EBIOS RM dans la Pratique

Socle de sécurité

Mode opératoire pour constituer un socle basé sur le Guide d'Hygiène Informatique

v0.3

Ouvrir les autres pages

AMN BRAINS

amnbrains.com/blog

EBIOS RISK MANAGER

EBIOS RM dans la pratique

Présentation du document

Au titre de l'atelier 1 de la méthode EBIOS Risk Manager, ce document fournit un mode opératoire pour constituer un socle de sécurité, basé sur le **Guide d'Hygiène Informatique.**

Ce document fournit en particulier un guide pour :

- décliner, pour un système étudié, les règles du Guide d'Hygiène Informatique,
- identifier les menaces qu'il convient de considérer dans l'étude des risques, selon l'état de mise en oeuve de chaque règle.

Ce guide :

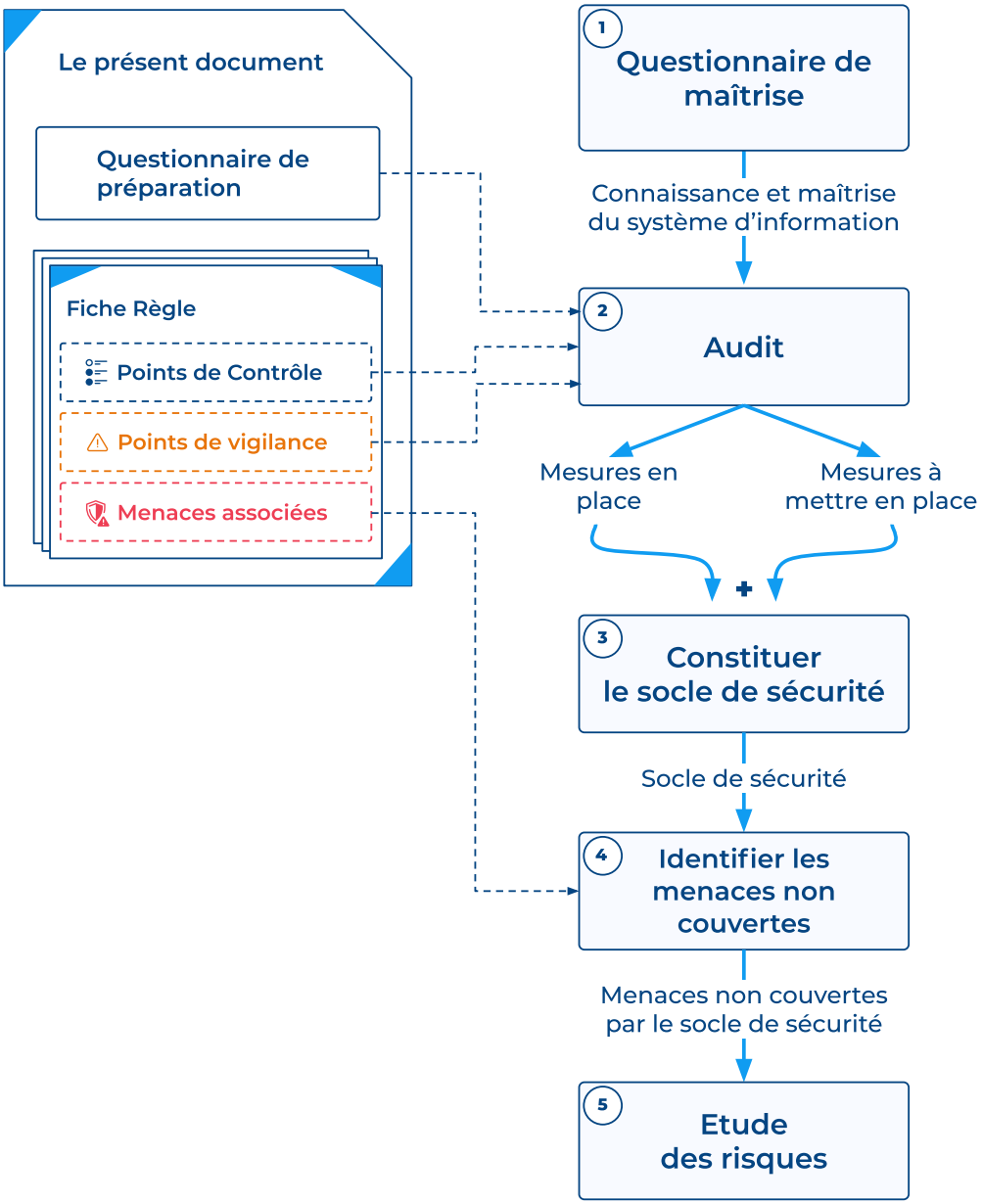
1. décrit le déroulement de l'activité de constitution d'un **socle de sécurité** basé sur le **Guide d'Hygiène**, en passant particulièrement par un **audit** de sécurité ;
2. et puis, pour chaque section du guide d'Hygiène :
    - fournit des instructions pour identifier les **éléments du système** étudié auxquels **s'applique** chaque **règle** de sécurité ;
    - détaille les **points de contrôle** extraits du descriptif de chaque règle,
    - fournit des **points de vigilance** à prendre en compte,
    - et liste les **menaces** qu'il convient de considérer dans l'étude des risques, selon l'état de mise en œuvre de chaque règle.

Ce guide est **utilisable** aussi bien :

- pour la définition d'un **socle de sécurité** basé sur le Guide d'hygiène Informatique,
- que pour réaliser un **audit** de sécurité par rapport à ce référentiel.

EBIOS RM dans la pratique

Mode opératoire



Le mode opératoire pour définir un socle de sécurité est décrit par la figure ci-dessus. Il se compose des étapes suivantes :

1 - Acquérir une maîtrise globale du système d'information

Pour ce faire, il convient de s'appuyer sur le questionnaire téléchargeable par ici.

