Accès à de l'information non cryptée.
- Attaque de type man in the middle pour intercepter le formulaire de réclamation ou le fichier PDF du statut de la demande.
- Un accès non autorisé à la base de données des mots de passe utilisateurs
- Une erreur involontaire de la configuration pourrait exposer de l'information sensible aux utilisateurs du site
- Divulgation du code source et aux sauvegardes
- Un attaquant pourrait tenter d'intercepter les communications des clients et des agents.

Denial of service

Le déni de service survient lorsqu'une plateforme (site internet, application, serveur, un protocole, etc.) n'arrive plus à répondre ou en d'autres mots a effectué la tâche pour laquelle elle a été programmée, car elle est surchargée de requêtes ce qui interrompre ou perturber un service. Dans le cas de l'entreprise ACME il se peut que :

- Le site tombe en panne à la suite des requêtes intensives d'ordinateur zombie contrôlé par un pirate informatique. Ce qui rendra le site accessible pour les clients et les agents.
- Un sinistre (catastrophe naturelle, accident, panne de courant) pourrait survenir et affecter les serveurs du site.
- Perturbation de la configuration du réseau de l'entreprise par un pirate (ARP poisoning).
- Un pirate pourrait empêcher un client de communiquer avec un agent en redirigeant ses messages (ICMO redirect).
- Un administrateur pourrait interrompre le service en modifiant la configuration du système ou les paramètres (Houes,2018)
- Panne ou ralentissement du serveur web empêchant les clients d'accéder au site.
- Si un attaquant peut accéder aux ressources limitées telle la mémoire, le stockage du système de fichiers, les entrées du pool de connexion, les bases de données ou le processeur alors l'attaquant pourrait provoquer un déni de service qui consomme toutes les ressources disponibles. (Cwe,2022)

Elevation of privilege

L'élévation de privilège c'est lorsqu'une personne à essayer d'autorisation plus élevée que ce qui lui est normalement accordé, et ce dans le but d'accéder à de l'information sensible ou à modifier les paramètres d'un système (Geekflare,2022) dans le cas de l'entreprise ACME il se peut que :

- Un agent malveillant tente de modifier ses autorisations dans le but des privilèges d'administrateur du serveur du site web d'ACME

	➢ Un pirate pourrait après s'être authentifié comme étant quelqu'un de légitime à l'entreprise modifier ses autorisations dans le but d'accéder à de l'information sensible. ➢ Exploitation de comptes avec un bas niveau de sécurité ➢ Un client pourrait exploiter des failles et tenter d'élever ses privilèges en faisant usage d'ingénieries sociales. ➢ Un attaquant peut transmettre des données dans afin de modifier le flux d'exécution du programme. ➢ Modification du flux d'exécution des programmes par un attaquant. ➢ Un mauvais usage des mots de passe pourrait permettre à une personne mal intentionnée d'accéder à un compte à haut privilège. ➢ Accumulation des privilèges par un administrateur.
Question 4 : **Niveau de risque**	L'analyse de risque nous permet d'évaluer les impacts que peuvent avoir un système, une application, des menaces, l'environnement (loi, exigence…) sur les activités d'une entreprise ou organisation. Ces risques peuvent être évaluer en tenant compte de plusieurs facteurs, l'environnement, les pertes financières, les menaces, les engagements de service et la criticité des équipements et applicatifs Mais cela se fait aussi en tenant compte au type de solution choisit par l'entreprise pour livrer le service à ces clients. L'entreprise peut choisir l'impartition de service dans ce cas les équipements sont hébergés sur le cloud et la responsabilité des applications et systèmes sont confiés à un fournisseur de service qui est garant de la qualité du service fourni et l'entreprise veille au respect du contrat qui le lie à son fournisseur, le SLA (Service Level Agreement est plus suivi ici pour suivre les pannes). Et l'autre approche ou l'entreprise est responsable de ses infrastructures et applications dans ce cas l'entreprise a l'entière responsabilité sur ces services donc l'analyse de risque ici tiendra compte des systèmes et applications qui sont sous la responsabilité direct de l'entreprise. Dans les deux cas les menaces au niveau du service restent les mêmes, car pour le client bien de choses restent transparentes, il ne demande qu'un service fiable, mais l'approche de l'entreprise en matière de risque reste différente. ACME, étant une société d'assurance les conséquences directes de ces impacts seront ressentis sur le bénéfice, l'image (l'opinion de se font les gens) et la satisfaction de la clientèle. Nous évaluerons les risques en tenant compte de quatre niveaux de sévérités à savoir (Critique, majeur, moyen et mineur), ces sévérités correspondront à des scores mesurés en fonction de la Disponibilité, l'intégrité et la confidentialité (DIC) qui auront une conséquence directe sur le service rendu aux clients internes et externes.

