Tendances technologiques

Les réseaux zéro confiance

Architecture d'entreprise, Direction générale du dirigeant principal de la technologie

Version 0.1
Date : 2019-5-8

Services partagés Canada
Shared Services Canada
Canada

Table des matières

Sommaire opérationnel

Les *réseaux zéro confiance* (ou « Zero Trust Networking [ZTN] ») désignent un modèle d'architecture de réseaux de données, proposé à l'origine par John Kindervag de la firme Forrester en 2010 et dont bien des éléments sont utilisés depuis plusieurs années. Le coût total de la cybercriminalité (des répercussions directes, mais aussi des mesures d'atténuation) devrait passer de 3 billions de dollars américains en 2015 à 5 billions de dollars américains d'ici 2020. Les solutions les plus courantes en matière de sécurité des données, de l'information et des réseaux s'articulent autour du concept de la *défense du périmètre*, aussi connu comme étant un *modèle de château et de douve*. Selon ce modèle, le périmètre extérieur de l'organisation est défendu (comme dans le cas de la douve d'un château), et les données peuvent entrer et sortir au moyen d'un ensemble de points d'accès très restreint (le *pont-levis* du château) qui sont mis en place comme pare-feu d'entrée et de sortie. L'hypothèse (autrefois valide) est que les auteurs de menace sont à l'extérieur, alors les intervenants situés à l'intérieur du périmètre sont *fiables*.

La réalité actuelle par rapport à la menace est nettement différente pour quelques raisons :

- La majorité des organisations encouragent actuellement l'utilisation massive de l'*informatique mobile* ainsi que de l'approche « *utilisez vos appareils personnels* », tout en augmentant la quantité de données et d'applications hébergées dans le nuage, ce qui fait disparaître complètement la notion de périmètre.
- Les *auteurs de menace* utilisent des techniques de plus en plus sophistiquées : en plus des pirates informatiques externes traditionnels, diverses attaques permettent désormais d'avoir accès à des intervenants internes volontaires et involontaires qui contribuent à l'infraction à la sécurité. Après avoir réussi à pénétrer une première fois dans un système, les attaquants sont habituellement en mesure de se *déplacer de façon latérale* vers plusieurs autres systèmes. Depuis quelques années, une augmentation des *menaces persistantes avancées* (MPA) a pu être observée dans tout le domaine de la menace.

Ces facteurs supposent que les auteurs de menace sont *déjà à l'intérieur* de l'organisation. Une première tentative pour atténuer le problème consiste à établir une *double limite de confiance* selon laquelle les serveurs contenant les « joyaux de l'organisation » sont protégés par une couche supplémentaire, bien que les données distribuées et l'infonuagique rendent cette protection insuffisante de nos jours.

À l'heure actuelle, le modèle des réseaux zéro confiance est la meilleure approche accessible en matière de mécanisme de défense[1]. Cette approche repose sur un certain nombre de principes :

- Toutes les *ressources sont accessibles de manière authentifiée*. Cette authentification de l'accès fait appel à une notion d'*identité*, laquelle s'applique aux humains, aux applications ou aux autres processus ayant accès aux données, à d'autres processus et services ou aux ressources informatiques. Cette méthode permet de minimiser les menaces internes potentielles ou les déplacements latéraux des auteurs de menace.
- Toutes les *ressources sont accessibles de manière sécurisée*. Lorsque l'accès est autorisé, l'information échangée est chiffrée de façon sécuritaire. Cette méthode permet de se protéger contre l'écoute clandestine des auteurs de menace déjà à l'intérieur de l'organisation.
- Un *« droit d'accès minimal »* (nécessaire pour accomplir le travail) est accordé à toute personne identifiée ayant besoin d'avoir accès aux ressources. Les répercussions du vol d'identité sont ainsi limitées.
- La *journalisation et l'inspection* de toutes les activités de trafic sur le réseau, de serveur et d'identité. Combiné à l'*analytique*, ce principe permet d'assurer l'existence d'une piste de vérification pour détecter les tentatives inhabituelles d'accès aux ressources.

Tous ces principes sont explicites et certains sont peut-être déjà en usage au sein des organisations, bien qu'une approche globale en ce qui concerne les réseaux zéro confiance nécessite l'intégration de leur utilisation ainsi que des aspects liés à la gouvernance et à la gestion du changement.