2 - Auditer le système d'information par rapport au Guide d'Hygiène Informatique

Pour chaque section du Guide d'Hygiène Informatique :

- identifier et comprendre les éléments du système auxquels s'appliquent les règles de sécurité. Il convient pour ce faire de dérouler le questionnaire de la section « préparation » ;
- dérouler les points de contrôle disponibles dans la fiche de chaque règle ;
- porter une attention particulière aux points de vigilance indiqués dans la fiche de chaque règle.

3 - Constituer le socle de sécurité

Le "socle de sécurité" se constitue des :

- mesures de sécurité existantes identifiées par l'audit ;
- mesures retenues à mettre en place, issues des recommandations de l'audit.

4 - Déduire les menaces persistantes

Dans l'approche par les risques (atelier 4 en particulier), considérer les menaces indiquées dans la fiche de chaque règle, comme actions élémentaires.

Pour chaque menace, la fiche indique les conditions dans lesquelles elle doit être considérée, et ce en fonction :

- de l'environnement du système ;
- de l'état de mise en oeuvre de la règle ;
- et des recommandations retenues dans l'audit.

La version actuelle de ce document traite les sections “III”, "V" et "VI" du guide d’hygiène. `

Ce document sera progressivement enrichi afin de couvrir les autres sections du guide et sera publié sur notre blog amnbrains.com/blog.

III

AUTHENTIFIER ET CONTRÔLER LES ACCÈS

Partie 1

PRÉPARATION

Identifier les points d'accès "utilisateurs"

Considérer en particulier :

- L'ouverture des sessions sur les postes de travail
- Les accès aux répertoires réseaux
- Les accès web pour chaque application
- Les accès API (BackEnd) pour chaque application "client lourd" ou "mobile"
- Les accès à la messagerie
- Les accès au Proxy Internet
- Les accès filaires au réseau
- Les accès WIFI

Pour chaque point d'accès identifié :

- Identifier les populations y ayant accès
- Identifier les populations ayant réellement le besoin d'y accéder
- Identifier les profils d'accès et les droits associés

Identifier les points d'accès "administrateurs" (1/3)

- **Pour le SI d'administration, considérer en particulier :**
  - L'accès au réseau d'administration
  - L'ouverture de sessions sur les postes d'administration et les postes de maintenance
  - L'accès aux outils d'administration (Ex. Machines de rebonds)

Identifier les points d'accès "administrateurs" (2/3)

Pour les ressources à administrer, considérer en particulier :

Au niveau Système :

- L'accès administrateur, local ou distant, aux postes de travail utilisateurs
- L'accès administrateur, local ou distant, aux serveurs
- L'accès à l'administration de l'Active Directory
- L'interface d'administration, en local ou à distance, des hyperviseurs (virtualisation)
- Les cartes d'administration "bas niveau" des serveurs (ex. DELL IDRAC, HP ILO)

Au niveau Réseau :

- Les interfaces d'administration à distance des équipements réseau
- Les ports locaux d'administration des équipements réseau.

Au niveau Applicatif :

- Les interfaces de configuration des composants applicatifs (ex. Serveur d'application, serveurs de bases de données, services d'annuaires, ...)

Pour les équipements industriels (automates, calculateurs, ...) / objets connectés :

- Les interfaces de programmation et de configuration

Identifier les points d'accès "administrateurs" (3/3)

- **Pour chaque point d'accès "administrateur" identifié:**
  - Identifier les populations y ayant accès
  - Identifier les populations ayant réellement le besoin d'y accéder
  - Identifier les profils d'accès et les droits associés

Identifier les points d'accès "de services"

Considérer en particulier

- Les comptes de service sur les systèmes d'exploitation des serveurs
- Les accès API (ex. web services) inter-applicatifs
- Les accès applicatifs aux services supports (ex. Serveurs de bases de données, services d'annuaires, moteurs de recherche, ….)
- Les accès, dans un sens ou dans un autre, entre les équipements industriels / objets connectés et les serveurs de contrôle-commande.
- D'une manière générale, tout point d'accès "machine to machine"

Pour chaque point d'accès identifié :

- Identifier le(s) service qui y a/ont accès
- Identifier le(s) service qui a/ont réellement le besoin d'y accéder
- Identifier les droits d'accès associés

Partie 2

DÉCLINAISON DES RÈGLES

&

MENACES ASSOCIÉES

8 Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur

Points de contrôle extraits de la description de la règle

- Les comptes d'accès utilisateur doivent être nominatifs.
- L'utilisation de comptes génériques (ex : admin, user) doit être marginale et ceux-ci doivent pouvoir être rattachés à un nombre limité de personnes physiques.
- Les comptes génériques et de service doivent être gérés selon une politique au moins aussi stricte que celle des comptes nominatifs.
- Un compte d'administration nominatif, distinct du compte utilisateur, doit être attribué à chaque administrateur, avec des identifiants et secrets différents.
- Le compte d'administration, disposant de plus de privilèges, doit être dédié exclusivement aux actions d'administration.
- Le compte administrateur doit être utilisé sur des environnements dédiés à l'administration.
- Dès que possible la journalisation liée aux comptes (ex : relevé des connexions réussies/échouées) doit être activée.

Déclinaison de la règle pour le système étudié

- Pour tout **point d'accès "utilisateur"** identifié
- Pour tout **point d'accès "administrateur"** identifié
- Pour tout **point d'accès "service"** identifié

⚠ Points de vigilance

- Vérifier que les comptes "de service" sont maîtrisés et sont individuels par "service".
- Vérifier les mesures de traçabilité d'usage des comptes génériques, pour l'imputabilité des actions.

Menaces associées, à considérer dans l'étude des risques

- Abus de privilège non imputable, si un compte générique est utilisé, en fonction du niveau de confiance associé à la population en question.
- Le maintien des accès aux comptes génériques par des personnes qui n'ont plus le besoin d'y accéder, si le mot de passe n'est pas changé.
- En cas d'utilisation des comptes d'administration dans des tâches autres que l'administration et/ou sur des environnements non dédiés à l'administration :
  - ces comptes deviennent plus exposés et le risque de leur compromission augmente ;
  - en cas de compromission de la session de l'administrateur sur des tâches bureautiques ou lors d'un accès à Internet, l'attaquant obtient des privilèges d'administration sur le SI.

