



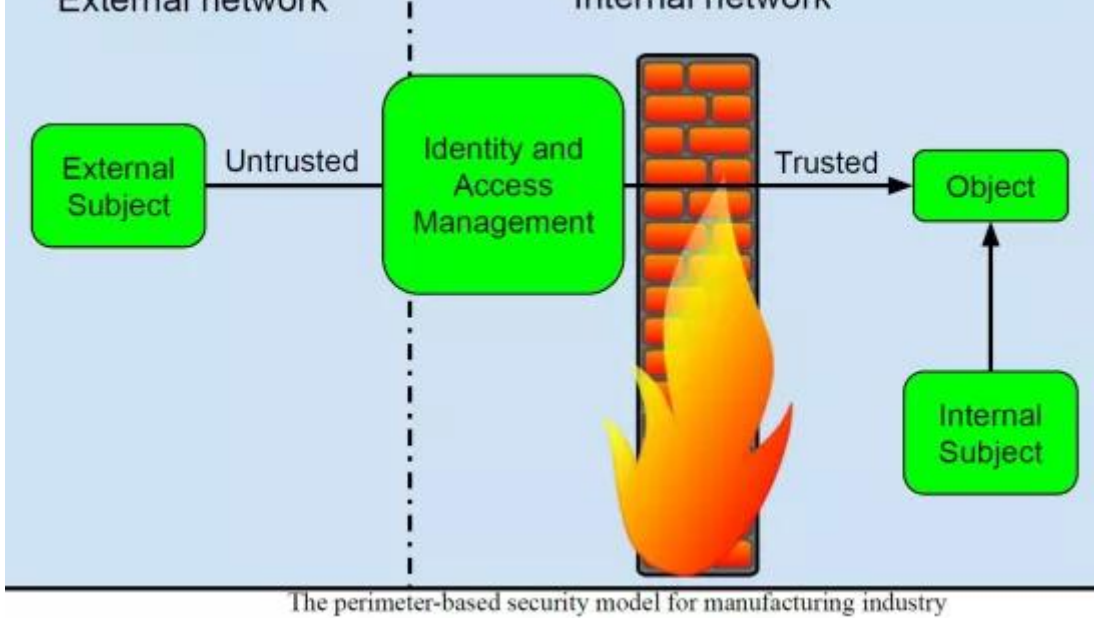
Zero Trust - vers une architecture de fabrication intelligente et sûre

16 février 2023, 10:02

Farhad Aghili

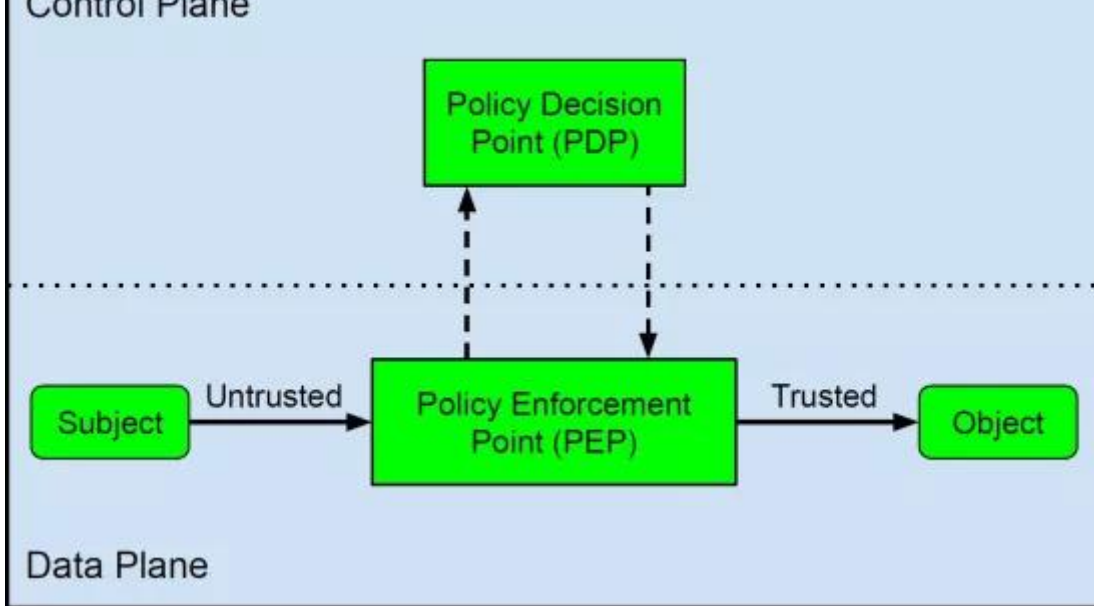
Stratégie de cybersécurité fondée sur le principe « ne jamais se fier, toujours vérifier », Zero Trust vise à maintenir le niveau de sécurité numérique d'une entreprise en éliminant toute confiance implicite et en validant chacune des étapes que présentent les interactions numériques, de leur création à leur achèvement.