Sommaire technique

Heureusement, les réseaux zéro confiance sont très dépendants des *technologies existantes*, ce qui signifie que les risques techniques et les coûts sont bien compris. Ces technologies et approches architecturales sont les suivantes :

- *Gestion de l'identité et de l'accès*. Une gestion adéquate de l'identité est évidemment cruciale pour veiller à ce que toutes les tentatives d'accès aux ressources soient authentifiées et autorisées. Ces ressources peuvent être des données, mais aussi des services informatiques, des appareils, etc. Les systèmes d'information sont déjà conçus pour intégrer la notion d'identité des utilisateurs humains, mais la gestion de l'identité et de l'accès pour les réseaux zéro confiance nécessite que tous les utilisateurs potentiels d'une ressource soient également identifiés et autorisés. Cette gestion de l'identité et de l'accès doit s'appliquer aux

[1] Il convient de noter que la firme Forrester n'est plus « propriétaire » de cette approche dans la mesure où de nombreux fournisseurs offrent des solutions dites « zéro confiance ». Par ailleurs, les analystes de la firme concurrente Gartner ont créé un modèle beaucoup plus élaboré connu sous le nom de *Continuous Adaptive Risk & Trust Assessment* (CARTA) [évaluation continue du risque et de la confiance en matière d'adaptation] qui intègre en partie le principe de zéro confiance.

processus, par exemple un composant de logiciel qui en utilise un autre, ou des appareils *Internet des objets (IdO)* qui s'alimentent dans un *lac de données*. Ces scénarios d'utilisation font en sorte d'augmenter considérablement le nombre d'identités à gérer, jusqu'à plusieurs milliards lorsque l'IdO est inclus. En règle générale, cette identification non humaine (et parfois humaine) est fondée sur les serveurs mandataires d'identité comme l'adresse IP, laquelle est de toute évidence vulnérable aux attaques étant donné qu'elle peut être faussée. Les solutions modernes de gestion de l'identité et de l'accès utilisent des certificats, des signatures et une authentification à facteurs multiples aux fins d'assurance de la fiabilité. La capacité de traitement n'était pas suffisamment abordable pour justifier l'utilisation de ces solutions à grande échelle jusqu'à tout récemment. Ces techniques sont toutes mises en place à Services partagés Canada (SPC), bien que principalement à l'intention des employés, et elles auront peut-être besoin d'une mise à niveau au cours des années à venir pour minimiser les menaces associées à l'informatique quantique.

- *Micro-segmentation* des réseaux. La segmentation des réseaux est une technique bien connue pour séparer les sous-réseaux, à l'origine pour des raisons de performance, puis de sécurité. Lorsque la sécurité devient une motivation, la séparation entre deux segments de réseau peut être faite de façon efficace à l'aide d'un pare-feu qui inspecte le trafic réseau entre les segments, consigne le trafic problématique et autorise peut-être uniquement le trafic provenant de certaines adresses IP ou se conforme à des protocoles précis. Dans le cas des réseaux zéro confiance, il s'avère nécessaire d'utiliser une granularité fine –chaque machine (ou tout au plus un petit nombre de machines de même fonctionnalité) est essentiellement dans son propre micro-segment. De plus, le pare-feu entre les segments *doit* limiter le trafic à l'ensemble minimal de protocoles (types de trafic) requis. Si la machine qui offre un service n'utilise pas de fonction d'authentification, ce pare-feu interne effectue également la gestion de l'identité et de l'accès requise. Une adresse IP n'est en aucun cas suffisante pour l'authentification. Ces pare-feu internes exigent une capacité importante de journalisation et de génération de rapports plus centralisée (voir ci-dessous). Comme on peut s'y attendre, le placement de chaque machine dans un micro-segment entraîne une prolifération de pare-feu internes, bien que la capacité de traitement ait atteint le point où elle peut être mise en œuvre dans un logiciel par opposition au matériel monté sur châssis dans un centre de données. Dans le cas d'une infrastructure virtualisée ou infonuagique, le pare-feu et la micro-segmentation font partie du *réseau défini par le logiciel* (SDN), ce qui réduit encore plus le coût de mise en œuvre. Les mises en œuvre de type SDN comportent une mise en garde importante : elles nécessitent des *hyperviseurs* de virtualisation hautement sécurisés. Une violation d'un hyperviseur non sécurisé paralyserait les réseaux zéro confiance et donnerait accès à toutes les données et au trafic sur au moins cette machine physique spécifique.

- *Chiffrement omniprésent*. Étant donné que les auteurs de menace se trouvent effectivement à l'intérieur du « périmètre » de l'organisation et peuvent espionner le trafic réseau, toutes les interactions sur le réseau doivent être chiffrées. De plus, les données inactives doivent être chiffrées pour atténuer les risques associés aux

intrusions dans une base de données ou un serveur de fichiers en particulier. Les algorithmes, les unités centrales et les accélérateurs modernes ont rendu le chiffrement à grande échelle particulièrement rapide.

