RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

DÉFENSE EN PROFONDEUR – MÉTHODOLOGIE

Le concept de défense en profondeur part du principe que tout composant ou mesure de sécurité peut être faillible. Il repose sur une **combinaison coordonnée** de mesures techniques, organisationnelles et physiques alignées sur des **scénarios d'attaque**, afin d'en augmenter le coût pour l'attaquant, en faciliter la détection et en limiter l'impact métier. Cette stratégie se caractérise par la **multiplicité**, la **robustesse** et l'**indépendance** des mesures afin de créer des barrières successives et éviter qu'une seule méthode d'attaque ne contourne plusieurs dispositifs.

La mise en œuvre de cette stratégie doit être itérative et priorisée selon les risques, en s'appuyant sur les quatre piliers que sont la **gouvernance**, la **protection**, la **défense** et la **résilience**.

1/ GOUVERNANCE – PILOTER ET CADRER

La gouvernance vise à encadrer et piloter les risques numériques avec des mesures organisationnelles afin d'anticiper les menaces, suivre le niveau de sécurité et renforcer en continu la sécurité d'un système d'information (SI).

- **Établir un cadre de gestion des risques** pour identifier et gérer les priorités, notamment via une cartographie des SI ainsi que la réalisation et le maintien d'une analyse de risques cybersécurité (ex. : EBIOS RM).
- **Identifier et auditer régulièrement les parties prenantes de l'écosystème pour maîtriser les risques liés à la chaîne d'approvisionnement** (*supply chain*). Des mesures peuvent notamment être imposées aux sous-traitants pour, par exemple, assurer la protection des données sensibles de l'entité ou la sécurité des développements.
- **Auditer régulièrement les mesures de sécurité appliquées au SI de l'entité** avant sa mise en service et jusqu'à sa fin de vie.
- **Sensibiliser et former les utilisateurs et intervenants externes** à la sécurité sur leurs périmètres de responsabilité.
- **Assurer une veille sur les vulnérabilités et les menaces** applicables au SI.

2/ PROTECTION – PRÉVENIR ET BLOQUER

Les mesures de protection visent à prévenir ou bloquer les attaques sur le SI, en réduisant la surface d'attaque et en rendant plus coûteuse toute tentative ciblant les actifs stratégiques de l'entité.

- **Protéger les accès physiques au SI** pour empêcher tout accès non autorisé aux composants critiques, par exemple avec des mécanismes de contrôle d'accès physique et de vidéoprotection.
- **Cloisonner et filtrer les communications** pour réduire la surface d'attaque, limiter la propagation latérale et appliquer des politiques de sécurité différenciées par zone de sécurité en portant une attention particulière aux moyens d'administration.
- **Contrôler les accès logiques au SI** pour assurer l'imputabilité des actions et appliquer le **principe du moindre privilège** en renforçant notamment les mécanismes d'authentification, la sécurité des annuaires et la non dissémination des secrets.
- **Protéger les données au repos ou en transit** pour en assurer la confidentialité et/ou l'intégrité. Des mécanismes cryptographiques peuvent être utilisés selon leur exposition et criticité.
- **Maintenir en condition opérationnelle et de sécurité (MCO/MCS) le SI**, pour assurer sa robustesse pendant son cycle de vie, via l'application de correctifs /de mesures palliatives adaptées aux risques propres à l'entité.

V1.0 (07/26)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

3/ DÉFENSE – DÉTECTER ET RÉAGIR

Les mesures de défense permettent une posture proactive pour détecter et réagir aux activités malveillantes, réduisant l'impact d'une attaque sur le SI.

- **Définir une stratégie de supervision** afin de détecter les scénarios d'attaque pertinents pour le SI, articulée autour de : (i) **la collecte** des évènements du SI et (ii) **la détection** en temps réel des activités suspectes par la création et le maintien à jour de règles de corrélation.
- **Définir une stratégie de réponse aux incidents** pour reprendre le contrôle du SI : qualification des alertes, endiguement de l'attaque, éviction du cœur de confiance et éradication des emprises résiduelles.

4/ RÉSILIENCE – RÉSISTER ET RESTAURER

Les mesures de résilience visent à résister aux attaques et à restaurer le SI dans son fonctionnement nominal, en assurant la continuité d'activité avec un niveau de dégradation acceptable, puis une reprise progressive pour limiter les impacts métier.

- **Définir un plan de continuité d'activité et de reprise d'activité (PCA/PRA)** pour maintenir les services en mode dégradé (moyen ou infrastructure de secours, site de repli, etc.) et restaurer le système dans son fonctionnement nominal, notamment au travers des procédures de sauvegarde et de restauration.
- **Définir un plan de gestion de crise** afin d'assurer au niveau stratégique les prises de décision, la coordination des équipes et la gestion de la communication.
- **Évaluer régulièrement la résilience du système et de l'organisation** par des exercices de gestion de crise, des tests de PCA (dont les tests de restauration) et de PRA.

5/ DÉMARCHE DE MISE EN ŒUVRE

La mise en œuvre d'une stratégie de défense en profondeur, pour un SI nouveau ou existant, doit être adaptée à la criticité du SI et à son niveau d'exposition à la menace. Une démarche itérative est recommandée :

- **Établir un référentiel du système** en identifiant son périmètre, son écosystème, ses biens essentiels, leurs interdépendances, ainsi que les mesures de sécurité applicables et leur éventuel état de mise en œuvre.
- **Définir les objectifs de sécurité et la cible à atteindre** en cohérence avec la criticité des missions du SI et de son exposition à la menace.
- **Assurer la multiplicité et la variété des mesures** en combinant protection, défense et résilience au regard des scénarios de menace.
- **Assurer la robustesse des mesures** par leur évaluation régulière, l'utilisation de briques de confiance et le déploiement des mises à jour.
- **Assurer la supervision de sécurité du SI** lorsque celui-ci a atteint un niveau de maturité suffisant en matière de protection, afin d'identifier tout éventuel contournement.
- **Privilégier une indépendance des mesures de sécurité** pour éviter qu'une seule méthode d'attaque puisse en contourner plusieurs. Cela inclut, par exemple, une diversité technologique des solutions déployées ou la non mutualisation de plusieurs mesures sur un même socle physique.
- **Assurer l'amélioration continue** en évaluant régulièrement la posture de sécurité de l'entité et en ajustant les mesures en fonction des retours d'expérience et de l'état de l'art de la SSI selon l'évolution des menaces.
- **Prioriser le renforcement des piliers de gouvernance et résilience** avant d'améliorer les mesures de protection et de défense. Avant toute chose, il est essentiel de s'assurer que le SI est pleinement maîtrisé et que l'entité est capable, en cas d'incident, de basculer rapidement vers un mode qui, bien que dégradé, permet le maintien des activités essentielles.
- **Renforcer les mesures de protection et de défense du SI**, en adéquation avec les capacités organisationnelles, pour en assurer la robustesse dans le temps. Une entité mature sur les quatre piliers peut alors déployer des mécanismes avancés, combinant de manière dynamique protection et défense (approche *Zero Trust*).

V1.0 (07/26)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr