L'adoption du "Zero Trust" ou la confiance revisitée !

protiviti®
Global Business Consulting

La résilience des entreprises repose, notamment et de plus en plus, sur leur capacité à s'adapter au changement du mode de travail et leur aptitude à la transformation numérique. Il devient, en effet, essentiel pour de nombreux employés, de pouvoir travailler en toute sécurité depuis n'importe quel endroit, via différents types de terminaux, PC-smartphones-tablettes, et ce, à tout moment. Cette tendance de fond a explosée lors de la pandémie de COVID-19, qui a contraint des millions de personnes à travailler depuis leur domicile en utilisant des moyens mis à disposition par l'entreprise mais également personnels (BYOD – Bring Your Own Device), même si cette dernière tendance reste assez marginale pour différentes raisons et notamment celle de la sécurité.

Alors que les attaques cyber ne cessent d'augmenter et que parallèlement la transformation numérique reste une priorité vitale pour nombre d'entreprises, avec notamment le passage vers les services de Cloud, le concept de Zero Trust "confiance zéro" est passé au premier plan. Ce concept est assez ancien et était développé sur une logique inverse de celle couramment utilisée pour la défense périmétrique. La défense périmétrique était un principe de sécurité efficace et maitrisé quand les systèmes de l'entreprise étaient hébergés en interne (On Premise) et accessibles par un nombre restreint d'utilisateurs, et ce, depuis les locaux de l'entreprise. A l'aire du Cloud et de tout numérique, le passage à une logique Zero Trust devient essentiel pour garantir la sécurité des données, des services et globalement d'assurer de la robustesse du business face aux menaces cyber.

Qu'est-ce que le Zero Trust ?

Le Zero Trust est un changement de paradigme en matière de cybersécurité par rapport à l'architecture périmétrique traditionnelle, selon laquelle ce qui se trouvait à l'intérieur d'un périmètre était implicitement considéré comme fiable et une fois qu'un élément était authentifié, il l'était sur toute la durée de la session. Le Zero Trust en prend le contrepied.

Le Zero Trust n'est pas un produit, mais plutôt une logique de construction de services et ne représente pas une technologie en particulier. Le Zero Trust est un ensemble de concepts établis selon une approche de sécurité orientée risques et processus métier. En effet, les données et leur traitement sont des éléments essentiels à la démarche.

Le modèle change les principes de sécurité qui se basaient sur des éléments considérés comme sûrs. La confiance numérique dans l'identité d'une personne ou d'un système accédant à ces données, ne peut plus être implicite. Cela signifie qu'elle doit souvent être revérifiée, et ce, au plus près des ressources auquel elle accède afin de les protéger.

La démarche Zero Trust consiste à réévaluer régulièrement la confiance accordée aux utilisateurs, aux processus, aux accès, aux transactions …. Ainsi, les dispositifs ne doivent plus être considérés comme fiables par défaut, même s'ils sont déjà connectés à un réseau autorisé ou qu'ils ont déjà été vérifiés auparavant. Par exemple, si un comportement est identifié comme suspect, il doit être possible de modifier les conditions d'accès et les droits accordés à la volée. Cette modification voire suppression de droits doit être possible même s'ils avaient été validés précédemment, et cela, de manière dynamique.

Origine et évolution du concept Zero Trust ?

Comme nous l'avons vu précédemment, le Zero Trust est fondé sur le principe de "ne jamais faire confiance et toujours vérifier". Ce concept a été principalement conçu pour contrer les attaques lors de la phase de latéralisation. Cette phase appelée « mouvement latéral » est la phase de propagation de l'attaque dans le réseau en utilisant les droits hérités des machines précédemment compromises. C'est cette étape de latéralisation qui permet, si elle n'est pas empêchée, une large compromission des systèmes de l'entreprise par l'attaquant.

Le Zero Trust adresse des thématiques comme l'utilisation de la micro-segmentation avec des points d'accès contrôlés, la vérification permanente de l'identité, le contrôle continu des autorisations d'accès … Cette évaluation continue du niveau de sécurité permet aux entreprises de réduire leur surface d'attaque et donc les possibilités pour l'attaquant de réaliser ces « mouvements latéraux ».

