EBIOS RM dans la Pratique

# Questionnaire pour une compréhension de base d'un système d'information


AMN BRAINS
amnbrains.com/blog

# EBIOS RM dans la pratique

# Questionnaire pour une compréhension de base d'un système d'information

Ce document s'inscrit dans de le cadre de la série «EBIOS RM Dans la Pratique», **une formation en ligne gratuite à la méthode EBIOS Risk Manager**. Il fournit une liste de questions qu'il convient de (se) poser en vue d'acquérir une compréhension de base du système étudié. Cette compréhension est indispensable pour mener à bien les ateliers de la méthode.

Ce questionnaire couvrent toutes les couches du système, depuis la couche physique, jusqu'aux aspects fonctionnels et métier, en passant par le réseau, les systèmes et les applicatifs. Il couvre également l'organisation relative au système et les éléments qui gravitent autour (écosystème).

Dans une analyse des risques comme dans la cybersécurité de manière générale, cette maîtrise est essentielle. Pour vous aider, ce document sert comme liste de course pour démarrer.

# Couche fonctionnelle et métier

## Missions, Fonctions, Données

### Identifier les missions stratégiques du système d'information

**Pour remplir chacune des missions :**

- Quelles sont les fonctions rendues pour les remplir ?
- Quelles sont les données manipulées ?
- Quelles sont les utilisateurs métier ? Comment ils interagissent avec le système ?

# Couche fonctionnelle et métier

## Les Données

### Identifier les données manipulées par le système

**Pour chaque donnée :**

- Dans quel(s) processus elle est impliquée ?
- Quels composants applicatifs, systèmes et matériels sont impliquées dans son traitement, transfert ou stockage ?
- Qui peut y accéder, en lecture ou en écriture ? Par quels moyens ?

# Couche Applicative

## Les Composants Applicatifs

### Identifier les composants applicatifs constituant le système

**Pour chaque composant applicatif identifié :**

- Quelles sont les fonctions rendues ?
- Quelles sont les données manipulées ?
- Quelles sont les composants logiciels ? Quelles solutions sont utilisées ? Sur quelles machines ils s'exécutent ? Avec quels droits système ?
- Quelles sont ses interfaces d'interaction (IHM, réseau…) ? Sous quelles conditions sont-elles accessibles (pour un attaquant) ? Quelles sont les méthodes d'authentification ? ? Comment les accès sont-ils authentifiés ? Quels sont les interlocuteurs légitimes ? Quels sont leurs droits associés ?
- Quelles sont les communications associées (en tant que source ou destination) ?

# Couche Applicative

## Les Communications

### Identifier les communications au sein du système ou avec l'extérieur

**Pour chaque communication identifiée :**

- Quelle est son utilité ?
- Quelles sont les données transportées ?
- Dans quelle(s) fonction(s) cette communication est-elle impliquée ?
- Source : Quel composant logiciel ? Sur quelle machine ? sur quelle interface réseau ? Depuis quel réseau ?
- Destination : Quel composant logiciel ? Sur quelle machine? sur quel port réseau ? Sur quelle interface réseau ? Dans réseau ?
- Chemin : Quelles sont les réseaux et les interconnexions traversés ?
- Quel est le protocole utilisé ?
- Comment la communication est elle protégée en confidentialité, en intégrité et en authenticité (dans les deux

# Infrastructure Système

## Les Machines 1/2

- **Identifier les machines, physiques ou virtuelles, constituant le système**

**Pour chaque machine identifiée :**

- Quelle est son utilité ?
- Dans quelles fonctions est-elle impliquées ?
- Quelles données y sont stockées ou manipulées ?
- Quel système d'exploitation ? Quelle version ?
- Le cas échéant, à quel domaine elle appartient ?
- [Machine Virtuelle] Quel(s) serveur(s) ou cluster de virtualisations ? Quelle est la solution de virtualisation ?
- [Machine Virtuelle] Où est-elle situé ? Et dans quelle mesure est-elle accessible physiquement ?
- Quels sont les logiciels et applicatifs installés ? Avec quels droits sont-ils exécutés ? Quelle est leur utilité ?
- Pour les serveurs windows, quels rôles sont activés ?

# Infrastructure Système

## Les Machines 2/2

- Combien d'interfaces réseau ? A quel(s) réseau(x) sont-elles connectées ?
- Quels sont les ports réseau ouverts ? Par quel logiciel/ service ? Sous quelles conditions sont-ils accessibles (pour un attaquant) ?
- A quels réseaux la machine donne-t-elle accès ? A-t-elle accès à Internet ?
- Quels sont les moyens de prise en main disponibles (Ecran/ Clavier/Souris, RDP, WINRM, SSH, ...) ? Sous quelles conditions sont-ils accessibles (pour un attaquant) ? Quelles sont les méthodes d'authentification ?
- Quels individus sont autorisé à la prise en main de la machine ? Par quels moyens ? Avec quels droits ? Pour quel usage ?
- Des partages réseau existent ? Avec quelles données ? Qui peut y accéder (en lecture ou en écriture) ?

