BRADLEY & ROLLINS

Conseil stratégique en Technologies et Cyberdéfense

« ZERO-TRUST »
GUIDE D'IMPLANTATION

Rappels pour créer des phases d'implantation rapides

Résumé

Le « Zero-Trust » signifie qu'il faut repenser la sécurité de chaque élément technologique d'un écosystème de réseaux. Découvrez les étapes de la création d'un environnement répondant à une philosophie tactique de zéro confiance.

BRADLEY & ROLLINS

Préparé pour ASIMM

BRADLEY & ROLLINS
Conseil stratégique en Technologies et Cyberdéfense

Contenu

Le guide de mise en œuvre du « Zero-Trust »

Le concept global du modèle « Zero-Trust »

Le « Zero-Trust » est un concept de sécurité qui exige que tous les utilisateurs, même ceux qui se trouvent à l'intérieur du réseau corporatif de l'organisation, soient authentifiés, autorisés, et qu'ils valident en permanence la configuration et la posture de sécurité, avant de se voir accorder ou de conserver l'accès aux applications et aux données. Cette approche s'appuie sur des technologies avancées telles que l'authentification multifactorielle, la gestion des identités et des accès (IAM) et la technologie de sécurité des terminaux de nouvelle génération pour vérifier l'identité de l'utilisateur et maintenir la sécurité du système.

Le « Zero-Trust » s'écarte considérablement de la sécurité traditionnelle des réseaux, qui suivait la méthode « faire confiance mais vérifier ». L'approche traditionnelle faisait automatiquement confiance aux utilisateurs et aux points d'extrémité situés dans le périmètre de l'organisation, mettant celle-ci en danger par des acteurs internes malveillants et permettant aux utilisateurs non autorisés d'accéder à un large éventail de données une fois à l'intérieur.

Cependant, le « Zero-Trust » ne peut réussir que si les équipes de l'organisation sont capables de contrôler et de valider en permanence qu'un utilisateur et son appareil disposent des bons privilèges et attributs. Une validation unique ne suffira pas, car les menaces et les attributs des utilisateurs sont tous susceptibles de changer.

Par conséquent, les équipes de l'organisation doivent s'assurer que toutes les demandes d'accès sont continuellement vérifiées avant d'autoriser la connexion à l'un des actifs corporatifs ou de cloud. C'est pourquoi l'application des politiques « Zero-Trust » repose largement sur la visibilité en temps réel des attributs des utilisateurs, tels que :

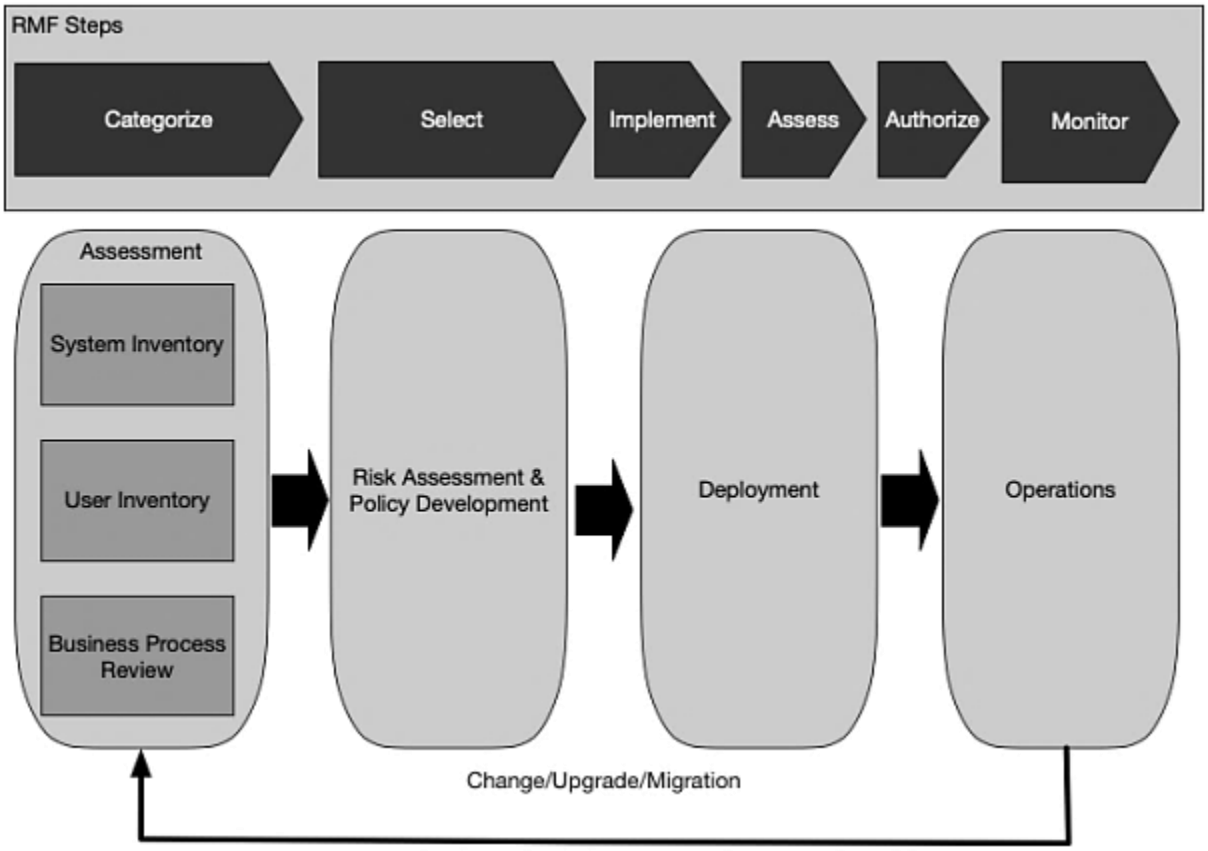
- L'identité de l'utilisateur
- Le type de matériel des points terminaux
- Les versions des intergiciels
- Les versions des systèmes d'exploitation
- Les niveaux de "patchs"
- Les vulnérabilités connues
- Les applications installées
- Les options de connexion des utilisateurs
- Les contrôles de détections de sécurité ou d'incidents

