|  |  |
| --- | --- |
| **BTS SIO2**  **bloc 1** | **B1-Act3-TD1 – Évaluation des risques EBIOS RM (0h30)** |

**Introduction**

La méthode **EBIOS-RM** (Expression des Besoins et Identification des Objectifs de Sécurité - Risk Manager) est un outil de gestion des risques qui permet d'évaluer les menaces et vulnérabilités pesant sur le système d'information (SI) d'une organisation. Pour illustrer l’utilisation concrète d’EBIOS-RM dans une PME, nous allons prendre le cas d’une entreprise, "**TechnoCo**", spécialisée dans la vente en ligne de matériel électronique.

**Contexte de l’entreprise**

TechnoCo emploie 50 salariés et dispose d'un système d'information qui gère :

* un site e-commerce pour les ventes
* une base de données clients contenant des informations sensibles (noms, adresses, moyens de paiement).
* un ERP (Enterprise Resource Planning) pour la gestion des stocks, commandes, et logistique ;
* des e-mails et systèmes de communication interne utilisés par les employés ;
* des partenaires externes (logisticiens, prestataires de services de paiement).

**Évaluation des menaces et vulnérabilités de la société TechnoCo**

1. **Atelier 1 : cadrage et socle de sécurité**

Objectif : Définir le périmètre de l'analyse des risques, les événements redoutés et la gravité

Périmètre analysé : Le SI de TechnoCo, incluant le site e-commerce, la base de données clients, l’ERP et les communications internes.

Acteurs concernés : Les équipes IT, les responsables du site web, la direction, et les partenaires externes.

Méthode utilisée : EBIOS-RM sera utilisé pour évaluer les risques liés à la confidentialité, l'intégrité et la disponibilité des données.

**On a repéré pour vous 3 risques concernant le SI de la société TechnoCo. Il est à noter qu’une liste plus importante des risques pourrait être établie.**

Travail demandé : complétez les colonnes de l’atelier 1 dans le tableau page 3, concernant ces 3 risques.

1. **Atelier 2 : sources de risque et pertinence**

Objectif : Identifier le niveau de pertinence des risques visés dans l’atelier 1.

Travail demandé : complétez la colonne évaluant le niveau de pertinence pour chacun des risques.

1. **Atelier 3 : scénarios stratégiques**

Objectif : Identifier les parties prenantes externes les plus vulnérables et de bâtir des scénarios stratégiques : chemins d’attaques que pourrait emprunter une source de risque pour atteindre son objectif.

Travail demandé : complétez la colonne décrivant le chemin d’attaque pour chacun des risques étudiés.

1. **Atelier 4 : vraisemblance du risque**

Objectif : évaluer la vraisemblance du risque.

Travail demandé : évaluez la vraisemblance pour chacun des risques étudiés.

1. **Atelier 5 : traitement du risque**

Objectif : définir une stratégie de traitement du risque avec une série de mesures de sécurité à mettre en œuvre

Travail demandé : proposez des mesures de sécurité à mettre en œuvre pour supprimer ou limiter les risques étudiés.

