CNAM ÎLE-DE-France
SEC 101

Devoir: Analyse de risques 1

Vous devez faire l'atelier 1 et 2 sur l'entreprise DataSecure Tech

Atelier 1:

Les Valeurs Métier:

Définition selon la méthode ebios risk manager: *"composante importante pour l'organisation dans l'accomplissement de sa mission. Cela peut être un service, une fonction support, une étape dans un projet et toute information ou savoir-faire associé"*.

Les valeurs métier représentent le patrimoine informationnel qu'une source de risque aurait intérêt à attaquer pour porter atteinte à l'objet de l'étude, c'est donc dans cette optique que l'on va dresser celles-ci:

- L'innovation et l'excellence technologique:
  - Elle permettra de se distinguer par des solutions innovantes et de qualité en matière de sécurité des données et de gestion des processus d'affaires.
  - Importance: permet de rester compétitif sur le marché des technologies de l'information et de répondre aux besoins évolutifs des clients.

- La sécurité et la conformité:
  - Elles permettent de garantir la protection des données et respecter les normes réglementaires.
  - Importance: critique pour maintenir la confiance des clients et éviter les sanctions légales.

- La confidentialité et l'intégrité des données:
  - Permet de protéger les données des clients contre toute divulgation non autorisée et assurer leur exactitude.
  - Importance: essentiel pour la crédibilité de l'entreprise et la fidélité des clients.

- Le service client et la satisfaction:
  - Description: Fournir un support exceptionnel et maintenir des relations positives avec les clients.
  - Importance: Favorise la rétention des clients et génère des recommandations positives.

- La collaboration et les partenariats:
  - Permettra de travailler en collaboration avec des partenaires technologiques et des fournisseurs pour offrir des solutions complètes.
  - Importance: augmente la capacité d'innovation et l'étendue des solutions offertes.

Biens Supports

Définition selon la méthode ebios risk manager: Le bien support est la composante du système d'information sur laquelle repose une ou plusieurs valeurs métier. Un bien support peut-être de nature numérique, physique ou organisationnelle.

- L'infrastructure cloud:

- Son rôle est d’héberger et gérer les services essentiels, stocker les données critiques, ce bien support est particulièrement critique pour DataSecureTech qui est spécialisée dans les plateformes cloud.
- L’impact: La perte ou la compromission pourrait paralyser l'entreprise.

- Le réseau d’entreprise:
  - Rôle: Permet des communications sécurisées et l'accès aux ressources internes.
  - Impact: des interruptions peuvent causer des pertes de productivité et exposer des données sensibles, ce qui serait particulièrement dommageable pour DataSecureTech spécialisée dans les solutions de sécurité des données.

- Les applications et les logiciels:
  - Rôle: Supporter les opérations de gestion des relations clients et de développement de produits, bien support également critique du fait que DataSecureTech soit spécialisée dans les solutions de sécurité des données.
  - Impact: La compromission peut entraîner des fuites de données ou des interruptions de service.

- Les bases de données:
  - Rôle: Elles stockent des données clients et opérationnelles cruciales.
  - Impact: La corruption ou le vol de données peut entraîner des pertes financières et de la réputation.

Missions

Définition selon la méthode ebios risk manager: Fonction, finalité, raison d’être de l’objet de l’étude.

- Le développement de solutions de sécurité:
  - L’objectif est de créer des applications et des services qui protègent les données des clients et assurent leur intégrité.
  - Il faut garantir la sécurité des données pour les clients et maintenir une réputation de fiabilité.

- La gestion des processus d'affaires:
  - L’objectif est d’offrir des outils et plateformes pour améliorer l'efficacité et la transparence des opérations commerciales des clients.
  - Permet d’améliorer la productivité et la gestion des données pour les entreprises clientes.

- La conformité réglementaire:
  - Objectif: Assurer que les solutions et les processus internes respectent les normes de sécurité et de protection des données.
  - Impact: Éviter les sanctions légales et maintenir la conformité aux lois.

