**Analyse des Risques – Web**

1. ***Identification des Actifs***

*Voici le périmètre de l’analyse :*

*Données : Fichiers Interne & Externe*

*Systèmes : Serveurs : dysnfs01p ; odysftp02p, Réseaux : 001-int-prd-odys ; 008-ext-dmz-odys*

*Personnel : Tous les employés.*

*Aucune accessibilité aux ressources de l’entreprise et client*

1. ***Identification des Menaces***

Voici les différentes Menaces identifiées :

Menaces Physiques : Incendie, Inondation, Vol de Matériel, Attaques sur les Systèmes Embarqués.

Menaces Technologiques : Attaques par Malwares, Intrusions Réseau,Zero-Day, attaques par credential stuffing, attaques de phishing, attaques par force brute, injectionSQL.

Menaces Humaines : Erreurs Humaines, Vol de Données par les Employés, Fuites d'Informations, Insider Threats (Menaces Internes), Attaques sur les Systèmes de Contrôle Industriel, attaques d'ingénierie sociale.

1. **Évaluation des Vulnérabilités**

Voici les différentes Vulnérabilités identifiées :

Manque de Sécurité Physique : Absence de Systèmes Anti-incendie, Contrôles d'Accès Inadéquats, absence de contrôles physiques adéquats.

Défauts de Sécurité Informatique : Logiciels Non Mis à Jour, Faiblesse des Mots de Passe, gestion inadéquate des privilèges, absence de systèmes de surveillance et de détection d'intrusion, Défauts de Configuration, négligence des normes de sécurité.

Insuffisance des Procédures : Absence de Plan de Continuité d'Activité, Procédures de Sauvegarde Inadéquates, Manque de Chiffrement, Manque de Mises à Jour de Sécurité, Faiblesse dans la Gestion des Correctifs, absence de sauvegardes régulières, Défauts dans la Gestion des Logs, empêcher les injections SQL.

1. **Estimation de la Probabilité & de l'Impact**

Voici la Probabilité qu’une menace se concrétise :

Menaces Physiques :

* Incendie : Moyen
* Inondation : Faible
* Vol de Matériel : Faible

Menaces Technologiques :

* Logiciels Non Mis à Jour : Moyen
* Faiblesse des Mots de Passe : Elevée
* Gestion inadéquate des privilèges : Moyen
* Défauts de Configuration : Elevée
* Négligence des normes de sécurité : Elevée
* Attaques par Malwares : Moyen
* Intrusions Réseau : Moyen

Menaces Humaines :

* Erreurs Humaines : Faible
* Vol de Données par les Employés : Elevée

Voici l’Impact potentiel sur les activités de l'entreprise si une menace se matérialise :

Menaces Physiques :

* Incendie : Elevée
* Inondation : Elevée
* Vol de Matériel : Moyen

Menaces Technologiques :

* Logiciels Non Mis à Jour : Moyen
* Faiblesse des Mots de Passe : Elevée
* Gestion inadéquate des privilèges : Elevée
* Défauts de Configuration : Elevée
* Négligence des normes de sécurité : Elevée
* Attaques par Malwares : Elevée
* Intrusions Réseau : Elevée

Menaces Humaines :

* Erreurs Humaines : Elevée
* Vol de Données par les Employés : Elevée

1. **Calcul du Risque**

Voici le tableau du calcul du niveau de risque :

|  |  |  |  |
| --- | --- | --- | --- |
| **Probabilité \ Impact** | **Faible** | **Moyen** | **Elevée** |
| **Faible** | Négligeable | Modéré | Critique |
| **Moyen** | Modéré | Significatif | Majeur |
| **Elevée** | Critique | Majeur | **Catastrophique** |

Risque :

Menaces Physiques :

* Incendie : Majeur
* Inondation : Critique
* Vol de Matériel : Modéré

Menaces Technologiques :

* Logiciels Non Mis à Jour : Significatif
* Faiblesse des Mots de Passe : Catastrophique
* Gestion inadéquate des privilèges : Majeur
* Défauts de Configuration : Catastrophique
* Négligence des normes de sécurité : Catastrophique
* Attaques par Malwares : Majeur
* Intrusions Réseau : Majeur

Menaces Humaines :

* Erreurs Humaines : Elevée
* Vol de Données par les Employés : Elevée

1. **Priorisation des Risques**

Voici le tableau du calcul de la criticité :

|  |  |  |  |
| --- | --- | --- | --- |
| **Probabilité \ Impact** | **Faible** | **Moyen** | **Elevée** |
| **Faible** | Non Critique | Non Critique | Critique |
| **Moyen** | Non Critique | Critique | **Stratégique** |
| **Elevée** | Critique | **Stratégique** | **Stratégique** |

Voici les risques par ordre de priorité en fonction de leur niveau de criticité :

* Stratégique
  + Incendie
  + Vol de Données par les Employés
  + Logiciels Non Mis à Jour
  + Faiblesse des Mots de Passe
  + Gestion inadéquate des privilèges
  + Négligence des normes de sécurité
  + Attaques par Malwares
  + Intrusions Réseau
* Critique
  + Inondation
  + Erreurs Humaines
* Non Critique
  + Vol de Matériel

1. **Recommandation & Gestion des Risques**

Contrôles Physiques : Installation de Systèmes Anti-incendie, Renforcement des Contrôles d'Accès,.

Contrôles Informatiques : Mises à Jour Régulières des Logiciels ou applications, Renforcement des Politiques de Mot de Passe, empêchement d’injections.

Procédures de Sécurité : Élaboration d'un Plan de Continuité d'Activité, Amélioration des Procédures de Sauvegarde, Redondance, Load Balancing.

Gestion des Risques : Élaboration d'un Plan pour chaque menace qui se concrétise.