Au cours de la dernière décennie, le Zero Trust a évolué naturellement avec le recours au Cloud Computing et représente désormais un ensemble de principes de cybersécurité et d'éléments d'architectures de références qui s'appliquent globalement à l'environnement des entreprises et ceci quel que soit l'emplacement de données et de leurs traitements.

Divers modèles d'implémentation de ce concept sont disponibles auprès d'organismes gouvernementaux (par exemple, NIST SP-800- 207, …), de fournisseurs de solutions (tels que Microsoft, Palo Alto Networks, Netskope, Okta, …), et d'instituts de recherche (tel que Forrester). La plupart des modèles sont synergiques et permettent aux entreprises de choisir celui qui correspond le mieux à leurs profils de risques et leur structure.

Les principaux éléments à considérer pour une mise en œuvre Zero Trust

La démarche de Zero Trust est indissociable des éléments constitutifs suivants qui doivent être orchestrés au sein d'une gouvernance pertinente de la cybersécurité (N.B : cette liste n'est pas exhaustive et dépend du périmètre adressé).

Gestion des données

Le recensement, l'évaluation et la localisation des données ainsi que le suivi et la maîtrise de leur traitement doivent être garantis. Il est fondamental que chaque donnée et que chaque traitement ait un propriétaire identifié et formé aux enjeux de protection de l'information. Les données doivent donc être classifiées qu'elles soient structurées ou non. Les mécanismes de protections seront adaptés et proportionnels à la valeur de chaque type de données.

Gestion des identités et des accès

Cette composante permet d'établir des rôles et responsabilités en fonction du « besoin d'en connaitre » et de s'assurer que des contrôles préventifs, comme l'authentification adaptative, et des contrôles détectifs, comme la gouvernance des identités sont mises en place. Chaque identité doit être vérifiée et sécurisée par des mécanismes d'authentification forte comme l'authentification multifactorielle, l'accès adaptatif et conditionnel ou les contrôles d'accès basés sur les rôles (RBAC – Role Based Access Controls) afin de valider l'identité sur l'ensemble.

Gestion des ressources IT

Elle est indispensable et vise à établir les principes d'inventaire et de suivi de parc informatique afin de maitriser les surfaces d'attaque et l'état du système d'information face à une nouvelle vulnérabilité mais également de détecter et limiter le shadow IT. Ces règles permettront également d'identifier où sont stockées et comment les données transitent et également comment elles sont traitées.

Architecture des services

Cette composante définit les principes de sécurité à suivre pour l'urbanisme des infrastructures, l'intégration des terminaux et serveurs et l'intégration et le développement des services qu'ils hébergent. Il sera par exemple présenté les règles de micro-segmentation pour limiter les mouvements latéraux dans l'environnement informatique et de points de contrôles permettant de visualiser les flux de données.

Supervision

Cette dimension est importante dans le cadre du Zero Trust, car elle permet par exemple de définir la gestion dynamique des accès et droits en fonction des éventuelles alertes liées à des comportements anormaux détectés par le SOC. Cela permet également de cloisonner dynamiquement des zones réseau et donc des mouvements latéraux potentiels.

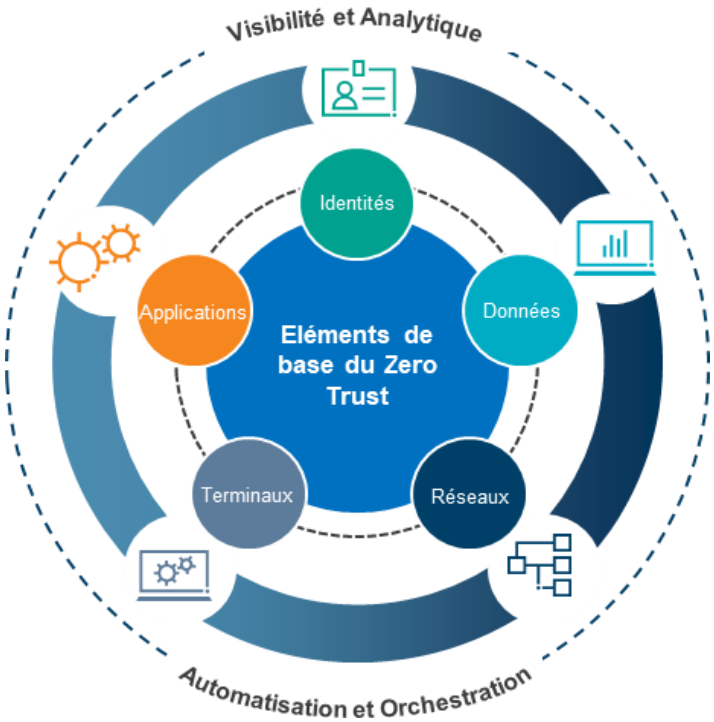
Automatisation et orchestration de la sécurité