9 Attribuer les bons droits sur les ressources sensibles du système d'information

Points de contrôle extraits de la description de la règle

- Etablir une liste précise des ressources sensibles du système d'information.
- Définir pour chaque ressource sensible quelle population peut y avoir accès.
- Contrôler strictement l'accès à chaque ressource sensible, en s'assurant que les utilisateurs sont authentifiés et font partie de la population ciblée.
- Eviter sa dispersion et sa duplication à des endroits non maîtrisés ou soumis à un contrôle d'accès moins strict.
- Les répertoires des administrateurs regroupant de nombreuses informations sensibles doivent faire l'objet d'un contrôle d'accès précis.
- Les partages réseau contenant des informations sensibles doivent faire l'objet d'un contrôle d'accès précis.
- Une revue régulière des droits d'accès doit être réalisée afin d'identifier les accès non autorisés.

Déclinaison de la règle pour le système étudié

- Pour tout **point d'accès "utilisateur"** identifié
- Pour tout **point d'accès "administrateur"** identifié
- Pour tout **point d'accès "service"** identifié

⚠ Points de vigilance

- Pour chaque ressource et chaque population concernée, comparer les droits attribués avec les besoins réels.
- Attention particulière au droit "administrateur de domaine Windows".
- Ne pas négliger les droits des comptes de service.
- Ne pas négliger les droits d'accès au réseau.
- Attention particulière aux droits d'administration OS pour les comptes utilisateurs et les comptes de service.

Menaces associées, à considérer dans l'étude des risques

- L'absence d'une liste précise des ressources sensibles et des droits associés entraîne un manque de maîtrise des populations qui y ont accès. Cela donne généralement lieu à des droits d'accès illégitimes.
- Abus de privilège, en fonction du niveau de confiance associé à la population concernée.
- Exploitation des privilèges d'une victime depuis sa machine compromise.
- Exploitation des privilèges d'une victime en cas d'usurpation d'identité.
- Exploitation des privilèges du compte de service d'un logiciel compromis.
- Accès illégitime si le point d'accès en question ne supporte pas d'authentification, en fonction de son exposition réseau et/ou physique.
- Accès malveillant exploitant des droits illégitimes, si la procédure d'attribution, de réexamen et de revue des droits n'est pas suffisamment maîtrisée.

10 Définir et vérifier des règles de choix et de dimensionnement des mots de passe

Points de contrôle extraits de la description de la règle

- Respecter les règles et bonnes pratiques énoncées par l'ANSSI en matière de choix et de dimensionnement des mots de passe.
- Sensibiliser les utilisateurs aux :
  - règles de choix et de dimensionnement des mots de passe et aux risques liés au choix d'un mot de passe qui serait trop facile à deviner;
  - risques liés à la réutilisation de mots de passe d'une application à l'autre et plus particulièrement entre messageries personnelles et professionnelles.
- Mettre en oeuvre un blocage des comptes à l'issue de plusieurs échecs de connexion.
- Désactiver les options de connexion anonyme.
- Utiliser un outil d'audit de la robustesse des mots de passe.

Déclinaison de la règle pour le système étudié

- Pour tout **point d'accès "utilisateur"** identifié
- Pour tout **point d'accès "administrateur"** identifié

⚠ Points de vigilance

- Vérifier si la politique des mots de passe comprend une interdiction des mots de passe des dictionnaires d'attaques ou des bases de fuites.
- Vérifier si cette politique est imposée techniquement.
- Vérifier si un contrôle du respect de la politique est réalisé (dans le cas où elle n'est pas imposée techniquement).

Menaces associées, à considérer dans l'étude des risques

- Vol/prédiction du mot de passe si :
  - la politique de complexité n'est pas suffisamment robuste ;
  - ou la politique de complexité n'est pas imposée techniquement et que les utilisateurs ne sont pas suffisamment sensibilisés à la respecter.
- Attaques par dictionnaire si une vérification n'est pas effectuée.
- Attaque par brute-force, en l'absence d'un mécanisme de verrouillage.
- Vol / prédiction du mot de passe dans la procédure de première génération si :
  - le mot de passe généré n'est pas aléatoire ;
  - il est transmis à l'utilisateur de manière non sécurisée ;
  - et/ou il n'est pas changé à la première utilisation.
- Interception du mot de passe sur le réseau s'il est transmis dans un flux non sécurisé.
- Fuite depuis des systèmes non sécurisés, si les utilisateurs ne sont pas suffisamment sensibilisés à ne pas réutiliser les mêmes mots de passe.

11 Protéger les mots de passe stockés sur les systèmes

Points de contrôle extraits de la description de la règle

- Les mots de passe des utilisateurs doivent impérativement être protégés au moyen de solutions sécurisées au premier rang desquelles figurent l'utilisation d'un coffre-fort numérique et le recours à des mécanismes de chiffrement.
- Le choix d'un mot de passe pour ce coffre-fort numérique doit respecter les règles énoncées précédemment et être mémorisé par l'utilisateur, qui n'a plus que celui-ci à retenir.

Déclinaison de la règle pour le système étudié

- Pour tout **point d'accès "utilisateur"** identifié
- Pour tout **point d'accès "administrateur"** identifié

⚠ Points de vigilance

RAS

Menaces associées, à considérer dans l'étude des risques

- Vol du mot de passe depuis un support de stockage, si celui-ci n'est pas suffisamment sécurisé
- Fuite groupée des mots de passe depuis le coffre fort, en fonction du niveau de sécurité de celui-ci et du niveau de sensibilisation des utilisateurs à la sécurité du mot de passe associé.

12 Changer les éléments d'authentification par défaut sur les équipements et services

Points de contrôle extraits de la description de la règle

- Les éléments d'authentification par défaut des composants du système doivent donc être modifiés dès leur installation.
- Procéder au renouvellement régulier des éléments d'authentification des comptes par défaut.