Les principaux concepts d'architecture (architecture « Zero-Trust » - ZTA) sont en cours d'élaboration dans le projet de publication spéciale du NIST 800-207 (*https://doi.org/10.6028/NIST.SP.800-207-draft*). Un déploiement ZTA implique l'élaboration de politiques d'accès en fonction d'un risque acceptable pour la mission ou le processus opérationnel désigné (voir section 7.3.3). Il est possible de refuser tout accès au réseau à une ressource et de n'autoriser l'accès que via un terminal connecté, mais cela est disproportionnellement restrictif dans la plupart des cas. Pour qu'une organisation puisse remplir sa mission, il existe un niveau de risque acceptable. Les risques associés à l'exécution de la mission donnée

doivent être identifiés, évalués et atténués. Pour y parvenir, le cadre de gestion des risques (RMF) du NIST a été élaboré.

Pour identifier les besoins et les prérequis de la « Zero-Trust », plusieurs questions doivent être abordées :

- Qu'est-ce qui est connecté ? Quels sont les appareils, les applications et les services utilisés par l'organisme ? Il s'agit notamment d'observer et d'améliorer la posture de sécurité de ces artefacts au fur et à mesure que des vulnérabilités et des menaces sont découvertes.
- Qui utilise le réseau ? Quels utilisateurs font partie de l'organisation ou sont externes et autorisés à accéder aux ressources de l'entreprise ? Cela inclut les entités non-personnelles (ENP) qui peuvent effectuer des actions autonomes.
- Que se passe-t-il sur le réseau ? Les entreprises ont besoin de connaître les schémas de trafic et les messages entre les systèmes.
- Comment les données sont-elles protégées ? L'entreprise a besoin d'une politique définie sur la manière dont les informations sont protégées au repos et en transit.



Le modèle « Zero-Trust » est basé sur les principes suivants :

- Réexaminer tous les contrôles d'accès par défaut.
- Exploiter diverses techniques de prévention.
- Permettre une surveillance en temps réel pour identifier rapidement les activités malveillantes.

- S'aligner sur la stratégie de sécurité plus large / holistique.

1. Réexaminer tous les contrôles d'accès par défaut.

Dans un modèle « Zero-Trust », il n'existe pas de source fiable. Le modèle suppose que des agresseurs potentiels sont présents à l'intérieur et à l'extérieur du réseau. Ainsi, toute demande d'accès au système doit être authentifiée, autorisée et cryptée.

2. Exploiter diverses techniques de prévention.

Un modèle de « Zero-Trust » repose sur diverses techniques préventives pour arrêter les infractions et minimiser leurs dégâts.