La mise en œuvre de l'automatisation afin de faciliter les traitements rapides d'opérations IT doit être proposée. L'automatisation de la sécurité apporte des possibilités qui permettent des actions instantanées lorsque des événements connus se produisent. L'orchestration permet également de mettre à niveau les processus pour des opérations de routine et le traitement des incidents. Ceci accélère également les temps de réponse et de traitement des opérations de sécurité.

Ces différents composants doivent se refléter dans la gouvernance et cela passe donc par la mise à jour du corpus sécurité (politique, directive ou guide) selon l'existant et intégrera la logique Zero Trust afin de pouvoir choisir les éléments techniques de son implémentation.

Un projet global qui va au-delà d'une simple solution technologique

Il existe de nombreuses tendances sur le marché du Zero Trust, la plupart se concentrant sur des solutions qui ne permettent de couvrir qu'un composant architectural ou une caractéristique spécifique du Zero Trust. De nombreuses entreprises pensent que le Zero Trust commence par l'identité, principalement parce que les fournisseurs de solutions d'IAM (Identity & Access Management) sont matures et ont adopté les principes d'Architecture Zero Trust tels que l'authentification multifactorielle (MFA) et l'accès conditionnel - et en font la promotion. Bien qu'il soit un composant essentiel, le Zero Trust est à considérer comme une stratégie et un programme holistique qui se compose de divers éléments.



Quelques considérations additionnelles à prendre en compte pour le Zero Trust

Zero Trust et Intelligence Artificielle

Pour pouvoir être efficace, une démarche Zero Trust doit reposer sur un moteur de sécurité centralisé prenant en compte le risque de manière continue. En permanence, les accès utilisateurs doivent être évalués par rapport à un certain nombre de facteurs. Dans un modèle classique, les règles sont préétablies et dès lors qu'une action correspond à une règle une réaction se déclenche. Avec l'aide l'intelligence artificielle, il serait possible de créer des règles de sécurité dynamiques directement crées par le moteur de l'IA. De plus, il est de plus en plus compliqué de traiter les informations de manière suffisamment réactive car leur volume est de plus en plus conséquent et provient de sources de plus en plus variées. Il est très difficile dans ce contexte de détecter les signaux faibles sans l'aide d'une Intelligence Artificielle et de l'automatisation. Il parait donc difficile de mettre en œuvre ce modèle sans s'appuyer sur cette technologie.

Zero Trust et l'accélération vers le tout numérique

Dans le cadre de la technologie de l'information historique (IT – Information Technology) qui est basé sur des utilisateurs et des processus, la notion de Zero Trust s'applique assez bien. Dès lors que l'on passe sur des systèmes industriels ou de type objets connectés ce modèle est plus complexe à mettre en œuvre, car les conséquences par exemple d'un cloisonnement dynamique peuvent être très préjudiciables à l'entreprise. Toute cette complexité de sécurisation liée à la numérisation du monde qui nous entoure au travers de toutes ses déclinaisons comme peuvent l'être, l'Internet des objets pour le particulier (Internet of Things - IoT), la numérisation des industries (Operational Technology - OT) ou (Industrial Internet of Things - IIoT), les communications automatisées de systèmes (machine-to-machine - M2M), voire du contrôle automatique de systèmes autonomes (Supervisory Control And Data Acquisition - SCADA) … demande l'élaboration de nouveaux modèles et l'application stricto sensu de stratégie de sécurité éprouvée doit être réévalué et adapté.

Limitations historiques et/ou réglementaires

Certaines entreprises ont un héritage significatif d'anciens systèmes qui restent pour autant essentiel au business, il reste de nombreux mainframe par exemple qui ne peuvent pas être embarqués dans ce modèle. Il existe également des restrictions à l'adoption du Zero Trust du fait des exigences réglementaires qui imposent très souvent un modèle de type périmétrique. En effet, les obligations en tant que OIV (Opérateur D'importance Vitale) imposent un cloisonnement périmétrique de leur SIIV (Système d'Information d'Importance Vitale) et interdisent le déploiement dans le cloud.