Déclinaison de la règle pour le système étudié

- Pour tout **point d'accès "utilisateur"** identifié
- Pour tout **point d'accès "administrateur"** identifié
- Pour tout **point d'accès "de service"** identifié

⚠ Points de vigilance

- Attention particulière aux ports/interfaces d'administration utilisés pour le secours.

Menaces associées, à considérer dans l'étude des risques

- Accès illégitime si un compte par défaut n'est pas ou ne peut pas être supprimé ou changé

13 Privilégier lorsque c'est possible une authentification forte

Points de contrôle extraits de la description de la règle

- Mettre en œuvre une authentification forte nécessitant l'utilisation de deux facteurs d'authentification.
- Mettre en œuvre une authentification forte, utilisant des cartes à puces ou, à défaut, les mécanismes de mots de passe à usage unique avec jeton physique.

Déclinaison de la règle pour le système étudié

- Pour tout **point d'accès "utilisateur"** identifié
- Pour tout **point d'accès "administrateur"** identifié

⚠ Points de vigilance

Considérer en particulier :

- les points d'accès exposés logiquement; accessible depuis Internet ou depuis des réseaux tiers non fiables.
- les points d'accès exposéS physiquement (ex. équipements terrain).
- Vérifier que le facteur d'authentification « que je possède » ou « que je suis » n'est pas reproductible facilement.

Menaces associées, à considérer dans l'étude des risques

- Cf. Règle 10
- Vol / Reproduction des facteurs d'authentification, en fonction de leurs natures, de leur durcissement et du niveau de sensibilisation des utilisateurs.

V

SÉCURISER LE RÉSEAU

Partie 1

PRÉPARATION

Les segments constituant le réseau

- **Identifier les segments constituant le réseau;**
- **Pour chaque segment identifié :**
  - Identifier les interconnexions avec les autres réseaux, internes ou externes (y compris le routage inter-vlan) Pour chaque interconnexion identifiée :
    - Quelles règles de filtrage sont appliquées ?
    - Quels sont les flux légitimes ?
  - Identifier les machines et équipements actifs qui y sont connectées ;
  - Evaluer le niveau de sensibilité de chaque équipement connecté ;
  - Etudier les éventuelles fragilités que chaque équipement peut présenter pour le segment réseau :
    - accessibilité depuis Internet ou depuis un réseau non fiable ;
    - exposition physique (zone publique, open-space, équipement terrain, ...);
    - Accessibilité par un personnel non fiable;
    - vulnérabilités non corrigées... etc.

Les points d'accès au réseau (1/2)

- **Identifier les points d'accès filaire (ex. Prise RJ45). Pour chaque point d'accès identifié :**
  - A quel segment réseau donne-t-il accès ?
  - Où est-il situé physiquement ?
  - Qui peut y accéder ?
  - Qui a le besoin d'y accéder ?
  - Les accès sont-il authentifiés (ex. 802.1x) ? Comment ?
- **Identifier les points d'accès WIFI. Pour chaque point d'accès identifié :**
  - A quel segment réseau donne-t-il accès ?
  - Quelles sont les bornes WIFI associées ? Où sont-elle situées physiquement ? Qui peut y accéder ?
  - Quelle est la zones de couverture physique du signal WIFI ? Qui peut y accéder ? Qui a besoin d'y accéder ?
  - Comment les accès sont-ils authentifiés ?

Les points d'accès au réseau (2/2)

- **Identifier les points d'accès distant (VPN) :**
  - Site-To-Site ou Client-To-Site ?
  - Quel est l'équipement de terminaison ?
  - Depuis quels réseaux est il accessible ?
  - Depuis quels locaux est il accessible ?
  - Qui peut y accéder ?
  - Qui a le besoin d'y accéder ?
  - A quel segment réseau donne-t-il accès ?
  - Comment les accès sont-ils authentifiés ?

Identifier les communications

- **Identifier les communications, au sein du système ou avec l'extérieur.**
- **Pour chaque communication identifiée :**
  - Quel est son niveau de sensibilité ?
  - Source : Quel composant logiciel ? Sur quelle machine ? Sur quelle interface réseau ? Dans quel réseau ?
  - Destination : Quel composant logiciel ? Sur quelle machine ? Sur quelle interface réseau ? Dans quel réseau ?
  - Quel est le protocole utilisé ?
  - Comment est-elle sécurisée, en confidentialité, en intégrité et en authenticité ?

Partie 2

DÉCLINAISON DES RÈGLES

&

MENACES ASSOCIÉES

19 Segmenter le réseau et mettre en place un cloisonnement entre ces zones

Points de contrôle extraits de la description de la règle

- Segmenter le réseau et mettre en place un cloisonnement entre ces zones.

Déclinaison de la règle pour le système étudié

- Pour tout **réseau ou sous-réseau** identifié

⚠ Points de vigilance

- Les machines présentant une fragilité pour le réseau (cf. Section « Préparation ») doivent être cloisonnées, plus particulièrement:
  - Les machines exposées physiquement (zone publique, Open-Space, équipement terrain, ...);
  - Les machines accessibles depuis des réseau non fiables (VPN, Partenaire, ...);
  - Les machines accessibles par un personnel non fiable;
  - Les machines ayant des vulnérabilités non corrigées,
- Les machines particulièrement sensibles (métier ou d'infrastructure) doivent être cloisonnées selon leur niveau de sensibilité.
- Le routage inter-vlan doit être traité comme interconnexion et doit être filtré en conséquence (par pare-feu).

Menaces associées, à considérer dans l'étude des risques

- Mouvements latéraux et propagation facile des attaques en cas d'un réseau à plat ou d'une faible segmentation.
- Exploitation malveillante de flux légitimes autorisés depuis des réseau non fiables.
- Rebond depuis une machine compromise vers les machines voisines du même segment réseau.
- Rebond depuis une machine compromise vers d'autres machines dans d'autres segments en exploitant un flux légitime autorisé.

