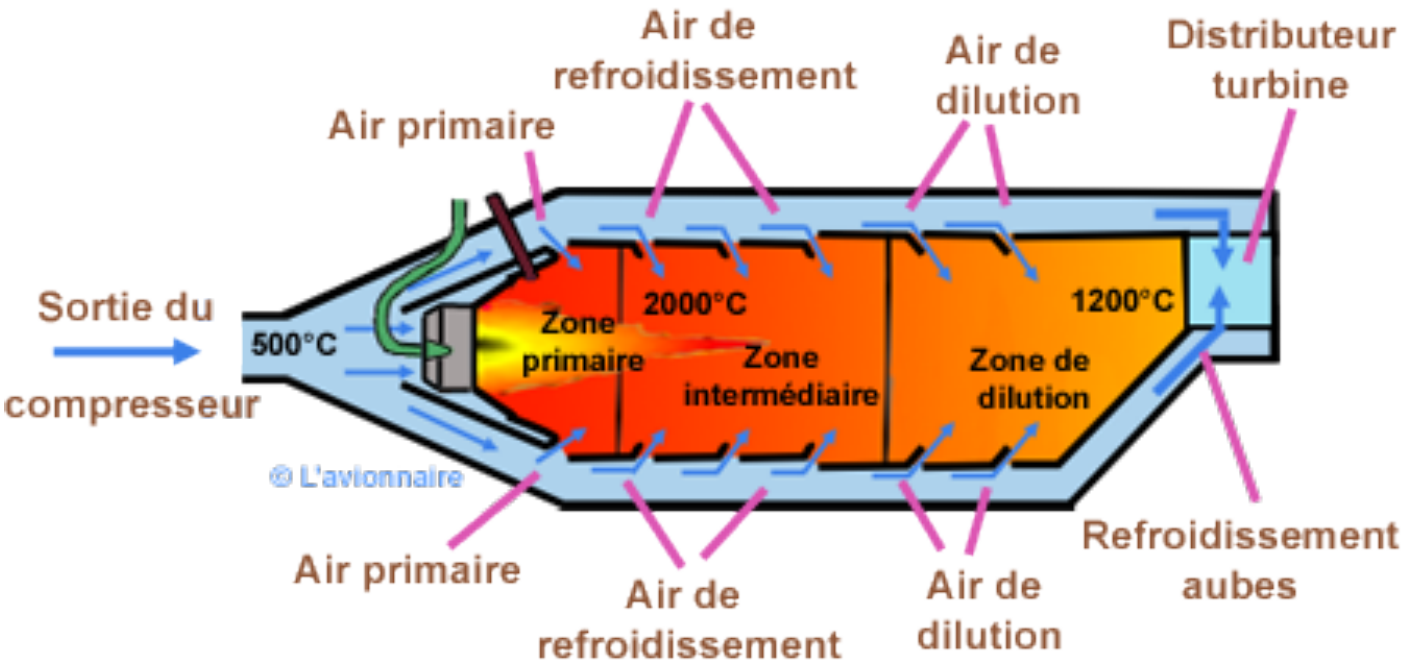
Examen 3SI

Gouvernance de la sécurité

Etude de cas



@AéroTomu corporation

Notes d'amélioration

Préciser que les exclusions sont a justifier
Si PDG a confiance dans une situation, les élèves ont tendances à suivre : a changer
Renforcer la notion de prévention dans le cours : empêcher une action de survenir vs protection empêcher action de réussir
Renforcer dans le cours le fait qu il ne faut pas inclure dans les scénario les attaques indirecte pour chaque biens support (exemple incendie)
Indiquer que les autres choix d'option de traitement des risques ne servent pas à grand chose
Ne pas mettre les conditions de travail perturbe trop apparemment
Renforcer le cours sur menace et source de menace

Introduction

La société AéroTomu est un fabriquant de pièces mécaniques opérant à l'échelle régionale. C'est une PME Toulousaine employant une trentaine de personnes et réalisant un chiffre d'affaire d'environ 50 Million d'euros par an.

