Le modèle Zero Trust

Le modèle *Zero Trust* exerce un attrait croissant car il est promu comme une garantie d'accès sécurisé aux ressources informatiques dans les contextes d'usages mixtes (télétravail, BYOD1/AVEC) et fait l'objet d'un engouement de la part d'éditeurs de solutions technologiques et de sécurité qui y voient la perspective de nouveaux gains.

Or, à ce jour, le recours à ces solutions est ardu, faute de maturité : le déploiement est susceptible d'entraîner des erreurs d'installation ou de configuration, d'accroître la vulnérabilité des systèmes d'information et de donner aux entreprises un faux sentiment de sécurité.

Si le modèle *Zero Trust* s'inscrit dans la logique de « *défense en profondeur* » promue historiquement par l'ANSSI, il constitue une modification du paradigme de la stricte logique périmétrique qui a longtemps prévalu. Par conséquent, si une mise en œuvre du modèle est envisagée, elle ne peut être que progressive : elle suppose le recours à des solutions de sécurité nouvelles qui doivent s'intégrer dans un système global de défense sans s'y substituer. Le recours à de telles solutions est ardu : le déploiement est susceptible d'entraîner des erreurs d'installation ou de configuration, d'accroître la vulnérabilité des systèmes d'information et de donner aux entreprises un faux sentiment de sécurité.

1. Principes du *Zero Trust* : une remise en cause de la « confiance implicite » accordée dans le modèle périmétrique

Les récentes évolutions des technologies et des usages remettent en question le modèle traditionnel de défense périmétrique. Le recours accru à l'informatique nuagique *(cloud)*, le développement du télétravail et l'utilisation de moyens personnels (BYOD) pour accéder à des données professionnelles réduisent le contrôle que les entités exercent sur leurs systèmes d'information et leurs données. En parallèle, le niveau de menace augmente. Dans ce contexte, les mesures traditionnelles de sécurisation du système d'information (SI), telles que les pare-feux, le cloisonnement (physique ou logique) ou les VPN, rencontrent des limites.

Le modèle *Zero Trust* propose de pallier ces problèmes de sécurité en faisant évoluer la notion de périmètre. Le *Zero Trust* est avant tout un concept d'architecture dédié au renforcement de la sécurité d'accès aux ressources et aux services et non pas une technologie en soi, a fortiori ce n'est pas une solution logicielle « tout-en-un » commerciale.

Dans une logique de défense périmétrique traditionnelle, les utilisateurs connectés depuis le réseau de l'entité ont le droit d'accéder à de larges ressources, sans que soient appliquées des mesures élémentaires de cloisonnement ou des contrôles ultérieurs à leur authentification et l'accès à leur session : les utilisateurs sont considérés, par hypothèse, comme étant « de confiance ». **La démarche *Zero Trust* consiste au contraire à réduire la « confiance implicite » accordée aux utilisateurs et aux activités menées par le biais des équipements de l'entité.** Les « protections périmétriques » ne disparaissent pas pour autant : il y a toujours, par exemple, des pare-feux, des proxies, des annuaires de confiance.

[1] *Bring Your Own Device* / Apportez Votre Equipement Personnel

Pour réduire la « confiance implicite », les contrôles doivent devenir réguliers, dynamiques et granulaires (référence 1) **:**

- l'accès aux ressources doit être accordé sur la base du besoin d'en connaître ;
- l'accès doit être donné sur la base du plus faible niveau de privilège nécessaire pour réaliser la tâche ;
- les demandes d'accès doivent être contrôlées de la même manière quelles que soient leurs origines (le périmètre « intérieur » ou « extérieur » de l'entité) ;
- la politique d'accès aux ressources doit être dynamique et prendre en compte un large nombre d'attributs (identités de l'accédant et de la ressource accédée, sensibilité des ressources sollicitées, analyse comportementale de l'utilisateur, horaires d'accès, *etc.*) ;
- l'entité doit veiller à la sécurité de tous ses actifs à l'occasion des demandes d'accès et de manière récurrente durant l'usage ;
- les authentifications et autorisations d'accès aux ressources doivent faire l'objet de réévaluations régulières.

2. Le *Zero Trust* : plusieurs déclinaisons opérationnelles

Une bascule complète vers un modèle *Zero Trust* apparaît peu envisageable pour les entités dotées d'un patrimoine informatique hérité et sédimenté car elle requerrait une remise à plat totale du système d'information. **Les promoteurs du *Zero Trust* défendent logiquement une mise en œuvre progressive.** Une stratégie proposée fait du recours au modèle *Zero Trust* un processus en deux étapes, la première consistant à intégrer au SI « traditionnel » un ensemble de solutions de chiffrement, d'outils permettant de prévenir la fuite de données (*data loss prevention*), de contrôles de conformité (type *NAC*). Le NIST anticipe de son côté une transformation incrémentale des SI : les entités opéreront d'abord un SI hybride mettant en œuvre un modèle à mi-chemin entre le modèle *Zero Trust* et le modèle périmétrique.