20 S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages

Points de contrôle extraits de la description de la règle

- Filtrer et restreindre au minimum nécessaire les flux en provenance des postes connectés au réseau d'accès Wi-Fi.
- Mettre en œuvre un chiffrement robuste des communications WIFI (mode WPA2, algorithme AES CCMP).
- Mettre en œuvre une authentification des accès WIFI, centralisée, si possible par certificats clients des machines.
- Administrer les points d'accès de manière sécurisée (ex : interface dédiée, modification du mot de passe administrateur par défaut).
- Séparer les connexions WIFI des terminaux personnels ou visiteurs de celles des terminaux de l'entité.

Déclinaison de la règle pour le système étudié

- Pour tout **réseau WIFI** identifié

⚠ Points de vigilance

- S'assurer que l'accès WIFI en question est indispensable.
- Porter une attention particulière à la zone de couverture physique du signal WIFI. La méthode d'authentification doit être choisie en conséquence.
- Le mode WPA-PSK est à éviter en environnement professionnel. Dans le cas inverse, s'assurer que la clé est changée régulièrement.
- S'assurer de l'authentification de la borne WIFI auprès du terminal (pour éviter les fausses bornes) et non seulement l'inverse.

Menaces associées, à considérer dans l'étude des risques

- Augmentation de la surface d'attaque par la simple utilisation d'un réseau WIFI (exposé de par sa nature).
- Accès illégitime depuis des zones publiques couvertes par le signal WIFI.
- En cas d'utilisation du mode WPA-PSK :
  - accès illégitime par une personne qui a quitté l'organisation et qui possède la clé partagée;
  - possibilité d'intercepter et de déchiffrer toutes les communications par tout équipement ayant accès au même réseau.
- Exploitation d'éventuelles vulnérabilités logicielles au niveau des bornes WIFI pour accéder au réseau.
- En cas d'absence d'authentification de la borne auprès du terminal : connexion automatique à des bornes malveillantes avec le même SSID

21 Utiliser des protocoles réseaux sécurisés dès qu'ils existent

Points de contrôle extraits de la description de la règle

- Utiliser des protocoles réseaux sécurisés dès qu'ils existent.

Déclinaison de la règle pour le système étudié

- Pour toute **communication, interne ou externe** identifiée

⚠ Points de vigilance

- Porter une attention particulière à l'authentification mutuelle au niveau des communications machine-to-machine, souvent négligées.
- S'assurer de la gestion correcte des clés cryptographiques.
- S'assurer de l'utilisation/imposition de suites cryptographiques avec un niveau de sécurité acceptable.
- S'assurer que les certificats auto-signés sont proscrits, même pour les services internes.
- S'assurer de l'utilisation d'une version sécurisée de TLS.
- S'assurer de la sensibilisation des utilisateurs au traitement des avertissements du navigateur en cas de certificat invalide.
- S'assurer de la vérification de la validité des certificats dans les communications machine-to-machine (assez souvent négligée)

Menaces associées, à considérer dans l'étude des risques

- Interception des flux et écoute passive des communications si elles ne sont pas protégées en confidentialité.
- Interception des flux et altération des communications si elles ne sont pas protégées en intégrité et en authenticité.
- Par défaut, TLS n'assure que l'authentification du serveur. Si l'authentification mutuelle n'est pas activée, et en l'absence d'une authentification au niveau applicatif, une usurpation d'identité du client auprès du serveur est possible.
- Man-In-The-Middle dans une communication HTTPs et déchiffrement puis rechiffrement du flux. La probabilité de réussite d'une telle attaque dépend de la sensibilisation de l'utilisateur au traitement des avertissements du navigateur.

22 Mettre en place une passerelle d'accès sécurisé à Internet

Points de contrôle extraits de la description de la règle

- Filtrer les accès à internet au travers d'un pare-feu.
- Mettre en œuvre un serveur mandataire d'accès à Internet (Proxy).
- Mettre en œuvre une authentification des utilisateurs au niveau du serveur mandataire (proxy) d'accès à Internet.
- Mettre en œuvre une traçabilité des requêtes au niveau du serveur mandataire (proxy) d'accès à Internet.
- Mettre en œuvre une analyse antivirus du contenu au niveau du serveur mandataire (proxy) d'accès à Internet.
- Mettre en œuvre un filtrage par catégories d'URLs au niveau du serveur mandataire (proxy) d'accès à Internet.
- Mettre en œuvre des procédures de maintien en condition de sécurité des équipements de la passerelle d'accès à Internet.
- Mettre en œuvre une redondance des équipements de la passerelle d'accès à Internet, suivant le nombre de collaborateurs et le besoin de disponibilité.
- Déléguer les résolutions DNS de noms de domaines publics au serveur mandataire et désactiver les résolutions en direct.
- Les postes nomades établissent au préalable une connexion sécurisée au système d'information de l'entité pour naviguer sur le Web à travers la passerelle.

Déclinaison de la règle pour le système étudié

- Pour tout **point d'accès à Internet** depuis le réseau Interne

⚠ Points de vigilance

- Etudier la mise en place d'une interception TLS au niveau du serveur mandataire afin de pouvoir analyser les contenus chiffrés.
- Si une interception TLS est en place, s'assurer que les utilisateurs en sont explicitement informés.
- S'assurer que les sites de confiance et particulièrement sensibles (ex. sites bancaires) sont exclus de l'interception TLS.
- Si les communications Https sont déchiffrées au niveau du serveur mandataire, s'assurer que celle-ci valide le certificat serveur.
- S'assurer que les règles de cloisonnement et de filtrage ne permettent pas de contourner le serveur mandataire.

Menaces associées, à considérer dans l'étude des risques

- En l'absence de filtrage d'URL et d'analyse antivirus du contenu web, accès utilisateur à des pages malveillantes et infection du terminal (à considérer en fonction du niveau de sécurité de ce dernier)
- En l'absence d'authentification d'accès à Internet ou de la traçabilité de cet accès :
  - perte des traces d'attaque impliquant des accès à Internet
  - perte du pouvoir dissuasif contre les abus des utilisateurs relatifs aux accès à Internet
- En l'absence de redondance de la passerelle, incident d'indisponibilité de celle-ci et coupure totale de l'accès à Internet.
- Perte de maîtrise des accès à internet depuis les postes nomades si l'établissement préalables d'une connexion vers le réseau interne n'est pas obligatoire.
- Interception de l'ensemble des flux en cas de compromission du serveur mandataire. Les flux sont en clair si l'interception TLS est activée.