- Innovation Technologique:
  - Objectif: Rechercher et intégrer des technologies de pointe pour rester à la pointe de l'innovation en matière de sécurité et de gestion des processus.
  - Impact: Maintenir la compétitivité et la pertinence sur le marché.

Événements Redoutés et leur Niveau de Gravité

- Violation de Données:
  - Accès non autorisé aux données clients ou internes.
  - Gravité: Élevée
  - Impact: Pertes financières, atteinte à la réputation, sanctions réglementaires.

- Intrusion Réseau:
  - Attaque visant à compromettre l'infrastructure réseau.
  - Gravité: Très élevée
  - Impact: Interruption des services, accès non autorisé aux systèmes critiques.

- Panne de Service Cloud:
  - Interruption des services hébergés dans le cloud.
  - Gravité: Très élevée du fait de la nature de l'entreprise (spécialisée dans les plateformes cloud).
  - Impact: Perte d'accès aux données et services essentiels, perte de productivité.

- Perte de Données:
  - Perte de données critiques en raison d'un échec de sauvegarde ou d'une attaque.
  - Gravité: Élevée
  - Impact: Pertes opérationnelles, incapacité à restaurer des services, critique pour les bases de données SQL et NoSQL de DataSecureTech pour stocker les données clients.

- Non-Conformité Réglementaire:
  - Non-respect des exigences légales ou des standards de sécurité.
  - Gravité: Élevée
  - Impact: Sanctions financières, atteinte à la réputation, perte de confiance des clients de notre start-up.

Socle de Sécurité : Référentiels Applicables

- ISO/IEC 27001:
  - Norme internationale pour la gestion de la sécurité de l'information.
  - Applicabilité: Établissement d'un Système de Management de la Sécurité de l'Information (SMSI) pour protéger les informations.

- ISO/IEC 27017:
  - Contrôles de sécurité de l'information pour les services **cloud**. Norme donne des directives pour la sécurité de l'information et pour le contrôle applicable à la disposition et à l'utilisation de services du cloud computing. Cette norme est intéressante pour notre start-up du fait de sa gestion des processus d'affaires via des applications mobiles et des plateformes cloud.
  - Applicabilité: Spécifique à la gestion de la sécurité dans les environnements cloud comme **AWS pour l'hébergement de services**.

- ISO/IEC 27018:
  - Protection des données personnelles dans le **cloud**.
  - Applicabilité: Pertinent pour assurer la conformité avec les réglementations sur la protection des données.

- Le RGPD:
  - Réglementation européenne sur la protection des données personnelles.
  - Applicabilité: Oblige à mettre en place des mesures de protection des données pour les clients européens.

- Le NIST:
  - C'est un guide pour la gestion des risques en matière de cybersécurité.
  - Applicabilité: Utilisé pour structurer et améliorer la posture de sécurité de l'entreprise.

Échelles de Mesure de la Sécurité

- Échelle de Gravité des Incidents:

