RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

ARCHITECTURE SÉCURISÉE DE SI

La conception ou l'évolution de l'architecture d'un système d'information (SI) a des conséquences directes sur son niveau de sécurité. L'ANSSI propose donc un **ensemble de bonnes pratiques d'architecture sécurisée** ainsi que les **thématiques attendues dans un dossier d'architecture technique** pour garantir la bonne gestion et la documentation du SI. De plus, afin d'accompagner au mieux les architectes SI ou sécurité, **des liens vers des publications complémentaires de l'ANSSI** sont proposés.

1/ QUELQUES GRANDS PRINCIPES

- **Disposer d'une analyse de risque** (p. ex. selon la méthode EBIOS RM) et **connaître le contexte réglementaire** applicable au SI.
- **Cloisonner les ressources en fonction des risques et des besoins métier**, notamment suivant l'exposition et la sensibilité des données.
- **Ériger plusieurs barrières** maîtrisées, complémentaires, indépendantes et surveillées suivant le principe de défense en profondeur.
- **Faire circuler** dès que possible **les flux depuis une zone de plus haute confiance** vers une zone de moindre confiance (ex. : SI d'administration vers SI bureautique), et non l'inverse.
- **Sécuriser les opérations nécessitant des privilèges élevés** (ex. : actions d'administration) sur le SI, en particulier en les cloisonnant des environnements de production.
- **Élaborer une cartographie**, des inventaires, et prévoir leurs mises à jour.
- **S'assurer régulièrement que les choix technologiques et d'architecture sécurisée sont réellement motivés** par des besoins métiers avérés.

2/ DOSSIER D'ARCHITECTURE TECHNIQUE

Voici **une liste de thématiques à développer dans un dossier d'architecture technique** :

- Contextes métier et réglementaire, nature et sensibilité des données et traitements
- Identification, authentification et gestion des droits d'accès
- Administration (dont la gestion des comptes à privilèges et DevSecOps)
- Cloisonnement réseau, système et stockage
- Chiffrement des données en transit et au repos
- Filtrage des flux
- Maintien en condition de sécurité (MCS)
- Accès à distance (nomadisme numérique, tiers)
- Interconnexions (dont celle à Internet)
- Protection contre les codes malveillants
- Sécurité physique, contrôle d'accès et vidéoprotection
- Continuité et reprise d'activité (dont les sauvegardes)
- Supervision de sécurité (journalisation, détection, traitement des incidents)

V1.0 (08/25)

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

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

3/ PUBLICATIONS COMPLÉMENTAIRES

Pour compléter et approfondir les thématiques d'un dossier d'architecture technique, vous pouvez également **consulter et vous référer aux publications suivantes** :

- L'administration sécurisée de SI en contexte Microsoft Active Directory
- Le choix de pare-feux dans les zones exposées à Internet
- Les architectures des services DNS
- La protection des SI essentiels
- Modèle Zero Trust
- L'hébergement dans le *cloud* des SI sensibles
- Les architectures de SI sensibles ou Diffusion restreinte
- Les architectures des interconnexions multiniveaux
- Systèmes d'information hybrides et sécurité, un retour à la réalité (article)