23 Cloisonner les services visibles depuis Internet du reste du système d'information

Points de contrôle extraits de la description de la règle

- Faire administrer les services et infrastructures visibles depuis internet par des administrateurs compétents, formés de manière continue (à l'état de l'art des technologies en la matière) et disponibles.
- Privilégier le recours à un hébergement externalisé auprès de professionnels.
- Cloisonner physiquement les infrastructures d'hébergement Internet des infrastructures internes du système d'information.
- Mettre en place une infrastructure d'interconnexion de ces services avec Internet permettant de filtrer les flux.
- Filtrer les flux liés à ces services Internet de manière distincte des autres flux de l'entité.
- Imposer le passage des flux entrants depuis Internet par un serveur mandataire inverse (reverse proxy).
- Le serveur mandataire inverse (reverse proxy) des flux entrants depuis Internet embarque différents mécanismes de sécurité.

Déclinaison de la règle pour le système étudié

- Pour toute **machine accessible directement depuis internet**
- Pour toute **machine accessible indirectement depuis Internet** (accessible par une machine accessible depuis Internet)

⚠ Points de vigilance

- Les communications initiées depuis une DMZ vers le réseau interne doivent être proscrites. Cela suppose que pour un service accessible depuis Internet, toute la chaîne doit être positionnée en DMZ, et non seulement le reverse proxy ou le front-end.
- Si un service en DMZ utilise un dépôt de données interne, s'assurer que celui-ci est répliqué dans la DMZ pour éviter les communications vers le réseau interne.
- Architecture non sécurisée à éviter : mettre un reverse proxy en DMZ qui re-route les requêtes vers le réseau interne.
- S'assurer que les règles de cloisonnement et de filtrage empêche le contournement du reverse proxy.

Menaces associées, à considérer dans l'étude des risques

- L'absence de filtrage des accès depuis internet augmente la surface d'attaque au niveau de ces services et ainsi la probabilité qu'ils soient compromis.
- En cas d'utilisation du même pare-feu pour le filtrage des flux Internet et des flux internes :
  - un dénis de service depuis Internet contre ce pare-feu impacterait aussi bien les flux internes qu'externes ;
  - la compromission depuis Internet du pare-feu externe donnerait accès au réseau interne.
- Un service visible depuis internet est potentiellement compromis :
  - En l'absence de cloisonnement, un mouvement latéral vers le réseau Interne serait possible ;
  - En cas d'un flux ouvert depuis la DMZ vers le réseau interne, celui-ci pourrait être exploité dans un mouvement latéral vers le réseau interne.

24 Protéger sa messagerie professionnelle

Points de contrôle extraits de la description de la règle

- Sensibiliser les utilisateur aux vecteurs d'infection provenant de la messagerie et aux moyens de prévention.
- Mettre en place des mesures organisationnelles pour se prémunir d'escroqueries (ex : demande de virement frauduleux émanant vraisemblablement d'un dirigeant) exploitant la messagerie.
- Proscrire la redirection de messages professionnels vers une messagerie personnelle.
- Disposer d'un système d'analyse antivirus en amont des boîtes aux lettres.
- Activer le chiffrement TLS des échanges entre serveurs de messagerie (de l'entité ou publics) ainsi qu'entre les postes utilisateur et les serveurs hébergeant les boîtes aux lettres.
- Mettre en place un serveur relai, en coupure d'Internet, pour ne pas exposer directement les serveurs de boîte aux lettres.
- déployer un service anti-spam au niveau de la messagerie.
- Mettre en place des mécanismes de vérification d'authenticité et configurer les enregistrements DNS publics liés à son infrastructure de messagerie (MX, SPF, DKIM, DMARC).

Déclinaison de la règle pour le système étudié

- Pour tout **service de messagerie** identifié

⚠ Points de vigilance

- S'assurer de la mise en oeuvre de procédures et de dispositifs de chiffrement et de signature des mails sensibles.

Menaces associées, à considérer dans l'étude des risques

- La sensibilisation des utilisateurs contribue à la réduction des attaques de phishing, mais les chances de réussite d'une telle attaque reste malheureusement très importantes.
- Les attaques de phishing ciblé sont difficile à éviter, même pour les utilisateur les plus prudents, voire experts.
- En cas d'activation de TLS, il est à noter que cela se limite aux communications impliquant le serveur de mail interne. Rien ne garantit le chiffrement sur toute la chaine depuis l'émetteur vers le destinataire. Une interception des mails en claire sur Internet reste possible.
- Fuite de données confidentielles par le biais de transferts vers des messageries non maîtrisées, s'ils ne sont pas interdits.
- L'absence d'un système d'analyse antivirus au niveau de la messagerie augmente les chances de réussite d'attaque de phishing avec pièce jointe malveillante.
- L'exposition directe sur Internet du serveur de messagerie augmente la surface d'attaque contre celui-ci et facilite l'exploitation d'éventuelles vulnérabilités.
- L'absence d'enregistrements SPF facilite l'envoi de mails frauduleux en usurpation des adresses issues du nom de domaine de l'organisme.
- Il n'est pas garanti que les récepteurs vérifient l'enregistrement SPF. Ils ne sont pas dans ce cas protégés contre les mails frauduleux usurpant des adresses issues du nom de domaine de l'organisme.
- Certains tiers n'ont pas d'enregistrements SPF. Il n'est pas possible dans ce cas de vérifier l'expéditeur, ce qui expose à des mails frauduleux usurpants des adresses issues des noms de domaine des tiers en question.