Les architectures de sécurité traditionnelles que l'on rencontre dans l'industrie manufacturière intelligente reposent sur un **modèle de sécurité périmétrique** dans le cadre duquel les opérateurs interconnectés au réseau interne sont considérés par défaut comme étant dignes de confiance. En conséquence, ils peuvent accéder aux ressources internes de l'entreprise. La sécurité périmétrique consiste à assurer la protection de l'entreprise contre les réseaux externes au moyen d'un pare-feu, d'un système de prévention des intrusions (IPS), etc. Ainsi, une authentification des utilisateurs connectés à tout réseau externe s'impose avant de les juger dignes de confiance. Qui plus est, après leur authentification, ces utilisateurs dignes de confiance à long terme pourront accéder aux ressources internes de l'entreprise, sous réserve d'autorisation.



Ainsi, aux termes de cette approche, une fois qu'un adversaire obtient le droit d'accéder au réseau interne (p. ex., en compromettant un opérateur/une identité digne de confiance), accéder aux ressources internes de la même manière que les utilisateurs légitimes ne lui pose aucun problème. En outre, tout adversaire ayant obtenu l'accès au réseau interne est à même de se mouvoir latéralement à travers le réseau et de compromettre d'autres hôtes, serveurs et infrastructures critiques. Rapport VMware 2022 : Quelque 25 % des attaques subies se sont caractérisées par un mouvement latéral.

À l'inverse, Zero Trust (ZT) est basé sur le concept suivant : ne jamais se fier et toujours vérifier. Dès lors, ZT applique les mêmes contrôles de sécurité et d'accès aux utilisateurs internes et externes. ZT limite également les mouvements latéraux internes en contrôlant le pont de données et en validant chaque accès par session. Le modèle de contrôle d'accès sur lequel se base ZT repose non seulement sur la mise en oeuvre de politiques statiques, mais aussi sur celle de politiques dynamiques prenant en considération les utilisateurs, ressources exploitées et attributs environnementaux tels que le terminal d'émission de la demande d'accès. **De plus, il est essentiel que le niveau de confiance attribué à tout périphérique ou utilisateur souhaitant accéder à des ressources spécifiques soit à la mesure du risque encouru.** Le schéma ci-après illustre la vision logique de ZT pour un système d'entreprise.



Modèles de contrôle d'accès

La conception d'une architecture ZT (ZTA) requiert l'élaboration mûrement réfléchie d'algorithmes **d'authentification d'identité**, de **contrôle d'accès** et **d'évaluation du niveau de confiance**. Toute architecture ZT requiert une analyse des modèles de contrôle d'accès susceptibles (ou non) d'être adaptés à l'industrie manufacturière intelligente. Il faut impérativement souligner que la soumission des utilisateurs et périphériques à un contrôle d'accès s'impose. Plus précisément, tout système ZT doit être à même de surveiller les différents périphériques qui tenteraient d'accéder au réseau de fabrication intelligente et de s'assurer que chacun de ces périphériques jouit d'une autorisation d'accès.

En particulier, l'industrie manufacturière intelligente a recours à des serveurs locaux ou des systèmes infonuagiques pour enregistrer des informations et des entités systémiques (utilisateurs, périphériques). Moyennant le respect de certaines règles de contrôle d'accès prédéfinies, ces entités sont à même d'accéder à ces données et d'effectuer des opérations spécifiques (p. ex., analyse de données, apprentissage automatique, intelligence artificielle). À l'instar des contrôle d'accès basé sur des rôles (RBAC), contrôle d'accès discrétionnaire (DAC) et contrôle d'accès obligatoire (MAC), ces mécanismes reposent sur divers modèles de contrôle d'accès statiques (c.-à-d., définis une seule fois, mais utilisés à plusieurs reprises). Comme évoqué plus haut, ZT est fondé sur le principe « ne jamais se fier et toujours vérifier » et la confiance de l'utilisateur se doit d'être toujours proportionnelle au risque et à la politique dynamique. Dès lors, les modèles de contrôle d'accès basés sur des règles de contrôle d'accès prédéfinies sont inadaptés à une architecture ZT.