L'authentification multi-facteurs (AMF) est l'un des moyens les plus courants de confirmer l'identité de l'utilisateur et d'accroître la sécurité du réseau. L'AMF s'appuie sur deux éléments de preuve ou plus, notamment des questions de sécurité, la confirmation par courriel/texte ou des exercices logiques pour évaluer la crédibilité de l'utilisateur. Le nombre de facteurs d'authentification utilisés par une organisation est directement proportionnel à la sécurité du réseau, ce qui signifie que l'intégration d'un plus grand nombre de points d'authentification contribuera à renforcer la sécurité globale de l'organisation.

Le « Zero-Trust » empêche également les attaques par le biais de l'accès le moins privilégié, ce qui signifie que l'organisation accorde le niveau d'accès le plus bas possible à chaque utilisateur ou dispositif. En cas de violation, cela permet de limiter les mouvements latéraux sur le réseau et de réduire au minimum la surface d'attaque.

Enfin, le modèle « Zero-Trust » utilise la micro-segmentation - une technique de sécurité qui consiste à diviser les périmètres en petites zones pour maintenir un accès séparé à chaque partie du réseau - pour contenir les attaques. Si une brèche se produit, le pirate est incapable d'explorer en dehors du micro-segment.

3. Activer la surveillance en temps réel pour identifier rapidement les activités malveillantes.

Bien qu'un modèle « Zero-Trust » soit en grande partie de nature préventive, l'organisation devrait également intégrer des capacités de surveillance en temps réel pour améliorer son "temps de panne" - la fenêtre critique entre le moment où un intrus compromet la première machine et celui où il peut se déplacer latéralement vers d'autres systèmes du réseau. La surveillance en temps réel est essentielle à la capacité de l'ORGANISATION à détecter, enquêter et remédier aux intrusions.

4. S'aligner sur la stratégie de sécurité plus large.

Une architecture « Zero-Trust » n'est qu'un aspect d'une stratégie de sécurité globale. En outre, si la technologie joue un rôle important dans la protection de l'organisation, les capacités numériques seules ne permettront pas d'empêcher les violations. Les entreprises doivent adopter une solution de sécurité globale qui intègre diverses capacités de surveillance, de détection et d'intervention au niveau des points d'accès afin de garantir la sécurité de leurs réseaux.

La voie à suivre pour réaliser la mise en œuvre du « Zero-Trust » (ZT)

Bien que les besoins de chaque organisation soient uniques, il est important de suivre à minima les recommandations suivantes pour développer et déployer un modèle « Zero-Trust » :

1. Évaluer l'organisation de façon holistique.

Définir la surface de protection et identifier les données, biens, applications et services sensibles (DAAS) dans ce cadre. Évaluer l'ensemble des outils de sécurité actuels de l'organisation et identifier toute lacune au sein de l'infrastructure. Veiller à ce que les actifs les plus critiques bénéficient du plus haut niveau de protection au sein de l'architecture de sécurité.

2. Créer un répertoire de tous les actifs et cartographier les flux de transactions.

Déterminer où se trouvent les informations sensibles et quels utilisateurs doivent y avoir accès. Examiner comment les différents composants du DAAS interagissent et assurer la compatibilité des contrôles d'accès de sécurité entre ces ressources.

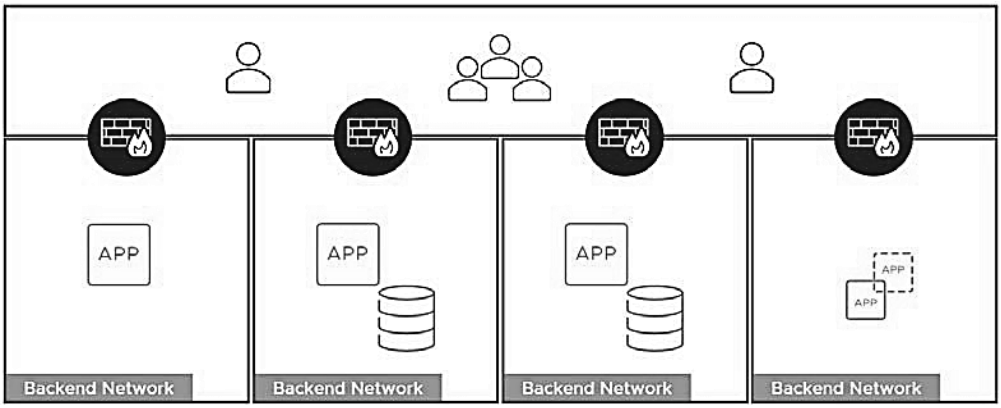
3. Mettre en place une série de mesures préventives.