25 Sécuriser les interconnexions réseau dédiées avec les partenaires

Points de contrôle extraits de la description de la règle

- Interconnexion sur Internet - Etablir un tunnel site à site, de préférence IPsec, en respectant les préconisations de l'ANSSI.
- Effectuer un filtrage à l'aide d'un pare-feu au plus près de l'entrée des flux sur le réseau de l'entité.
- L'équipement de filtrage IP pour les connexions partenaires est dédié à cet usage.
- Mettre en oeuvre un équipement de détection d'intrusion au niveau des connexions partenaires.
- Identifier un point de contact à jour chez le partenaire pour pouvoir réagir en cas d'incident de sécurité.

Déclinaison de la règle pour le système étudié

- Pour toute **interconnexion avec un réseau d'un tiers**

⚠ Points de vigilance

- Selon le niveau de fiabilité du réseau du partenaire, envisager la mise en oeuvre d'une DMZ pour se protéger des menace provenant de celui-ci.
- S'assurer que l'accessibilité de l'interconnexion du côté du réseau tiers est restreinte au strict nécessaire.
- Si seul un nombre très limité de postes utilisent cet accès distant, privilégier un tunnel client-à-site.

Menaces associées, à considérer dans l'étude des risques

- L'absence de filtrage et de dispositif de détection au niveau de l'interconnexion avec un partenaire augmentent la surface d'attaque depuis un réseau non maîtrisé :
  - Attaque par rebond depuis le réseau du partenaire ;
  - Attaque par des sources de risques présentes dans le réseau du partenaire.
- Un flux légitime depuis le réseau du partenaire pourrait être exploité pour s'introduire dans le réseau. Menace à considérer en fonction de la fiabilité du réseau du partenaire, et de l'accessibilité de l'interconnexion.

VI

SÉCURISER L'ADMINISTRATION

Partie 1

PRÉPARATION

Ressources à administrer (1/3)

- **Identifier tous les composants du système d'information**
  - Couvrir toutes les couches du système d'information :
    - Equipements matériels,
    - Infrastructure réseau,
    - Infrastructure système,
    - Composants applicatifs.
  - Se service du questionnaire de maîtrise téléchargeable par ici
  - Porter une attention particulière aux composants les plus senibles

Ressources à administrer (2/3)

- **Pour chaque composant identifié :**
  - Identifier, de manière exhaustive, toutes ses interfaces d'administration et de configuration (RDP, WinRM, Admin Shares, WMI, SSH, Telnet, CLI, ...) ;
  - Pour chaque interface identifiée :
    - Est-elle accessible via le réseau ou à pied œuvre ?
    - Elle utilise quel protocole ?
    - Elle est accessible sur quel port ? Sur quelle interface réseau ?
    - Elle est accessible depuis quel(s) réseau(x) ?
    - Comment les accès sont authentifiés ?
    - Quels sont les profils d'accès disponibles ?

Ressources à administrer (3/3)

- **Pour chaque composant identifié :**
  - Identifier tous les administrateurs / mainteneurs
  - Pour chaque administrateur ou profil d'administrateur identifié :
    - Quelles tâches sont réalisées ?
    - Quels droits sont nécessaires pour réaliser ces tâches ?
    - Quels droits ont-ils réellement ?
  - Identifier le(s) poste(s) utilisés pour l'administration
  - Identifier les serveurs d'outils d'administration utilisés

Ressources d'administration

- **Identifier tous les postes d'administration ou de maintenance.**
- **Pour chaque poste ou poste type identifié :**
  - Est-il dédié à l'administration ?
  - Est-il utilisé pour l'administration via le réseau ou en local à pied d'oeuvre ?
  - Quelles ressources sont administrées via ce poste ?
  - Est-il accessible à distance ? Si oui, depuis où et comment?
- **Identifier les serveurs d'outils d'administration**
- **Pour chaque serveurs identifié :**
  - Quelles ressources sont administrées via ce serveur ?
  - Comment est-il accessible ?
  - Depuis quels postes est-il accessible ? Depuis quel(s) réseau (s)

Ressources d'administration

- **Identifier les réseaux auxquels sont connectés les postes et serveurs utilisés pour l'administration**
- **Pour chaque réseau identifié :**
  - Est-il physique ou logique ?
  - Comment est-il cloisonné ?
  - Quelles sont ses interconnexions ?
  - Quelles sont les règles de filtrage au niveau de chaque interconnexion ?
  - Est-il dédié à l'administration ?
  - Qui peut y accéder ?
  - Quelles machines y sont connectées ?
  - Quel est le chemin réseau utilisé pour accéder aux ressources à administrer ? Ce chemin est-il dédié à l'administration ?

Télémaintenance

- **Identifier les dispositifs de télémaintenance**
- **Pour chaque télémaintenance identifiée :**
  - Identifier le mainteneur en question ;
  - Identifier le(s) composant(s) concerné(s) par la télémaintenance ;
  - Identifier l'architecture du chemin d'accès depuis le réseau du mainteneur vers le composant maintenu ;
  - Identifier les postes utilisés pour la télémaintenance.

Partie 2

DÉCLINAISON DES RÈGLES

&

MENACES ASSOCIÉES

27 Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système

Points de contrôle extraits de la description de la règle

- Un poste de travail ou un serveur utilisé pour les actions d'administration ne doit en aucun cas avoir accès à Internet
- Pour les usages nécessitant Internet, mettre à disposition des administrateurs un poste de travail distinct ou, à défaut, une infrastructure virtualisée distante pour la bureautique accessible depuis un poste d'administration
- L'accès distant à une infrastructure d'administration depuis un poste bureautique est déconseillée
- Les mises à jour logicielles des équipements administrés doivent être récupérées depuis une source sûre, contrôlées puis transférées, via un support amovible dédié ou une zone d'échange, sur le poste ou le serveur d'administration.