**Conclusion:**

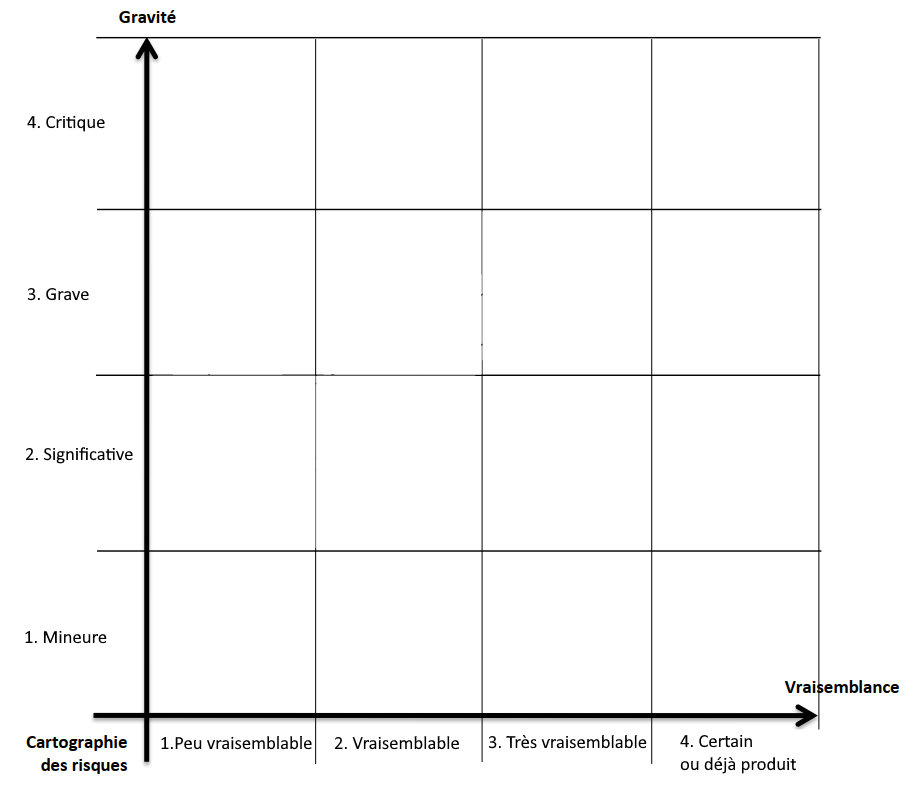
*L’utilisation de la méthode EBIOS-RM permet à PME TechnoCo de prendre conscience des risques pesant sur son SI, de les prioriser en fonction de leur gravité et de leur probabilité, puis de définir et appliquer des mesures de sécurité adaptées. Une fois ces mesures en place, un plan de suivi et de mise à jour périodique est essentiel pour s’adapter à l’évolution des menaces.*

**Les 5 ateliers de la méthode EBIOS-RM – À COMPLÉTER**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ATELIER 1** | | | | **ATELIER 2** | **ATELIER 3** | **ATELIER 4** | **ATELIER 5** |
| **Risques** | **Événements redoutés jugés comme les plus graves** (impacts sur les actifs et/ou personnes concernées) | **Actifs concernés** | **Gravité** | **Pertinence du risque** | **Scénarios Chemins d’attaques** | **Vraisemblance** | **Traitement du risque** |
| **R1 – Atteinte à la disponibilité du site e-commerce** | Un acteur malveillant externe (cybercriminel) effectuant une attaque DDoS (déni de service distribué).  **Conséquences** : Le site devient inaccessible, perte de ventes et d’image de marque. | Serveurs web du site e-commerce | G2 - Significative | Très pertinent (facilité de la mise en œuvre d’une attaque sur un service web.) | Un acteur malveillant externe (cybercriminel) effectuant une attaque DDoS. | Très vraisemblable | Installation d’un IPS |
| **R2 – Violation de la confidentialité des données clients** | Vol ou perte des données des clients (coordonnées,…)  **Conséquences** :  Perte de confiance des clients, perte financière, sanctions CNIL | Serveurs de base de données | G4 - Grave | Plutôt pertinent | Un prestataire malveillant ou négligent qui accède aux données. Il transmet ces données à des cyberattaquants sur le net. | vraisemblable | Chiffrement les données. |
| **R3 – Sabotage de des systèmes internes via phishing** | Sabotage des systèmes internes (logiciel ERP, serveurs) suite à du phishing  **Conséquences**:  Compromission du logiciel de gestion des stocks, des achats, des salaires, de la facturation, des livraisons,… | Comptes email des employés, logiciel ERP | G3 - grave | Plutôt pertinent | Un acteur malveillant, externe à l’entreprise, envoie un mail phishing pour récupérer des informations. Après quoi il s’introduit dans le SI de l’entreprise et s’attaque au logiciel ERP. | Vraisemblable | Prévention, configuration des clients mails, charte informatique,… |

**La matrice des scénarios des risques – À COMPLÉTER**

*Placez sur la matrice ci-dessous les risques R1 à R6 avant et après la mise en place des mesures.*



**RAPPELS SUR LA METHODE EBIOS-RM**