Tirer parti de diverses mesures préventives pour dissuader les pirates et contrecarrer leur accès en cas de violation, notamment

Authentification multi-facteurs : L'authentification MFA, 2FA, ou troisième facteur, est essentielle pour atteindre la « Zero-Trust ». Ces contrôles fournissent une autre couche de vérification à chaque utilisateur à l'intérieur et à l'extérieur de l'entreprise.

Les principes du moindre privilège : Une fois que l'organisation a déterminé où se trouvent les données sensibles, accordez aux utilisateurs le moins d'accès possible nécessaire à leur rôle. (POLP)

Micro-segmentation : Les micro-périmètres servent à contrôler les frontières au sein du système, empêchant tout mouvement latéral non autorisé. L'organisation peut se segmenter en fonction du groupe d'utilisateurs, de l'emplacement ou d'applications regroupées logiquement.



Les bonnes pratiques des utilisateurs finaux : Définir les bonnes pratiques internes pour le télétravail et la gestion des travailleurs à distance.

4. Surveiller le réseau en permanence.

Déterminez où se produit l'activité anormale et surveillez toute l'activité environnante. Inspectez, analysez et enregistrez tout le trafic et toutes les données sans interruption.

Les défis du modèle « Zero-Trust » (ZT)

Pour vraiment comprendre le concept de « Zero-Trust » à un niveau granulaire, nous devons comprendre les défis auxquels les entreprises sont confrontées lors de la mise en œuvre d'un cadre de « Zero-Trust ». Voici quelques exemples :

1. Les anciennes applications, les anciennes ressources réseau, les outils administratifs et les protocoles font partie des opérations du réseau et de l'entreprise. Par exemple, les systèmes Mainframe, HR, Powershell, PSexec et autres sont généralement exclus de l'architecture « Zero-Trust ». Cependant, ce sont des outils essentiels pour les opérations tout comme les protocoles tels que NTLM qui doivent disparaître il y a des années mais qui sont là pour rester.

Traditionnellement, tous ces systèmes ne peuvent pas être protégés par une vérification d'identité, ce qui constitue un obstacle à un coût prohibitif (il est souvent trop coûteux de réorganiser ces systèmes). Habituellement, ces systèmes hérités sont exclus de l'approche, ce qui en fait le maillon le plus faible. Dans d'autres cas, les équipes de sécurité créent une expérience utilisateur incohérente ou, lorsque cela est possible (par exemple, PSexec), interdisent l'utilisation des outils, ce qui réduit la productivité du personnel.

2. La réglementation n'a pas encore adopté le modèle « Zero-Trust », ce qui signifie que les équipes de l'organisation auront du mal à formaliser et passer un exercice d'audit spécifique. Exemple, si la norme PCI-DSS exige l'utilisation de pare-feu et la segmentation des données sensibles, comment passer les audits s'il n'y a pas de pare-feu ? Une telle mesure soumettra-t-elle l'ensemble de l'environnement au règlement ? Quelles sont les implications de la réglementation en matière de segmentation et pas de " Zero-Trust » ? Les règlements devront changer avant que nous puissions utiliser ce modèle de manière complète et robuste.

3. La visibilité et le contrôle au sein du réseau sont souvent l'un des principaux facteurs qui empêchent les entreprises de mettre en place des réseaux « Zero-Trust ». La plupart des organisations n'ont pas une vue d'ensemble de tous les utilisateurs individuels de leur réseau, ni la possibilité de définir des protocoles pour chacun d'entre eux, et sont donc vulnérables aux menaces que représentent les dispositifs non adaptés, les systèmes existants et les utilisateurs sur-privilégiés.

Bien qu'il existe d'autres exemples, ces points essentiels soulignent le fait que nous sommes loin d'avoir atteint un niveau de conformité « Zero-Trust » à 100 % : pour l'instant, cela nécessiterait une intervention chirurgicale majeure sur l'infrastructure informatique d'une organisation. À court terme, une approche hybride de la « Zero-Trust » sera probablement le statu quo.