Déclinaison de la règle pour le système étudié

- Pour tout **poste** utilisé pour **l'administration** ou la **maintenance**
- Pour tout **serveur** utilisé pour **l'administration** ou la **maintenance**

⚠ Points de vigilance

- Porter une attention particulière à la télémaintenance qui nécessite une connexion internet. Dans ce cas :
  - L'accès doit s'effectuer au travers d'un VPN et puis d'un Bastion d'administration
  - Chaque accès au VPN et/ou au Bastion doit faire l'objet d'une autorisation explicite par un administrateur local
  - Le poste de télémaintenance doit être dédié à l'administration ou, si possible, à l'administration du SI en question
  - La seule connexion internet possible depuis le poste de télémaintenance doit être la liaison VPN vers le SI en question
  - Seul le composant concerné par cette télémaintenance doit être accessible par cette télémaintenance
- En cas de transfert de fichiers vers un poste ou serveur d'administration par le biais d'un support amovible :
  - Imposer techniquement la désinfection de celui-ci par une station blanche
  - vérifier l'intégrité du fichier en question par rapport à son origine avant l'import
- Si une zone d'échange est en place :
  - Il convient de l'équiper d'un dispositif anti-malware
  - il convient de l'équiper d'un dispositif de vérification de l'intégrité des fichiers transféré par rapport à leur origine
  - L'accès initié depuis la zone d'échange vers le poste ou le serveur d'administration doit être interdit.

Menaces associées, à considérer dans l'étude des risques

- Si un poste ou un serveur d'administration a accès à Internet : Infection potentielle du poste ou du serveur d'administration et rebond vers les ressources administrées en abusant des droits de l'administrateur en question
- Si un poste ou un serveur d'administration est accessible depuis un poste bureautique : Infection potentielle du poste bureautique et rebond vers le poste ou le serveur d'administration et puis rebond vers les ressources administrées
- Si un poste de télémaintenance se connecte à Internet : Infection potentielle du poste de télémaintenance et rebond vers le poste ou le serveur d'administration ou vers les vers les ressources administrées selon l'architecture de télémaintenance
- Infection par le biais de fichiers importés dans le poste/serveur d'administration. Le risque est plus important en l'absence de de désinfection et de vérification de l'intégrité et de l'authenticité des fichiers.

28 Utiliser un réseau dédié et cloisonné pour l'administration du système d'information

Points de contrôle extraits de la description de la règle

- Privilégier en premier lieu un cloisonnement physique des réseaux d'administration
- À défaut, mettre en œuvre un cloisonnement logique cryptographique reposant sur la mise en place de tunnels IPsec
- Au minimum, mettre en œuvre un cloisonnement logique par VLAN.

Déclinaison de la règle pour le système étudié

- Pour toute **interface d'administration** d'une ressource administrée
- Pour tout **poste** ou **serveur d'administration**

⚠ Points de vigilance

- Considérer tous les composants du système d'information, avec une attention particulière aux composants les plus sensibles
- S'assurer que les interfaces d'administration des ressources administrées sont accessibles exclusivement depuis le réseau d'administration. L'interface d'administration peut être en écoute :
  - de préférence, sur une interface réseau physique d'administration, connectée au réseau d'administration ;
  - à défaut, sur une interface réseau virtuelle d'administration, associée à un Vlan d'administration ;
  - ou sur l'interface de production, avec un filtrage système et réseau qui la rend accessible uniquement depuis le réseau d'administration.
- Une machine virtuelle doit être administrée aux travers d'une interface réseau virtuelle dédiée à l'administration, connectée au réseau d'administration par le biais d'une interface réseau physique d'administration de la machine hôte.
- La compromission d'une ressource administrée ne doit pas permettre de remonter vers les postes ou serveurs d'administration.
- La compromission d'une ressource administrée ne doit pas permettre de rebondir vers les interfaces d'administration des autres ressources administrées.
- Il est à noter que pour certains composants, il est difficile de séparer les flux d'administration des flux de production. Il est en particulier le cas de l'Active Directory..

Menaces associées, à considérer dans l'étude des risques

- En l'absence d'un cloisonnement des interfaces d'administration, accès illégitime aux interfaces d'administration par une source de risque présentes dans les réseaux de production, relativement exposés comparés au réseau d'administration.
- En l'absence d'un cloisonnement entre les ressources d'administration et les ressources à administrer, la compromission d'une machine permettrait à un attaquant de rebondir, au travers de son interface réseau d'administration, vers les postes et serveurs d'administration.
- En l'absence d'un cloisonnement entre les ressources à administrer, la compromission d'une machine permettrait à un attaquant de rebondir, au travers de son interface réseau d'administration, vers les interfaces d'administration des autres ressources du SI.

29 Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail

Points de contrôle extraits de la description de la règle

- Proscrire, par défaut, les droits d'administration des utilisateurs sur les postes de travail
- Mettre en oeuvre une procédure d'attribution de droit d'administration temporaires, sur les poste de travail, pour des besoins nécessaires de l'utilisateur

Déclinaison de la règle pour le système étudié

- Pour tout **tout poste de travail**

⚠ Points de vigilance

- Si l'usage du poste de travail se limite à une seule application (ex. pour un SI industriel), mettre en place un mode kiosque
- S'assurer que les outils de scripting (cmd, powershell, ...) sont désactivés
- L'utilisateur ne doit pas pouvoir démarrer le poste de travail sur un autre système d'exploitation (avec un disque d'amorçage).

Menaces associées, à considérer dans l'étude des risques

- Si l'utilisateur dispose de droits d'administration sur son poste de travail :
  - il risque d'installer des logiciels malveillant à son insu (phishing, cheval de Troie, ...)
  - En cas de prise de contrôle de sa session (ex. suite à une attaque de phishing, suite au branchement d'un clavier malveillant, ...) l'attaquant/malware aura également des droits d'administration sur le poste
  - Si l'utilisateur est malveillant, ces droits d'administration le rendent plus dangereux (installation d'outil d'attaque, extraction de données, ...).
- Profitant de son accès physique à la machine, et sans droits d'administration, un utilisateur malveillant :
  - peut démarrer sur un disque d'amorçage, si une protection n'est pas en place, et puis modifier les exécutable et les configurations de l'OS
  - peut extraire le disque de l'ordinateur et modifier les exécutable les configurations de l'OS
  - peut s'attaquer aux microcodes des puces électroniques de l'ordinateurs pour modifier leurs comportement en sa faveur.