Un autre modèle de contrôle d'accès bien connu et abondamment utilisé ces derniers temps réside dans le **contrôle d'accès basé sur des attributs** (ABAC), lequel constitue une excellente alternative au RBAC. Avec l'ABAC, l'accès n'est accordé à un utilisateur/périphérique que si et uniquement si ce dernier répond aux attributs du modèle. Le modèle ABAC de base ne repose que sur des attributs statiques prédéfinis tels que l'« identité », le « rôle », etc. Les problèmes rencontrés avec ce modèle sont de deux ordres : (1) absence de vérification en temps réel et (2) enregistrement de tous les attributs statiques au sein du périphérique mobile de l'utilisateur. Tirant parti du potentiel intégral de l'ABAC, en exploitant les attributs statiques et dynamiques découlant

du comportement de l'utilisateur (p. ex., « heure » et « lieu »), ce modèle permet de procéder à une vérification systématique du comportement de l'utilisateur avant de lui accorder toute autorisation d'accès. Outre les particularités mentionnées ci-avant, le modèle de contrôle d'accès utilisé par le système ZT doit prendre en considération l'historique récent de l'utilisateur ou du réseau lors de l'évaluation des demandes d'accès.

Étant donné un environnement dynamique de fabrication intelligente et compte tenu du fait que le système ZT requiert un potentiel de prise de décision en temps réel, un **modèle de contrôle d'accès sensible aux risques** permet de résoudre les problèmes d'autorisation d'accès en se fondant sur divers niveaux de risque d'intervention. Au même titre que la fiabilité de l'utilisateur/périphérique demandeur, maints facteurs contextuels et environnementaux comptent au nombre des variables susceptibles d'être prises en considération lors du calcul du risque. En règle générale, tout modèle de contrôle d'accès sensible aux risques s'articule autour des éléments suivants : « facteurs de risque », « estimation des risques » et « module de contrôle d'accès ». L'autorisation dont jouit l'utilisateur, la sensibilité aux recours introduits, la gravité des actions, l'historique des risques, la confiance comportementale envers l'utilisateur, les avantages, l'impact des opérations et certaines particularités contextuelles pourraient être considérés comme une série de facteurs de risque vitaux dans le contexte de la fabrication intelligente. Les techniques d'estimation des risques applicables aux modèles de contrôle d'accès sensibles aux risques pourraient être fondées sur la logique floue, l'apprentissage automatique, la théorie des jeux et l'évaluation des risques. Toutefois, dans le contexte de la fabrication intelligente, le problème majeur réside dans l'absence de tout ensemble de données apte à représenter la probabilité et l'impact de chaque risque. L'intégration d'un modèle de contrôle d'accès sensible aux risques et d'un modèle ABAC dans le cadre duquel le facteur de risque est traité comme un attribut, permet d'en user comme modèle de contrôle d'accès pratique pour proposer une architecture ZT applicable à l'industrie manufacturière intelligente.

En route vers une architecture ZT sûre et fiable

Au fil du temps, l'architecture ZT (p. ex., la ZTA proposée par NIST en 2020) s'est essentiellement appliquée aux systèmes d'entreprise (la plupart des offres commerciales). Néanmoins, le déploiement de la ZT dans des domaines gourmands en technologies opérationnelles (OT), tels que la fabrication intelligente, en est encore à ses balbutiements et de nombreux défis subsistent quant aux principes, à l'architecture et à la mise en œuvre de la ZT. Forte de sa connaissance approfondie des modèles ZT et de l'architecture de sécurité en fabrication intelligente dans une foule de domaines, une brochette d'experts Sirris vous facilitera la vie. Leurs compétences vous permettront de concevoir une architecture ZT sûre et fiable pour votre industrie manufacturière intelligente.

Pour en savoir plus concernant les modèles ZT et leur application :

- Notre masterclass [Masterclass Cybersecurity - Manufacturing | Sirris](#)
- Notre projet collaboratif de renforcement / diffusion des connaissances [Cybersecurity 4.0 | Strategic and case-specific cybersecurity - for Industry 4.0 in SMEs | Sirris](#)

À l'heure actuelle, Sirris coordonne également plusieurs projets dans ce domaine dans le cadre du programme ITEA de l'UE. Si vous souhaitez en savoir plus, prenez contact avec nous! Rien ne s'oppose à l'ajout de nouveaux partenaires.

Auteurs



Farhad Aghili