Son activité consiste à réaliser des pièces techniques utilisées dans l'industrie aérospatiale. Ses produits sont spécialisés dans la combustion de carburant et sont issus de développements de longue durée. AéroTomu ne cherche pas pour le moment à étendre son activité dans d'autres types de pièce.

De par son savoir-faire unique et étant reconnu dans le secteur d'activité, AéroTomu possède de nombreux clients privés et publiques.

La structure de l'organisation

La direction

Le Président Directeur Générale (PDG) de l'entreprise est responsable de l'organisation de l'entreprise et de la définition de sa stratégie. Il est secondé par un directeur des opérations et un directeur commercial pour la gestion de la production et la vente auprès des clients.

Les services administratifs

Un bureau composé de 5 personnes est en charge de la gestion administrative de l'entreprise (RH, facturation, comptabilité etc.). La responsable de ce bureau est l'assistante de direction.

Les compétences des employés sont évaluées à leur embauche. La formation aux outils de production est effectuée par coaching.

Ce service a également en charge la gestion des fournisseurs et des sous-traitants (contrats, commandes, suivis, etc.). Seules les commandes de matières premières ne relèvent pas de sa responsabilité.

Les activités commerciales

2 commerciaux sont en charges de la gestion des comptes clients, du pilotage des contrats et du démarchage auprès de nouveaux clients. Le Directeur commerciale pilote actuellement un projet d'introduction de l'entreprise sur le marché Allemand.

La recherche et le développement

Historiquement, et par affinité avec les activités de recherche et développement, le PDG est également en charge du pilotage des activités de R&D.

Il assure à ce titre le suivi de l'ensemble des projets en cours.

7 ingénieurs sont en charge de ces activités de recherche.

Récemment le PDG a entendu, de la part de ses contacts, d'une société d'édition logiciel du même pôle d'activité Toulousain qu'AéroTomu ayant rencontré de sérieuses difficultés suite à un détournement de son savoir faire par ses développeurs. Cette actualité proche a particulièrement retenue l'attention du PDG.

La production

La production de pièces est assurée par une équipe de 10 personnes. Les activités principales de ce services sont :

- La commande et la réception de matières premières auprès de fournisseurs ;
- L'usinage et la transformation de pièces ;
- Gestion de la chaîne d'assemblage ;
- Test des pièces avant livraison.

L'usinage et la transformation de pièce et leur assemblage nécessitent des machines couteuses et dangereuses. La société dispose également de fours spéciaux pour les traitements thermiques. Une récente inspection du travail à rendu un rapport critique sur les conditions de sécurité dans lesquels travail les employés. Une mise en demeure a été notifiée à l'entreprise.

La chaine d'assemblage est semi-automatique et pilotée par un poste de travail. Récemment ce dernier a dû être remplacé du fait du déploiement d'un Ransomware, ce qui a entrainé une perte de productivité de plusieurs jours.

Partenaire:

Un partenariat industriel a été loué avec un motoriste local pour le test des pièces. En effet, les tests nécessitent des infrastructures couteuses pour une société comme AéroTomu. Les tests sont effectués par échantillonnage. Cette société fait partie du groupe indien Tata. Les activités de recherches peuvent également avoir à utiliser ces services. Cette société est considérée par le PDG comme un partenaire de confiance, ce dernier entretien de bonnes relations avec le Directeur qu'il rencontre régulièrement dans un club sportif de la région.

Transport

La logistique et le transport des pièces auprès des clients sont sous-traités auprès d'une société spécialisée appelée RaceTransit. Cette société assure également l'envoi et le retour des pièces testés.

Le site de l'entreprise

Le site de l'entreprise est un ancien hangar. L'espace est en majorité occupé par la chaîne d'assemblage.

Le point de livraison/chargement est attenant à cet espace. Il est séparé de ce dernier par un grillage de 3 m de haut disposant d'une porte fermée à clef en fin de journée. La porte permettant d'effectuer les chargements est un rideau de fer ouvert en journée et fermé le soir.

Les bureaux, salles de réunion et local pour les activités de R&D sont des préfabriqués installés à l'intérieur du hangar. Attenant aux espaces d'assemblage.