Le virage vers le Zero Trust est un changement logique complet et est structurant pour les organisations. La démarche Zero Trust est donc à envisager sur le long terme et requiert souvent plusieurs années pour qu'elle couvre l'ensemble du système d'information, ceci étant d'autant plus vrai que le "legacy IT" est important. Cependant, pour les entreprises ayant choisi une transformation profonde de leur IT, il est parfois plus simple de repartir directement de ce modèle en migrant massivement vers le cloud par exemple. En somme, dans un cas il faudra savoir être patient et dans l'autre agile en s'inscrivant au plus tôt dans la stratégie de transformation.

Protiviti vous accompagne dans la démarche Zero Trust, de la stratégie à sa mise en œuvre

Les experts de Protiviti vous assistent dans cette transformation de fond qu'est le Zero Trust dans toutes les composantes de la démarche.

Les étapes proposées ci-dessous peuvent par exemple être mise en œuvre progressivement pour s'adapter à un historique/legacy contraignant.

➢ Etablir une stratégie d'adoption du modèle

- **Préparer une stratégie Zéro Trust Globale –** Nos ateliers de design thinking peuvent aider les organisations à élaborer et à communiquer la stratégie Zéro Trust, y compris l'accompagnement de la conduite du changement nécessaire au sein des équipes, tout cela en cohérence avec la gouvernance actuelle tout en la faisant évoluer.

- **Animer le groupe de travail avec les décideurs qui porteront la stratégie de Zero Trust –** Pour réussir, l'architecture Zero Trust nécessite un engagement au plus haut niveau de la direction et à travers l'ensemble des lignes de métier.

- **Évaluer la maturité de l'organisation à adopter le modèle –** En partant des éléments de gouvernance existants et des technologies en place. Protiviti peut ainsi aider les organisations à identifier les moyens et capacités à mobiliser, puis à élaborer une feuille de route avec le jalonnement des étapes.

➢ Réaliser un Gap Analysis et établir un plan d'action

- **Evaluer l'existant des principaux composants à considérer pour une mise en œuvre du Zero** – Identifier et prioriser les principaux composants nécessaires à la mise en œuvre et d'établir une feuille de route pour disposer d'un programme adressant les points présentés précédemment et en ligne avec la gouvernance proposée.

- **Évaluer l'intégration de ce design dans la méthodologie projets –** Cette évaluation permettra d'identifier et de comprendre les méthodes de projets au sein de l'entreprise et d'y intégrer les différents jalons de sécurité.

- **Proposer un plan d'action de déploiement de la méthode –** Ce plan pourra se décomposer en plusieurs étapes en fonction des contraintes organisationnelles de l'entreprise.

➢ Accompagner la mise en œuvre

- **Réaliser une analyse de risques cybersécurité –** Cette étape sera une phase structurante et permettra d'identifier les actifs critiques à protéger en priorité et structurer la démarche de déploiement autour de ces éléments critiques.

- **Réaliser une cartographie des données –** Cartographie de la localisation des données les plus critiques de l'organisation et de leur traitement.

- **Mettre à jour ou rédiger les politiques et les standards de sécurité afin d'homogénéiser la gouvernance –** Les politiques et les standards de sécurité doivent être mis à jour pour tenir compte des changements liés au Zéro Trust.

- **Organiser des ateliers de préparation –** Animer et coordonner les équipes opérationnelles en charge de l'infrastructure, l'exploitation et de la sécurité afin d'adresser les sujets tels que (N.B cette liste sera à établir lors de la validation du plan d'action) :

  - La conception du nouveau réseau

  - La protection des données et leur accès

  - La mise en place des outils de monitoring

  - L'automatisation et l'orchestration de la sécurité

➢ Piloter le dispositif

Contacts

Bernard Drui
Managing Director & Country Market Lead
Bernard.Drui@protiviti.fr

Emmanuel Christiann
Associate Director
Emmanuel.Christiann@protiviti.fr

Anis Hammami
Senior Manager
Anis.Hammami@protiviti.fr

Lyes Oussadit
Senior Manager
Lyes.Oussadit@protiviti.fr