# Infrastructure Système

## Les Domaines Windows

- **Identifier les domaines windows constituant le système et leur structure**

**Pour chaque domaine identifié :**

- Quelles est le modèle d'habilitation associé (qui a accès à quoi) ?
- Quelles machines sont contrôleurs de domaine ?
- Quelles sont les machines associées ?
- Quels sont les utilisateurs associés ?
- Quelles relations d'approbation sont en place ?

# Infrastructure réseau

## Les Réseaux 1/2

### Identifier les réseaux / sous-réseaux, physiques ou virtuels

**Pour chaque réseau / sous réseau identifié :**

- Quelle est son utilité ?
- Quelles machines y sont connectées ?
- Quels individus s'y connectent ? Par quel moyen (Filaire, WIFI, VPN) ?
- Quelles interconnexions a-t-il avec les autres réseaux / sous-réseaux ?
- Quelles sont les règles de filtrage associées à chaque interconnexion ?
- Quels sont les points d'accès filaires (ex. prise RJ45) associés ? Où sont ils situés physiquement ? Sous quelles conditions sont-ils accessibles (pour un attaquant) ? Comment les accès sont authentifiés/Contrôlés ?

# Infrastructure réseau

## Les Réseaux 2/2

- Quels sont les points d'accès radio associés ? Quelle est leur zone de couverture ? Sous quelles conditions sont-ils accessibles (pour un attaquant) ? Comment les accès sont authentifiés/Contrôlés ?
- Quels sont les point d'accès à distance (ex. VPN) ? Sous quelles conditions sont-ils accessibles (pour un attaquant) ? Comment les accès sont authentifiés/Contrôlés ?
- Quels sont les équipements réseau associés ? Quels modèles et quelles versions ? Où sont-ils situés physiquement ? Sous quelles conditions sont-ils accessibles (pour un attaquant) ?
- Par quels endroits sont acheminés les câbles réseau associés ? Dans quelles mesures sont-ils accessibles pour un attaquant ?

# Dispositif d'administration

- **Pour chaque composant identifié précédemment, identifier l'ensemble de ses interfaces d'administration**

**Pour chaque interface d'administration :**

- Elle est de quel type ? Elle utilise quel protocole ?
- Sous quelles conditions est-elle accessible physiquement pour un attaquant ?
- Sous quelles conditions est-elle accessible logiquement pour un attaquant ?
- Comment les accès sont authentifiés/Controlés ?
- L'administration est réalisé par quels individus ? Avec quels profils et droits d'accès ?
- L'administration est réalisée depuis quel(s) poste(s) d'administration ? Depuis quel(s) réseau(x) ? Une machine de rebond est-elle utilisé ? Dans quel réseau ?
- Une télémaintenance est-elle en place ? Par qui ? Par quel Canal ? Sous quelles conditions est-elle accessible pour un attaquant ?

# Infrastructure matérielle et physique

## Les Locaux

### Identifier les locaux hébergeant les équipements physiques du système

**Pour chaque local identifié :**

- Quels équipements y sont hébergés ? Quels sont leurs rôles/ utilités pour le système ?
- Dans quel bâtiment / site est il situé ?
- Quelles sont les natures de ses cloisons (toit, sol, murs, fenêtres, portes) ?
- Quels sont les locaux adjacents ? Dans quelle mesure sont-ils accessibles pour un attaquant ?
- Comment les accès sont contrôlés ?
- Quels dispositifs de surveillance et de détection d'intrusion sont en place ?
- Comment le contrôle d'accès est-il effzvvectué ?
- Par qui le local est-il fréquenté ? Pour quelles raisons ? A quelle fréquence ?

# Rôles et responsabilités

## Rôles et responsabilités 1/2

- **Identifier les rôles et responsabilités relatifs au système d'information**
  - Qui a autorité sur le système ?
  - Quels sont les utilisateurs du système ?

**Pour chaque composant du système :**

- Qui assure dans la gestion des habilitations ?
- Qui assure la maîtrise d'ouvrage ?
- Qui assure le développement et l'intégration ?
- Qui assure la production ?
- Qui assure le maintien en conditions opérationnelles et de sécurité (MCO / MCS)
- Quels sont les éditeurs logiciels et les constructeurs des matériels ?
- Quels composants sont externalisés (ex. Cloud, SaaS...) ? Quels sont les fournisseurs associés ?

# Rôles et responsabilités

## Les rôles et responsabilités 2/2

- Pour les locaux hébergeants les équipements matériels, qui assure leur entretien ?
- Pour les équipements matériels, qui assure leur transport ?

### Pour chaque entité identifiée

- Est-elle interne ou externe ?
- Quels sont les périmètres et frontières de ses responsabilités ?
- Quels sont ses privilèges d'accès logiques ?
- Quels sont ses privilèges d'accès physiques ?