Une mise à jour de l'**analyse de risque du SI est nécessaire avant tout déploiement :** la cartographie du SI est revue en distinguant clairement les périmètres pouvant être intégrés au déploiement *Zero Trust* (par exemple: applications Web, applications cloud) et ceux qui ne le seront pas.

Plusieurs axes d'effort sont envisageables pour intégrer à un SI « traditionnel » les principes du *Zero Trust* :

- une **gouvernance améliorée de l'identité** (l'accès aux ressources est contingenté à l'identification de l'utilisateur et de l'équipement utilisé, du statut de l'actif et de facteurs environnementaux tels que l'heure et la géolocalisation de la demande de connexion).
  En tant qu'éléments clés du modèle *Zero Trust*, le ou les référentiels d'identité doivent être assainis avec une politique stricte de mise à jour lors des arrivées, départs et mobilités. Ils doivent refléter fidèlement la situation courante des utilisateurs ;
- un **cloisonnement des ressources plus granulaire et dynamique**. Cette « micro-segmentation » réunit les ressources en groupes qui ont une signification métier et le filtrage des flux entre ces groupes devient indépendant des adresses IP des ressources. Cette couche d'abstraction supplémentaire (ex. : tags et *vxlan)* permet d'adapter la protection des ressources au plus juste besoin de protection, car toutes les ressources sont cloisonnées en fonction de leur rôle, de leur sensibilité et de leur exposition aux menaces ;
- une **utilisation des moyens d'authentification à l'état de l'art**, dans la mesure où l'authentification double facteur est généralement un prérequis à la mise en œuvre du modèle *Zero Trust*, il est recommandé d'être attentif au choix des facteurs d'authentification et de privilégier par exemple des certificats générés par une infrastructure de gestion de clés (IGC) de confiance ou des jetons FIDO ;

- un **renforcement des moyens de détection**, les journaux de sécurité générés doivent être judicieusement configurés puis centralisés dans un SIEM. Les équipes de supervision de la sécurité (SOC) doivent être suffisamment formées, expérimentées et dimensionnées pour réagir aux alarmes de sécurité. ;
- une **configuration à l'état de l'art** quant à la sécurité des services. Par exemple, pour le chiffrement de flux, TLS doit être configuré suivant le guide TLS de l'ANSSI[2] ;
- une **conduite du changement** à ne pas délaisser. Si le modèle *Zero Trust* est vu comme un levier de simplification de l'expérience utilisateur, il ne doit pas faire oublier que les utilisateurs sont les premiers concernés par la sécurité numérique de leur entité. Les nouveaux modes d'accès, d'authentification ou d'alerte doivent être communiqués de façon claire en rappelant l'importance d'être vigilant dans l'utilisation des moyens numériques.

Cette transformation doit être progressive et maîtrisée afin de s'assurer de la protection des données et des actifs traités et ne pas fragiliser le système d'information historique. Pour la mettre en œuvre, il n'existe pas de produit ou de composant normalisé.

Enfin, **l'exclusion des postes d'administration du modèle *Zero Trust* est impérative.** La doctrine décrite dans le guide d'administration sécurisée de l'ANSSI reste à privilégier[3]. En particulier, il est préférable de dédier des postes d'administration pour se connecter au SI d'administration avec un tunnel VPN IPsec non contournable.

3. Le *Zero Trust* : de nouveaux risques pour le niveau global de sécurité

Le *Zero Trust*, s'il est interprété de manière à rompre avec le modèle périmétrique traditionnel, est susceptible d'accroître les vulnérabilités. En particulier, le recours à des solutions logicielles nouvelles et nombreuses multiplie le risque de perte de contrôle par rapport aux solutions physiques (par exemple, du fait d'une mauvaise installation, d'erreurs de configuration ou de la présence de vulnérabilités exploitées par des attaquants tiers), donnant ainsi un faux sentiment de sécurité.

L'approche « tout-en-un » des fournisseurs de solutions commerciales *Zero Trust* peut sembler attractive sur le papier, or elle ne dispense aucunement d'une réflexion autonome sur l'état de l'art de toutes les déclinaisons possibles de la démarche : chiffrement des flux, jetons d'authentification, journalisations et sensibilisation des utilisateurs. **Il convient en outre de garder à l'esprit que l'adoption d'un modèle *Zero trust* et l'architecture associée ne se substituent aucunement à l'inventaire et au contrôle des terminaux clients utilisés pour accéder aux ressources et aux services.**

Dans la mesure où une entité souhaiterait s'engager dans une transformation progressive vers un modèle *Zero trust*, il conviendra de continuer d'appliquer les principes de gestion et de maîtrise des risques afin d'assurer la protection du patrimoine informationnel et applicatif : ces principes sont garants de la bonne continuité des missions et de la pérennité de l'entité.

Références

1. *Zero Trust Architecture*, NIST Special Publication 800-207, août 2020

[2] https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls/

[3] https://www.ssi.gouv.fr/administration/guide/securiser-ladministration-des-systemes-dinformation/