Les bureaux et autres espaces sont fermés à clé en fin de journée, les responsables d'équipe de la clé, la fermeture est à la charge du dernier employé qui part. Il est dernièrement apparu que certains locales ne sont pas régulièrement fermés à clés.

Les clés sont déposées dans une boite à clef blindée, à code et scellée à un pilier en béton. Les responsables d'équipe possèdent un double.

La société bénéficie la nuit des services de ronde du pôle d'activité et qui sont financés par la métropole.

Le système d'information local

Un responsable informatique gère l'ensemble du système d'information d'AéroTomu et s'appuie pour certaines tâches d'administration sur deux ingénieurs de production ayant des compétences informatiques. La gestion est effectuée au quotidien, suivant les besoins. Le budget informatiques étant limité, leurs activités se résument au maintient en service et au support utilisateurs.

Les ingénieurs en chargent de la R&D disposent de postes de travail fixes dotés de suites bureautiques et de logiciels de modélisation et de calcul.

L'ensemble des autres employés utilisent des postes de travail portables dotés des mêmes suites bureautiques.

Les suites bureautiques sont Open Source, les logiciels professionnels nécessaires à la réalisation des activités de R&D et de production sont sous licence (cela concerne également les appliances servers.

Les postes de travail des ingénieurs disposent de systèmes Unix qui ne disposent pas d'antivirus, le responsable informatique jugeant ces outils inutiles sur ce type d'environnement. Les autres postes de travail (dont le poste de la chaine d'assemblage) disposent de Systèmes Windows 7 et sont équipés d'une version gratuite d'Avast.

Les utilisateurs sont administrateurs de leurs postes de travail afin de faciliter leur travail quotidien et de limiter les sollicitations des responsables techniques

Deux serveurs, sous Windows Server 2012, sont hébergés dans une pièce dédiée du site de l'entreprise. Ils ont été installés par des professionnels il y a 2 ans. Ils couvrent les besoins suivants :

1. Un serveur pour les applications de conception (R&D) et de gestion des chaines d'assemblage, cela inclue leurs base de données. L'accès aux applications se fait via un navigateur à partir des postes de travail des équipes et de celui de la chaine d'assemblage.
2. Un serveur de domaine qui gère l'identification et l'authentification, ainsi que l'accès à Internet. Ce serveur fait également office de serveur de fichiers pour les taches administratives et commerciale et est relié à une baie de stockage.
3. Chaque serveur est équipé d'un lecteur de bande magnétique pour les sauvegardes. Celles-ci sont réalisées toutes les nuits et le responsable informatique extrait chaque matin les bandes pour les mettre dans un coffre ignifuge placé dans le

bureau du PDG.
La société dispose en complément de deux imprimantes en libre accès à coté de l'espace cafétéria par l'ensemble des collaborateurs. Cet espace fait partie des préfabriqués, il est à l'intersection des différents bureaux.

L'hébergement du site institutionnel de la société est assuré par un prestataire de service externe (ZenWeb) et hébergé sur des infrastructures d'OVH. La gestion de la messagerie est externalisée sur Office365, il s'agit d'un achat de service dit sur « étagère ».

L'accès internet est fournit par Orange qui met également à disposition une boxe professionnelle disposant d'un pare-feux. L'installation est d'origine et n'a été revue qu'il y a 3 ans suite au passage à la fibre optique. La boxe est située dans le bureau de l'assistante de direction du fait de l'historique de l'installation.

Le réseau est un réseau filière, ethernet avec une topologie en étoile, un switch est installé sur la même baie que les serveurs et permet de relier l'ensemble des machines. Ce réseau a été installé par l'opérateur Orange à l'occasion du passage à la fibre.

Un accès wifi (clé WPA2) est disponible pour les postes de travail portables.

Organisation de la production

Les plans sont issus des activités de R&D et sont disponibles sous format PDF sur le serveur de la chaine d'assemblage. Ils sont également disponibles sur les stations de travail des ingénieurs en charge de l'usinage et la transformation des matières premières.

Clientèle

La relation avec la clientèle est bonne et est assurée par le service commercial.