Choisir entre 2 modèles d'architecture de « Zero-Trust » (ZTA)

1. Une architecture 100% « Zero-Trust » (ZT).

Dans une approche « green field », il serait possible de construire un réseau d'architecture « Zero-Trust » à partir de la base. En supposant que l'entreprise connaisse les applications et les flux de travail qu'elle veut utiliser pour ses opérations, elle peut produire une architecture basée sur les principes de la stratégie « Zero-Trust » pour ces flux de travail. Une fois les flux de travail identifiés, l'entreprise peut réduire le nombre de composants nécessaires et commencer à définir les interactions entre les différents composants. À partir de ce point, il s'agit d'un exercice d'ingénierie pour construire l'infrastructure du réseau et configurer les composants. Dans la pratique, cette option est rarement viable pour les agences fédérales ou toute organisation disposant d'un réseau existant. Cependant, il peut arriver qu'une organisation soit amenée à assumer une nouvelle responsabilité qui nécessiterait la construction de sa propre infrastructure. Dans ces cas, il pourrait être possible d'introduire les concepts de " Zéro-confiance" dans une certaine mesure. Par exemple, une agence peut se voir confier une nouvelle responsabilité qui implique la construction d'une nouvelle application et d'une nouvelle base de données. L'agence pourrait concevoir l'infrastructure nouvellement nécessaire autour des principes de “ Zero-Trust », comme l'évaluation de la confiance des utilisateurs avant l'octroi de l'accès, la mise en place de micro-périmètres autour des nouvelles ressources, etc. Le degré de réussite dépend de la dépendance de cette nouvelle infrastructure par rapport aux ressources existantes (par exemple, les systèmes de gestion des identités).

2. ZTA hybride et architecture traditionnelle

Il est peu probable qu'une entreprise importante puisse migrer vers un réseau ZTA en un seul cycle de rafraîchissement technologique. Il y aura une période (peut-être indéfinie) pendant laquelle les flux de travail ZTA coexisteront dans une entreprise traditionnelle. La migration vers une approche ZTA de l'entreprise peut se faire un processus d’affaires à la fois. L'entreprise doit s'assurer que les éléments communs (par exemple, la gestion des identités, la gestion des appareils, l'enregistrement des événements, etc.) sont suffisamment souples pour fonctionner dans une architecture de sécurité hybride ZTA et traditionnelle. Les architectes corporatifs peuvent également vouloir limiter les solutions candidates au ZTA à celles qui peuvent s'interfacer avec des composants existants.

L’aide-mémoire des phases à suivre

1. **Évaluer le contexte de l’ORGANISATION :**
    a. Qu'est-ce qui est connecté ?
    b. Qui utilise le réseau ?
    c. Que se passe-t-il sur le réseau ?
        i. Actifs concernés
        ii. Segmentation du réseau
    d. Comment les données sont-elles protégées ?
        i. DaR
        ii. DiU
        iii. DiM
    e. Que sont les directives internes ZT ?
        i. Règlements.

   ii. Bonnes pratiques internes.
   iii. Exceptions internes à la règle des BYOD.

2. **Définir le meilleur modèle de ZTA :**
   a. 100%
   b. Hybride
3. **Mettre en œuvre les principes de la ZTA**
   a. Effectuer une analyse des écarts vs les directives ZT.
   b. Définir les mesures correctives des lacunes dans une feuille de route.
   c. Diviser les utilisateurs finaux en entreprises/écosystèmes de projet.
   d. Activer la micro-segmentation et l'activation permanente du VPN.
   e. Mettre en œuvre une solution avancée de CED avec des fonctions DLP (par exemple, blocage USB/Bluetooth).
   f. Enrichir le cryptage des flux accessibles à distance (par exemple, TLS partout).
   g. Réduire les accès HP et ajouter une solution d'escalade dynamique des droits.
   h. Activer l'enregistrement des audits pour couvrir les exigences de ZT.
   i. Créer des points de saut de micro-services, de virtualisation des données et de Hub de données.

Conclusion

Aujourd'hui, nous entrons dans une nouvelle ère du ZTA. Les organisations veulent un modèle de sécurité transparent, adapté à la nouvelle réalité du travail à distance massif, des services infonuagiques, de l’internet des objets et des communications mobiles.

Pour rester proche d’une posture de cybersécurité acceptable, les organisations d'aujourd'hui doivent pouvoir surveiller et contrôler facilement toutes les activités sur les réseaux de tout type, tant pour les utilisateurs que pour les points terminaux.