Risques lies aux menaces

Menaces					
	Disponibilité	Intégrité	Confidentialité	Score	Commentaires
Authentification		3	5	8 (critique)	Faille cause l'accès au compte des clients, donc modification des donnes, fausses déclarations, etc…
Deni de service	5	1	1	7 (Critique)	Pas de service possible
Usurpation d'identité		3	5	7 (Critique)	Difficulté ou pas de service, image et finance
Fuites de données		4	5	9 (critique)	Image de ACME, risque de poursuite par ces clients, perte financière
Répudiation		1	1	2(Mineur)	Peut être fait par des clients , mais ACME doit garder la traçabilité de logs, les clients n'y ont pas accès
Elévations de privilèges		5	3	8 (Critique)	Peut être fait par un employé ou lors d'une cyberattaque pour modification de données, injecter des codes ou virus ou rendre le système indisponible
Attaque DNS et écoute	4	3	1	8 (Critique)	Peut être fait par des cyberattaquants pour détourner le site vers un autre lien ou rendre le service indisponible
Attaque de virus	4	3		7(Critique)	Peut causer des pannes, lenteur, indisponibilité de service
Hameçonnages	2	2	2	6 (Majeur)	Un employé ou un client peut en être victime par voie de mail

Risques liés aux Systèmes et Applications

Actifs	Disponibilité	Intégrité	Confidentialité	Score	Commentaires

Serveur BD	5	5	5	15 (Critique)	Pas de service possible (pas d'accès aux données)
Serveur Applicatif	5	4	4	13 (Major)	Difficulté ou pas de service, image et finance
Serveur Web	5	4	4	13 (Major)	Difficulté ou pas de service, image et finance
Adobe	3	3	3	9 (moyen)	Difficulté de service, image
Java	4	3	3	10(Moyen)	Difficulté de service image
Internet	5	1	1	7 (mineur)	Ne dépend pas de ACME
Compte Client	5	2	3	10 (Moyen)	Responsabilité partagée
Compte employé	5	4	4	13 (Moyen)	Responsabilité ACEM
Compte agence	5	3	3	11(Moyen)	Responsabilité partagée

Les risques liés aux menaces, impactent plus ou moins une partie du service mais pas le tous en même temps sauf le déni de service qui peut causer l'indisponibilité complète du service, les clients auront un accès sur le service, mais la fiabilité du service rendu restera à désirer d'où une dégradation de l'image de l'entreprise donc des pertes financières suivront

Au niveau des infrastructures SI (serveur et applications ont de niveaux de risque très élevés car ils sont au centre des activités de ACME.

Ils auront donc un impact considérable sur le chiffre d'affaires, l'image et le respect des engagements, leur vulnérabilité n'est pas tolérable, car la protection des données clients en dépend. Il faut aussi accorder une grande importance a la protection physique ces infrastructures.

Le délai de livraison de service étant de trois jours, ACME aura une marge de manœuvre en cas d'indisponibilité d'une application, mais cela aura des impacts sur la qualité du service (disponibilité) rendu donc agira sur sa réputation de ACME ce qui aura une conséquence directe sur la fidélisation de sa clientèle.

Les accès (Comptes /clients/ et employés) : ACME a pour responsabilité première de fournir les accès aux personnes qui ont droits et de protéger leur comptes et avoir une traçabilité sur les comptes, mais l'utilisateur est aussi responsable de son compte (protection de son mot de passe et code utilisateur), ACME ne peut bloquer l'accès au compte qu'en cas de tentatives frauduleuses détectées (des échec d'authentifications) ou a la demande du clients bien sur après une authentification de se dernier. Donc comme on peut le constater la responsabilité est partager entre ACME et les clients en ce qui concerne les accès aux comptes.

	Les données étant la ressource la plus sensible que gère ACME pour mener à bien ces activités, elles doivent être disponible, confidentielles, intègres et traçables, elles ont donc un niveau de risque critique, comme elles sont gérées par les plates formes serveurs applications et comptes leur niveau de risque influent directement sur les donnes et leur accès. Les risques ne peuvent pas être tous éliminer, mais les bonnes pratiques permettent de les atténuer.
Question 5 : **Pistes de solutions et recommandations proposées**	**Pistes de solutions** ACME met à la disposition de ces clients une plateforme de service, cette plateforme doit être sécuritaire et disponible, pour respecter ces engagements, nous pouvons préconiser les pistes de solutions suivantes : -Authentification des usagers : Avant tout accès au service ou police le client doit avoir une authentification unique, combinaison nom utilisateur et mot de passe bien crypter, longueur, complexité et nombre de tentatives bien définies. Ou utiliser le MFA (Multi Factor Authentification) qui est très sécuritaire car l'utilisateur donne la preuve de son identité connue du système. -Sécurisation de l'URL protéger Https : Https bien qu'elle soit connue comme sécuritaire présente des vulnérabilités avec le protocole SSL, ACME doit donc activer le protocole plus sécuritaire TLS sur ces serveurs. -Veiller aux mises a jour applicatifs disponible avec ces fournisseurs (patches, anti-virus, logiciels…), ce qui évite les attaques par virus et des vulnérabilités applicatifs exploitable par un attaquant -La redondance des systèmes critiques (serveurs applicatifs, base de données, systèmes réseautiques), ce qui permettra d'assurer la continuité du service en cas de panne sur un équipement, donc une réponse a la disponibilité du service - Pour éviter les élévations de privilèges, une politique de GIA (Gestion des identités et accès) doits et accès des clients et employés bien définis selon les rôles et responsabilités, donc une vérification périodique des accès et utiliser des clé RSA pour les employés - Protection des systèmes et applications par des pares feux, antivirus, mise à jour système et applicatifs, ce qui permettra d'éviter les vulnérabilités), suivre les licences applicatives avec les fournisseurs -Faire des sauvegardes, pour une restauration du système en cas de crache, ce qui évite les pertes de donner - Auditer les Infrastructures et procédures de ACME (système de gestion et TI, accès usagers, base de données…) -Journalisation des évènements, les logs permettront ainsi d'avoir une traçabilité sur tous les évènements (comptes clients et employés, pannes, applications, etc…), ce qui protège contre les répudiations de données et donne un bon suivi activités clients et employés -Formation du personnel, permet d'éviter certaines failles comme les hameçonnages, les usurpations d'accès et la protection des données clients. -Veiller aux contrats, bien définir les rôles et responsabilités des parties prenantes (clients, employés et dirigeants…), nous pouvons citer la responsabilité du client a la confidentialité de son compte (mot de passe…) -Classification des donnés selon leur sensibilités (Confidentiel, Secret, Top Secret, non classifier), chaque partie sais a quoi elle a droits on gage de la confidentialité