Récemment un client a été particulièrement curieux des conditions de réalisation des pièces. En effet, il est apparu que ses autorités de tutelle lui demandait de plus en plus de compte sur la sureté de ses produits, dont ceux fournis par AéroTomu.

Cette émulation du marché résulte de différents incidents techniques récurrents sur certains types de moteurs.

Organisation de la R&D

L'équipe de R&D est en charge des projets de recherche mais également de l'amélioration des produits existants.

Les ingénieurs de production et de R&D peuvent régulièrement interchanger leurs activités pour éviter la routine et favoriser une émulation créatrice. Ce principe est un élément important de la culture d'entreprise et les employés y sont très attachés.

Organisation de la facturation

Tous les mois, des factures sont établies par le service administratif sur la base des livraisons effectuées et déclarées par les ingénieurs de production via l'outil de gestion. Ces factures sont ensuite imprimées localement et envoyées par courrier aux clients.

Le marché

Le marché aéronautique est en croissance constante malgré un ralentissement général ces derniers mois. Les programmes avioniques portent principalement sur la modernisation des appareils, et donc de leurs moteurs. Les sociétés comme AéroTomu sont très recherchées et convoitées.

Démarche de sécurisation du SI

Les récents évènements ont motivés le PDG sur la nécessité de se rapprocher d'un cabinet de conseil afin d'améliorer la sécurité informatiques de son entreprise.
Le cabinet a mandaté un consultant qui propose d'effectuer un état des lieux de procéder à une analyse de risque de l'entreprise. Le budget de ce projet est spécifique mais réduit, le PDG demande à ce que l'analyse se focalise sur l'essentiel et les menaces les plus importantes pour l'entreprise.
L'état des lieux consiste a identifier les actifs informationnels et techniques de l'entreprise, ses mesures de sécurité, et à analyser le contexte et les besoins métiers via un ensemble d'interview. En plus de. cette démarche classique, cette étude inclue une analyse de l'incident viral dont a été victime l'entreprise. Cette enquête à révéler que, en plus de faiblesses des systèmes antiviraux actuels, le virus c'était propagé via un plan reçu de la part de l'équipe de R&D. Il est demandé au cabinet de proposer des mesures afin de se prémunir de ce type d'incidents.

Consignes et conseils

A partir de cette étude de cas, réalisez une analyse de risque en utilisant la méthodologie EBIOS par groupe de 2/3 personnes.

L'étude doit s'arrêter à la déclaration d'applicabilité.

Intégrez dans votre étude d'état des lieux et d'étude de l'incident de sécurité par le cabinet de conseil.

Choisissez au minimum deux critères de sécurité pour l'étude.

L'ensemble des évènements redoutés est à rédiger. Par contre, la rédaction des scénarios et des risques portera sur un seul des biens essentiels que vous aurez identifiés.

La notion de planning n'est pas à intégrer dans le rapport (exemple planning de mise en oeuvre des mesures de sécurité).

N'oubliez pas le principe d'amélioration continue revenez régulièrement en arrière dans votre démarche d'analyse.

Il est déconseillé de sauter des étapes, faites les dans l'ordre.

Le rapport est à rendre avant le 04/02/2019.

Methode de notation

Il est attendu une analyse de risque respectant l'ensemble des étapes de la méthodologie EBIOS. Chaque module Ebios sera noté selon le barème suivant:

1. Module 1 : 15 points ;
2. Module 2 : 5 points ;
3. Module 3 : 15 points ;
4. Module 4 : 5 points ;
5. Module 5 : 5 points.

Vous utiliserez les métriques du guide méthodologique Ebios 2010.
Il est inutile de faire une déclaration d'applicabilité.

5 points seront dédiés à la cohérence d'ensemble et au respect de la méthodologie.

Votre capacité à synthétiser le contexte (textes schémas, tableaux) et à identifier les paramètres et enjeux sera appréciée.

Sortir du vocabulaire « scolaire » de la base de connaissance est encouragé mais non obligatoire.

Il n'est pas attendu à ce que votre étude soit exhaustive.