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 l'épisode 3 de la série « EBIOS RM Dans la Pratique », intitulé « Une question de maîtrise ». 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 couvre 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

Les Fonctions

Identifier les fonctions et sous fonctions rendues par le système

Pour chaque fonction ou sous-fonction :

- Dans quel processus elle s'inscrit ?
- Quels sont les éléments entrant et sortant ?
- Quelles sont les données impliquées ?
- Quels composants applicatifs sont impliqués ? comment ?
- Qui y a accès et avec quels droits ?

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 identifié :

- Quelles sont les fonctions rendues ?
- Quelles sont les données manipulées ?
- Quelles sont les solutions logicielles sous-jacentes ?
- Sur quelle machine il s'exécute ? Avec quels droits ?
- Quelles sont ses interfaces d'interaction (IHM, réseau...) ? Qui peut y accéder ? Comment les accès sont-ils authentifiés ?
- Est-il en écoute sur des ports réseau ? Qui peut y accéder ? depuis quels réseaux ?
- Quelles sont les communications associées (en tant que source ou destination) ?
- Quelles sont les entités utilisatrices ?
- Quel est le modèle d'habilitation associé (qui a accès à quoi)?

Couche Applicative

Les Communications

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

Pour chaque communication identifiée :

- Source : Quel composant logiciel ? Sur quelle machine ? sur quelle interface réseau ?
- Destination : Quel composant logiciel ? Sur quelle machine ? sur quel port réseau ? Sur quelle interface réseau ?
- Quel est le protocole utilisé ?
- Quelles sont les réseaux et les interconnexions traversés ?
- Quelles sont les données transportées ?
- Dans quelle(s) fonction(s) cette communication est-elle impliquée ?

Infrastructure Système

Les Machines 1/2

Identifier les machines, physiques ou virtuelles, constituant le système

Pour chaque machine identifiée :

- Quel système d'exploitation ? Quelle version ?
- Le cas échéant, à quel domaine elle appartient ?
- Pour les serveurs windows, quels rôles sont activés ?
- Quels sont les logiciels et applicatifs installés ? Avec quels droits sont-il exécutés ?
- Quelles données y sont stockées ?
- Combien d'interfaces réseau ? A quel(s) réseau(x) sont-elles connectées ?
- A quels réseaux a-t-elle accès ? A-t-elle accès à Internet ?

Infrastructure Système

Les Machines 2/2

- Quels sont les usages associés (pour les postes de travail en particulier) ?
- Qui peut y accéder ? Avec quels droits ?
- Une prise en main à distance est-elle possible ? Via quel(s) services(s) (RDP, SSH...) ? Qui peut y accéder ? depuis quel(s) réseau(s) ?
- Quels sont les ports réseau ouverts ? Par quel logiciel/ service ? Qui peut y accéder ? Depuis quels réseaux ?
- Des partages réseau existent ? Avec quelles données ? Qui peut y accéder (en lecture ou en écriture) ?
- Si la machine est virtuelle, quelle est la machine hôte ? Quelle est la solution de virtualisation ?
- Si la machine est physique, à quel élément matériel est-elle associée ?

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 :

- Quels sont les équipements réseau associés ? Quels modèles et quelles versions ?
- Quelles machines y sont connectées ?
- Quelles interconnexions a-t-il avec les autres réseaux / sous-réseaux ?
- Quelles sont les règles de filtrage associées à chaque interconnexion ?

Infrastructure réseau

Les Réseaux 2/2

- Quels sont les points d'accès filaires (ex. prise RJ45) associés ? Où sont ils situés physiquement ? Qui peut y accéder ?
- Quels sont les points d'accès radio associés ? Quelle est leur zone de couverture ? Qui peut y accéder ? Comment les accès sont authentifiés ?
- Est-il accessible à distance par VPN ? Qui peut y accéder ? Depuis quel réseau ? Comment les accès sont authentifiés ?
- Quelles sont les services réseau associés : Passerelle, DNS, DHCP, Radius, Proxy, Reverse Proxy ? Sur quelles machines sont-ils installés ?

Equipements industriels

Les Capteurs & Les Actionneurs

Identifier tous les capteurs et actionneurs

Pour chaque équipement identifié :

- Quelle est sa fonction ?
- A quelle unité de calcul (automates, calculateurs...) est-il relié ? Par quel type de liaison ?
- Comment il communique ?

Equipements industriels

Les Unités de Calcul

- **Identifier toutes les unités de calcul terrain (automates, calculateurs…)**

  Pour chaque équipement identifié :

  - Quelles sont ses fonctions ?
  - A quel capteurs / actionneurs est-il connecté ?
  - Communique-t-il avec un système de contrôle commande ? Lequel ? Par quel protocole ? Il se comporte comme client ou serveur vis-à-vis de ce système ? Comment la communication est-elle authentifiée ?

Dispositif d'administration

Pour chaque composant identifié précédemment

- Par qui est-il administré ? Avec quels droits ?
- Est-il administré en local (à pied d'oeuvre) ou via le réseau ?
- Via quel interface/service est-il administré (ex. RDP, WinRM, SSH, Telnet...) ? Comment les accès sont authentifiés ?
- Via quelle interface réseau est-il administré ?
- Depuis quel poste est-il administré ?
- Depuis quels réseaux est-il administré ?
- Est-il administré au travers d'une machine de rebond ? Si oui laquelle ?
- Depuis quels réseaux l'interface/service d'administration est-il accessible ?
- Quels réseaux sont traversés par les flux d'administration ?
- Une télémaintenance est en place ? Qui peut y accéder ? avec quels droits ? Par quel canal ? Comment les accès sont-il authentifiés ?

Infrastructure matérielle et physique

Les Equipements

Identifier les équipements informatiques constituant le système

Pour chaque équipement identifié :

- Quelle est sa nature (Serveur, poste de travail, commutateur...) ?
- Quel est son modèle et sa version ?
- Dans quel(s) emplacement(s) physique(s) il se situe ?
- Est-il nomade ?
- Qui peut y accéder physiquement ?

Infrastructure matérielle et physique

Les Câbles

- **Identifier les câbles réseau composants le système**

Pour chaque câble identifié :

- A quel réseau physique il appartient ?
- A quels équipements est-il connecté ?
- Par où est-il acheminé ?
- Qui peut y accéder physiquement ?
- Le cas échéant, à quelle prise réseau est-il associé ?

Infrastructure matérielle et physique

Les Locaux

Identifier les locaux hébergeant les équipements physiques du système

Pour chaque local identifié :

- Quels équipements y sont hébergés ?
- Dans quel bâtiment / site est il situé ?
- Quelles sont les natures de ses cloisons (toit, sol, murs, fenêtres, portes) ?
- Quels sont les locaux adjacent ?
- Qui peut y accéder ?
- Comment le contrôle d'accès est-il effectué ?

Rôles et responsabilités

Les Parties Prenantes 1/2

Identifier les parties prenantes du système

- 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 Parties Prenantes 2/2

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

Pour chaque partie prenante identifiée

- Est-il interne ou externe ?
- Quels sont les périmètres et frontières de ses responsabilités ?
- Quels sont ses privilèges d'accès logique ?
- Quels sont ses privilèges d'accès physique ?