- *Politiques dynamiques et conditionnelles*. Le principe du « droit d'accès minimal » est une pierre angulaire des réseaux zéro confiance. Au cours de la période d'emploi d'une personne en particulier ou de la période active d'un processus, les privilèges et les accès requis varient selon la tâche, et ces privilèges devraient être maintenus au niveau le plus restreint qui permet encore d'exécuter le travail[2]. Dans la plupart des organisations, la pratique actuelle consiste à augmenter le niveau de privilège au besoin (peut-être même à le fixer au niveau « élevé » dès le départ) et à ne pratiquement jamais le diminuer. Les réseaux zéro confiance changent cette pratique en étant beaucoup plus dynamiques, et veillent à abaisser le niveau de privilège une fois que la tâche spécifique a été accomplie. Lorsque de telles politiques sont appliquées à des processus ou des dispositifs (et non à des personnes), elles peuvent être mises en œuvre au moyen d'architectures et d'interfaces de programmation d'applications pour les micro-services. Le fait qu'elles ne prennent en charge qu'un seul service signifie qu'elles peuvent exécuter des processus avec le moins de privilèges possible.

- *Journalisation, inspection et analytique*. Il faut toujours être au fait de la présence d'auteurs de menace, même dans les réseaux zéro confiance. La meilleure façon d'y parvenir est de procéder à une inspection approfondie du trafic (à l'aide des micro-segments) et de consigner les données connexes dans des fichiers journaux. Plutôt que de faire l'objet d'une inspection manuelle, les fichiers journaux sont généralement traités par des algorithmes de science et d'analytique des données (pour des raisons de sécurité) et d'apprentissage machine pour relever les anomalies qui indiquent des tentatives d'attaque. Les analyses qui en résultent sont utilisées pour générer des rapports et des visualisations nécessaires à la gouvernance des réseaux zéro confiance.

Utilisation par l'industrie

Peu de données chiffrées ont été recueillies sur l'adoption des réseaux zéro confiance au sein de l'industrie, bien qu'il soit universellement reconnu que cette stratégie est actuellement la plus efficace pour la *sécurité de l'information*. Des banques technophiles, des entreprises de médias sociaux (LinkedIn, Facebook), des plates-formes d'achat en ligne (Amazon) et des fournisseurs d'infrastructure (Apple, Google, Microsoft) chefs de file ont tous mis en œuvre des réseaux zéro confiance dans une certaine

[2] Ce principe doit absolument tenir compte des questions liées à la gestion du changement et aux ressources humaines, car les employés se sentent inévitablement frustrés ou gênés dans l'exécution efficace de leur travail de routine. Pour cette raison, une certaine latitude est nécessaire dans l'interprétation du « droit d'accès minimal ».

mesure, mais parfois uniquement pour les renseignements les plus confidentiels à propos de leurs clients ou pour leurs systèmes financiers.

Des produits de réseaux zéro confiance sont également offerts par des fournisseurs de premier plan d'infrastructures de réseau, de services d'infonuagique et de services de chiffrement.

Utilisation par le gouvernement du Canada

Tel qu'il a été mentionné dans la section *Sommaire opérationnel*, la majorité des composants des réseaux zéro confiance sont déjà utilisés quelque part. Plus précisément, les entités responsables de la défense, des renseignements de sécurité et des services de police (le ministère de la Défense nationale, le Centre de la sécurité des télécommunications, le Service canadien du renseignement de sécurité et la Gendarmerie royale du Canada) ont déjà de vastes réseaux zéro confiance en place, ainsi que sur le plan interpersonnel (et non seulement des systèmes de technologie de l'information), selon le principe du « besoin de savoir » et du « droit d'accès minimal ».

Répercussions pour Services partagés Canada (SPC)

Proposition de valeur

La proposition de valeur de SPC a pour toile de fond les nouvelles réalités suivantes :

- Menaces plus sophistiquées : de l'intérieur, mais aussi des MPA, dont certaines peuvent être des offensives menées par des États-nations.
- Aucun périmètre de défense au gouvernement du Canada (et pour SPC et ses clients en particulier), en raison de la répartition géographique, des incitatifs au télétravail, des appareils mobiles, de l'approche « utilisez vos propres appareils », des villes intelligentes, de l'IdO et, de façon encore plus importante, de la vaste utilisation de l'infonuagique.

En d'autres termes, les auteurs de menace sont généralement déjà à l'intérieur de l'organisation grâce à des attaques et à des mouvements latéraux d'intervenants internes.

La proposition de valeur la plus évidente pour SPC et ses clients est de réduire le coût associé à la cybercriminalité et aux cyberattaques – un coût qui se calcule en multipliant le *risque* par les *répercussions* (en dollars). Le montant exact est difficile à quantifier, mais les réseaux zéro confiance réduisent les deux facteurs du coût.

