RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

MODÈLE *ZERO TRUST*

L'objectif principal du modèle *Zero Trust* (ZT) est de réduire la confiance implicite accordée à un sujet souhaitant accéder au système d'information (SI).

Le contrôle d'accès logique repose alors sur :

- **une évaluation dynamique et régulière du sujet** cherchant à accéder à une ressource ;
- **une évaluation dynamique et régulière du contexte d'accès d'un sujet** incluant notamment l'état de sécurité du poste utilisé pour réaliser ces accès ;
- **la criticité en termes de disponibilité, d'intégrité et de confidentialité de la ressource accédée**.

Le *Zero Trust* n'est pas une nouvelle technologie ou une solution commerciale tout-en-un. C'est un modèle de sécurité dédié au renforcement de la sécurité d'accès aux ressources d'une entité. Il utilise des principes connus de **défense en profondeur** parmi lesquels **l'authentification systématique, le principe de moindre privilège ou la micro-segmentation.**

Son adoption doit être **maîtrisée et progressive** sous peine d'affaiblir le SI, tout en donnant un faux sentiment de sécurité.

1/ UNE DÉMARCHE DE TRANSFORMATION

→ **Intégrer le modèle *Zero Trust* dans une démarche de défense en profondeur et de maîtrise des risques.** Le ZT ne doit pas être vu comme une alternative à la défense périmétrique, mais davantage comme une approche complémentaire.

→ **Définir une trajectoire de transformation en choisissant précisément les cas d'usage pour lesquels le modèle *Zero Trust* répond à un objectif de sécurité** : qui, dans quels contextes, pour quelles ressources ?

→ **Définir une politique de contrôle d'accès logique au regard des objectifs de sécurité fixés** pour chaque cas d'usage, uniquement sur la base d'attributs maîtrisés – c'est-à-dire des attributs que l'entité est capable de maintenir à jour et dont elle connaît le périmètre de couverture et le niveau de qualité.

→ **Réaliser et maintenir à jour une cartographie des applicatifs, données, utilisateurs, équipements et les flux** entre tous ces éléments pour mettre en œuvre des contrôles d'accès granulaires, dynamiques et réguliers.

→ **Réaliser des tests de sécurité et de bon fonctionnement avant mise en production**, d'une durée suffisante, afin de fiabiliser les décisions de contrôle d'accès logique et la remontée des alertes attendues.

→ **Porter une attention particulière à la centralisation des fonctions de contrôle d'accès logique**, et notamment à l'impact sur le SI d'une atteinte en disponibilité et/ou en intégrité de ces fonctions.

V1.0 (06/25)

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

2/ LES GRANDS PRINCIPES TECHNIQUES

→ **Déployer une infrastructure de contrôle des autorisations** s'appuyant sur le modèle ***Attribute-Based Access Control*** **(ABAC)** et permettant l'évaluation dynamique et continue des demandes d'accès selon :

> les attributs du sujet (par exemple sa fonction) ;

> les attributs de la ressource (par exemple son niveau de confidentialité) ;

> les attributs environnementaux liés au contexte de la demande d'accès (par exemple le niveau de conformité du moyen d'accès utilisé par rapport à la politique de sécurité de l'entité, l'heure, le lieu, etc.).

→ **Déployer une infrastructure de gestion des identités et des authentifiants** de ses utilisateurs, processus automatiques et équipements. Le cycle de vie des comptes uniques et des authentifiants doit être maîtrisé et progressivement automatisé afin d'en faciliter la gestion.

→ **Déployer une infrastructure de gestion des actifs et des vulnérabilités** des processus automatiques et des équipements. Le processus d'identification des écarts par rapport à la politique de sécurité et de mise en conformité doit être maîtrisé et automatisé (par exemple la gestion des correctifs de sécurité) lorsque cela est possible.

→ **Déployer une infrastructure de supervision de sécurité** afin de collecter et analyser les évènements de sécurité de chaque utilisateur et équipement. Une supervision de sécurité maîtrisée, c'est-à-dire avec un faible taux de faux positifs et de faux négatifs, est un prérequis essentiel avant toute utilisation dans les prises de décisions d'accès.

→ **Utiliser des mécanismes d'authentification multifacteur forte** pour les accès utilisateurs. Un fort niveau d'assurance sur l'identité de l'utilisateur est essentiel dans le modèle ZT.

→ **Utiliser des équipements durcis et maitrisés pour les accès aux données critiques de l'entité.** La visibilité sur l'état de sécurité des équipements personnels ou le niveau de confiance sur les informations retournées par ce type de poste est insuffisant.