RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

DÉFENSE EN PROFONDEUR – MISE EN ŒUVRE

La mise en œuvre du principe de défense en profondeur repose sur le déploiement de **barrières complémentaires** de sécurité, chacune étant constituée d'un ensemble de **mesures**.

Dans cette approche, une barrière représente un objectif de sécurité répondant à une étape d'un scénario de risque, tandis qu'une mesure constitue l'unité élémentaire (organisationnelle, technique ou opérationnelle) : son action participe à la couverture de l'objectif de sécurité d'une barrière.

La mise en œuvre d'une barrière s'articule autour de trois axes :

- **son rôle (« quoi »)**, dans la couverture d'un scénario de risque : **protection** (avant), **défense** (pendant) et **résilience** (après) ;
- **son placement (« où »)**, appliqué aux composants d'un SI : **utilisateurs, locaux, identités**, **réseaux, équipements, applications et données ;**
- **son implémentation (« comment »)**, selon les mesures de sécurité choisies pour répondre à son objectif de sécurité.

L'efficacité globale de cette stratégie repose sur des critères de **multiplicité, d'indépendance et de robustesse** qui s'appliquent au niveau :

- **des barrières,** afin d'assurer que le SI dispose de remparts successifs et autonomes, capables de s'opposer à chaque étape de progression d'un attaquant ;
- **des mesures,** afin d'assurer que chaque barrière est elle-même robuste et s'appuie sur des mesures variées, complémentaires, et sur des socles technologiques distincts ne partageant pas les mêmes faiblesses.

L'indépendance entre les barrières (protection, défense et résilience) est un critère particulièrement important. En effet, une défaillance d'une barrière de protection du SI de production ne devrait pas entraîner une perte de visibilité depuis le SI de supervision, ni compromettre les barrières de résilience du SI d'administration.

La mise en œuvre des mesures de sécurité sur un SI doit être adaptée en fonction de son niveau exposition, de sa criticité et des scénarios de risque retenus. L'exemple illustré ci-dessous ne traite qu'un seul scénario de risque parmi ceux possibles pour atteinte l'objectif d'un attaquant. Il n'est donc pas exhaustif, doit être adapté au contexte spécifique d'un SI, et complété par d'autres mesures pour couvrir l'ensemble des scénarios.

1/ EXEMPLE DE MISE EN OEUVRE

Pour se protéger d'une attaque par rançongiciel, les barrières et mesures à mettre en place pourraient être les suivantes :

- **Détecter et bloquer les tentatives d'hameçonnage (défense, réseau)** :
  - maintenir à jour les règles de détection ;
  - analyser les courriels de manière statique par signature et de manière dynamique dans une *sandbox ;*
  - utiliser une passerelle entrante pour réaliser ces analyses en amont du serveur de courriels.
- **Limiter la vraisemblance qu'un utilisateur exécute un logiciel malveillant (protection, utilisateur) :**

- sensibiliser régulièrement sur les tentatives d'hameçonnage ;
- tester le comportement des utilisateurs par des campagnes internes d'hameçonnage.

→ **Limiter les capacités d'un attaquant à installer des outils (protection, équipement) :**

- limiter les droits des utilisateurs suivant le principe du moindre privilège sur leurs postes de travail (ex. : ne pas donner de droits d'administration) ;
- assurer que les correctifs de sécurité des postes soient à jour.

→ **Détecter et bloquer l'installation de logiciels malveillants (défense, équipement) :**

- réaliser une analyse comportementale sur les postes utilisateurs (ex. : EDR) ;
- assurer la mise à jour des règles de détection sur les postes.

→ **Limiter les capacités d'un attaquant à établir un canal de commande/contrôle vers Internet (protection, réseau) :**

- mettre en œuvre un serveur mandataire pour les accès à Internet et un résolveur DNS pour les noms de domaine publics en DMZ ; les rendre non contournables par défaut ;
- maintenir à jour les règles de filtrage.

→ **Limiter les capacités de latérisation d'un attaquant par compromission d'un compte à privilèges** sur le poste de travail **(protection, identité) :**

- utiliser des comptes d'administration dédiés aux postes utilisateur ;
- réaliser des audits réguliers du service d'annuaire central.

→ **Pallier la perte de données (résilience, donnée) :**

- mettre en œuvre un mécanisme de sauvegarde des données avec au moins une copie hors ligne ;
- tester régulièrement les procédures de sauvegarde et restauration.

2/ EXEMPLES DE BARRIÈRES

Barrières génériques	Composant applicable	Exemple de multiplicité des mesures	Exemple d'indépendance des mesures	Exemples de robustesse des mesures
Protection : Authentification utilisateur	Identité	Authentification multi-facteur	Utilisation d'un jeton physique indépendant du poste d'accès au SI	Authentification par défi-réponse cryptographique Dimensionnement approprié des secrets
Défense : Analyse par anomalie des flux	Réseau	Multiplicité des points de collecte et d'analyse des flux	Centralisation des alertes sur des serveurs dédiés et séparés de la production Positionner les sondes derrière des TAP physiques	Maintien à jour des règles de détection Fiabilisation des alertes
Résilience : Site de repli à froid	Tous (ou juste le SI)	Redondance des fonctions critiques nécessaires à la continuité d'activité	Indépendance complète des composants du repli à froid de ceux de la production.	Test régulier des procédures de repli MCS des composants du repli