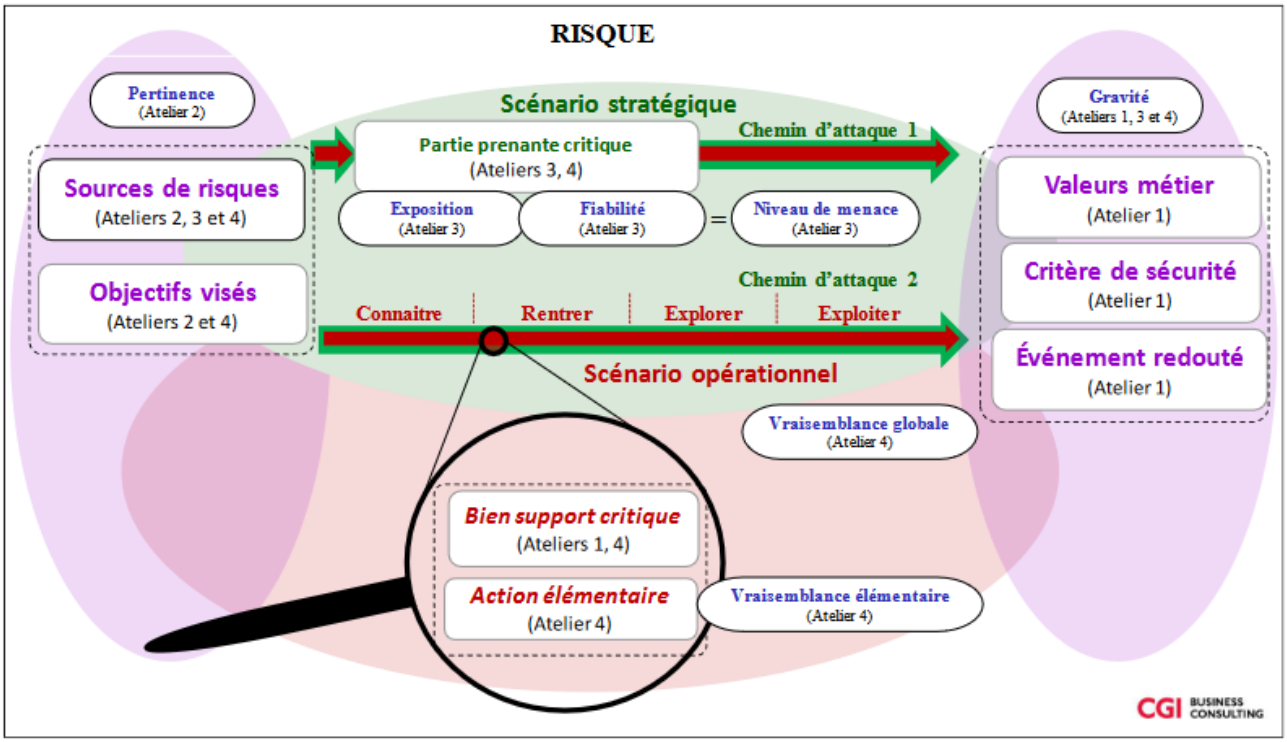
- Niveaux:
  - Faible: Impact minimal sur les opérations, résoluble rapidement.
  - Moyen: Impact modéré, nécessite une attention mais n'affecte pas les opérations critiques.
  - Élevé: Impact significatif, affecte les opérations clés, nécessite une intervention immédiate.
  - Très Élevé: Impact grave, menace la viabilité de l'entreprise, réponse d'urgence requise.

- Échelle de Probabilité des Menaces:
  - Niveaux:
    - Rare: Très peu probable, incident exceptionnel.
    - Occasionnel: Probable, peut se produire de temps en temps.
    - Fréquent: Hautement probable, incidents réguliers.
    - Certain: Inévitable, incidents très fréquents.

Atelier 2:

- Liste de couples SR/OV retenus
  - Avec la table: source de risque, objectif visé, motivation, ressources, pertinence, justification

Source de risque	Objectif visé	Motivation	Ressources	Pertinence	Justification
Cybercriminels	Phishing, Ransomware...	Très motivé	Significatives	Assez pertinent	Augmentation des menaces, en particulier les attaques par phishing et les violations de données
Concurrents	Espionnage industriel	Fortement motivé	Importante	Très pertinent	Fuite d'informations confidentielles et sensibles concernant les stratégies d'entreprise ou les développements technologiques
Employés et/ou prestataires malveillants	Sabotage, vol d'informations	Assez motivé	Importante	Plutôt pertinent	Divulgation non autorisée d'informations sensibles liées aux partenariats et aux accords commerciaux
Hacktivisme	Attaques par Déni de Service (DdoS), intrusion dans les réseaux d’entreprise	Fortement motivé	Significatives	Moyennement pertinemment	



Source: https://club-ebios.org/site/wp-content/uploads/productions/Club%20EBIOS%20-%20EBIOS%20Risk%20Manager%20-%20M%C3%A9mento%20-%202020-04-03.pdf