Les réseaux zéro confiance sont faciles à déployer *progressivement* : chaque fois que l'architecture de l'infrastructure est renouvelée (par exemple, en migrant vers l'infonuagique), les réseaux zéro confiance peuvent être intégrés comme une décision

de mise en œuvre de base. L'évolutivité d'une telle approche progressive est particulièrement importante compte tenu de l'utilisation grandissante de l'IdO par les clients de SPC, ce qui, en fin de compte, donnera lieu à l'interconnexion de milliards de dispositifs.

Enfin, le coût de la gouvernance de la technologie de l'information peut être réduit grâce aux réseaux zéro confiance, car des limites d'accès claires sont établies et beaucoup plus de données sont consignées concernant l'accès aux ressources.

Difficultés

Divers composants des réseaux zéro confiance sont déjà en place au sein de SPC et le premier défi concerne deux aspects de la gestion du changement : cesser de présumer qu'un périmètre est en place et de faire confiance à tous les intervenants internes (personnes ou systèmes); et effectuer la transition sans nuire aux relations entre les employés et SPC, où la confiance fait implicitement partie de la valorisation des employés. Le calendrier de déploiement des réseaux zéro confiance nécessitera d'établir les priorités en ce qui concerne certaines ressources (y compris les employés), tout en encourageant l'appréciation du gain sur le plan de la sécurité.

Puisque la gestion de l'identité fait partie intégrante des réseaux zéro confiance, les concepts d'identité existants de SPC devront être adaptés. Actuellement, la *gestion des justificatifs internes et externes* étend les notions de justificatifs d'identité (nom d'utilisateur et mot de passe) vers une véritable gestion des identités, et les défis les plus importants seront de permettre aux *dispositifs d'avoir une identité* (par exemple, les dispositifs d'IdO) et aussi une évolutivité (vers des milliards de dispositifs d'IdO).

D'un point de vue technique, les initiatives importantes de SPC pour adopter une infrastructure infonuagique facilitent la mise en œuvre des réseaux zéro confiance, mais celle-ci sera dépendante du recours à des hyperviseurs de très haute qualité pour la virtualisation. L'ensemble des réseaux zéro confiance échoue si un auteur de menace réussit à avoir accès à un hyperviseur. Le chiffrement et l'authentification de la plupart ou de la totalité des données et l'accès aux ressources nécessiteront également de nombreux calculs et le budget requis doit donc être établi en fonction des besoins matériels.

Considérations

SPC met déjà en œuvre les composants des réseaux zéro confiance sous diverses formes et la feuille de route devra être prise en considération pour en maximiser l'incidence. La gestion du changement est l'aspect le plus important, car cette transition touche directement l'état d'esprit des employés de SPC et des clients : penser en termes d'auteurs de menace déjà présents (virtuellement et numériquement) à l'intérieur de l'organisation. Au fur et à mesure que SPC accroît sa vigilance à cet égard, il faudra aussi déterminer de quelle façon maintenir l'engagement des employés alors que le concept

de zéro confiance donne, au moins superficiellement, le message de « ne faire confiance à personne » et exige le recours au principe du « droit d'accès minimal ». Il s'agit également d'une excellente occasion de songer à améliorer la qualité et l'efficacité de la production de rapports et de la gouvernance, comme le permettent les réseaux zéro confiance.

D'un point de vue logistique, l'engagement de SPC à l'égard de l'infonuagique représente le moment idéal et le meilleur moyen pour intégrer les réseaux zéro confiance. Tous les analystes conviennent que les systèmes devraient être des *réseaux zéro confiance dès la conception* plutôt que de les utiliser comme solution ultérieure. SPC devrait donc considérer ou reconsidérer l'inclusion des réseaux zéro confiance dans les feuilles de route de l'infonuagique. Puisque les réseaux zéro confiance nécessitent des mesures de chiffrement et d'authentification additionnelles, cette approche aura des répercussions sur les coûts de la migration vers l'infonuagique.

Enfin, il faut envisager d'élargir la portée de l'infrastructure actuelle de gestion des identités (gestion des justificatifs internes et externes) afin que les dispositifs et les processus deviennent des *intervenants identifiés* au sens large au sein de SPC, et que les autorisations, les accès et les activités qui y sont associés soient correctement gérés et consignés.

Références

- CSO from IDG, *What is Zero Trust? A model for more effective security*. https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html [en anglais seulement]
- Gartner, *Zero Trust is an Initial Step on the Roadmap to CARTA*, 10 décembre 2018. https://www.gartner.com/doc/reprints?id=1-641B4AK&ct=190114&st=sb [en anglais seulement]
- Forrester, *Defend Your Digital Business From Cyberattacks Using Forrester's Zero Trust Model*, 12 septembre 2018. https://reprints.forrester.com/#/assets/2/716/RES61555/reports [en anglais seulement]
- Doug Barth et Evan Gilman, *Zero Trust Networks*, O'Reilly Publishing, juillet 2017. [en anglais seulement]