	-Mise en place de cellule de gestion des crise et incidents majeur, pour les procédures, actions et la communication

Conclusion :

Les risques, les exigences et réponses à la cybersécurité varient en fonction de l'architecture du système informatique et d'une organisation a l'autre, mais les organisations d'un même secteur font plus ou moins face aux mêmes menaces.

ACME étant dans le secteur de l'assurance, la donnée est l'une voir la plus grande de ces ressources à protéger, garantir sa protection passe par la sécurisation des infrastructures et applications qui la supporte, mais pour bien répondre aux risques de fuites et fraudes de données, elle doit aussi avoir une bonne procédure et politique en termes de gestion des données entre autres leur classification et la gestion des accès.

Notre étude a permis d'évaluer le système de production de ACME avec la modélisation STRIDE et d'en ressortir les vulnérabilités possibles, émettre des hypothèses, fait une analyse de risques pour en ressortir des solutions pour la sécurisation de ses systèmes et applications.

Les cyberattaquants perfectionnant régulièrement leurs attaques afin de trouver et d'exploiter les failles de sécurité dans les systèmes d'informations. ACME doit donc aussi faire des ajustements au fil du temps pour le maintien d'un niveau de protection adéquat de ces systèmes et applications, d'où un bon suivi des contrats avec ces fournisseurs, les innovations dans le domaine et aussi une bonne formation de son personnel aux menaces de cybersécurités.

Nous pouvons conclure en disant ce qui suit : << Les risques existent toujours en cybersécurités mais ils s'atténuent avec les bonnes pratiques>>.

Références :

- Moes, T. (20221, 1 octobre) *What is a Spoofing Attack? The 5 Examples You Need to Know.* Softwarelab.org. https://softwarelab.org/what-is-spoofing/
- Menoth, R. (2018, 18 janvier) *Comprendre le modèle "STRIDE.* Microsofttechnet. https://social.technet.microsoft.com/wiki/contents/articles/51078.comprendre-le-modele-stride-fr-fr.aspx
- Common weakness Enumerartion. (2022, 28 juin). *CWE-400: Uncontrolled Resource Consumption.* https://cwe.mitre.org/data/definitions/400.html
- Haoues, M (2018, 2 mai) Déni de services distribué [notes de cours]. Département de cybersécurité. Polytechnique https://moodle.polymtl.ca/pluginfile.php/937846/mod_resource/content/0/CY110%20Cours5%20200205.pdf

- OWASP Foundation, (2017, 1 octobre). *A5:2017-Broken Access Control.* *https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control*
- OWASP Foundation, (2017, 5 octobre). *A3:2017-Sensitive Data Exposur.* *https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure*
- OWASP Foundation, (2022, 5 octobre). Web Parameter Tampering. *https://owasp.org/www-community/attacks/Web_Parameter_Tampering*
- OWASP Foundation, (2022, 5 octobre). *Repudiation Attack.* https://owasp.org/www-community/attacks/Repudiation_Attack
- Geek Flare, (2022, 1 octobre). *Attaques d'escalade de privilèges, techniques et outils de prévention.* *https://geekflare.com/fr/privilege-escalation-attacks/*
- Portswiger (2022, 1 octobre). *Information disclosure vulnerabilities.* *https://portswigger.net/web-security/information-disclosure*
- Hewko, A. (2022, 5 octobre).Softwaresecured. *STRIDE Threat Modeling: What You Need to Know.* *https://www.softwaresecured.com/stride-threat-modeling/*

https://www.ooaq.qc.ca/espace-membres/nouvelles/que-faut-il-savoir-loi-25/
https://www.techno-science.net/definition/5266.html
https://fr.wikipedia.org/wiki/Architecture_trois_tiers
https://softwarelab.org/
https://www.nist.gov/cyberframework
Le CISSP Démystifié Edition 2020 de Zakaria Hadj, CISSP