SOPHOS
Cybersecurity delivered.

L'importance du ZTNA : l'avenir des réseaux sécurisés

Le ZTNA sécurise l'accès distant et protège contre les ransomwares

Un livre blanc Sophos. Février 2022

En matière de cybersécurité, tout est une question de risques et de confiance. Faites-vous confiance à l'utilisateur qui vient de se connecter à votre réseau ? À celui qui essaie d'accéder aux applications de l'entreprise ? Et cet email qui semble provenir de votre partenaire commercial mais qui contient des requêtes inhabituelles, signe éventuel d'une attaque de compromission ? Si dans les années 80, la pratique générale était de « faire confiance mais vérifier », aujourd'hui le curseur s'est déplacé : « Ne faites confiance à rien, vérifiez tout ».

Avec ce nouveau modèle « Zero Trust » ou confiance zéro, quiconque souhaitant accéder au réseau doit être authentifié. Mais ce n'est pas tout. Toute tentative d'accès à une ressource réseau, telle qu'un serveur, une application ou des données, exige que l'appareil ou l'application utilisé pour accéder à cette ressource soit également vérifié pour valider sa conformité, puis ré-authentifié et validé à chaque nouvelle requête.

En matière de cybersécurité, la confiance ne se donne pas, elle se gagne. Chaque fois que l'utilisateur, l'appareil ou l'application tentent une action sur le réseau, le processus d'authentification est relancé.

Qu'est-ce que le ZTNA ?

Comme nous l'avons vu, le Zero Trust Network Access (ZTNA) repose sur le principe de la confiance zéro, autrement dit « Ne faites confiance à rien ni personne, vérifiez tout ». Ce modèle renforce considérablement la sécurité : il traite chaque utilisateur, appareil et application comme son propre périmètre sur son propre micro-segment du réseau, et il évalue constamment leur identité et leur état avant de valider et autoriser l'accès aux applications et aux données de l'entreprise. Les utilisateurs n'ont accès qu'aux applications et aux données définies explicitement par leurs politiques, ce qui réduit les mouvements latéraux et les risques qui en découlent.

Les victimes de ransomwares sont davantage familiarisées avec l'approche ZTNA, sans doute soucieuses de prévenir des attaques ultérieures. Nous approfondirons ce point un peu plus loin et nous verrons comment les utilisateurs Sophos appréhendent et utilisent la technologie ZTNA.

Le ZTNA fait partie intégrante du cadre de sécurité SASE (Secure Access Service Edge) qui décrit comment la sécurité du réseau et la sécurité du Cloud convergent au sein d'une seule et unique plateforme opérée dans le Cloud. Le SASE, concept introduit pour la première fois par Gartner en 2019, consiste essentiellement en une fusion des fonctionnalités traditionnelles de gestion et de sécurité des réseaux étendus (WAN) à l'aide d'architectures Cloud-native. Outre le ZTNA, l'architecture SASE comprend des agents de sécurité d'accès au Cloud, des pare-feux as-a-service, des systèmes de prévention des intrusions (IPS) et des passerelles d'accès sécurisé.

La gestion dans le Cloud offre des avantages considérables : vous pouvez être opérationnel instantanément, réduire votre infrastructure de gestion, faciliter le déploiement et l'enrôlement, et y accéder en tout lieu. L'un des principaux avantages de la gestion Cloud est de pouvoir se connecter et commencer à utiliser la solution instantanément, sans ajouter de serveurs ou d'infrastructure de gestion supplémentaires. La gestion Cloud offre également un accès sécurisé instantané de n'importe où et sur n'importe quel appareil, vous permettant de travailler comme vous le souhaitez. Elle permet enfin d'enrôler facilement de nouveaux utilisateurs, où qu'ils se trouvent dans le monde.

Mettre en œuvre le ZTNA, cependant, constitue une étape essentielle pour renforcer la sécurité des utilisateurs distants, pour améliorer significativement la sécurité dans un environnement réseau d'utilisateurs distants soumis à une pandémie ou encore pour protéger le réseau d'entreprise contre les attaques de malware et de ransomware.

Déconstruire la menace VPN

Si la pandémie a fait de terribles dégâts sur le plan humanitaire, elle a eu pour conséquence inattendue mais significative d'améliorer l'accès à distance, avec le déploiement du ZTNA à la place du vulnérable VPN. La crise sanitaire a obligé des millions d'individus à abandonner leur environnement de travail familier pour passer au télétravail, créant ainsi des millions de nouveaux postes de travail vulnérables, souvent hors du contrôle du personnel informatique de l'entreprise.

Ces postes sont devenus des cibles de choix pour les attaquants, une bonne partie n'étant plus protégée par la protection de niveau professionnel de l'entreprise. En outre, ces millions de nouveaux télétravailleurs ont fait peser un poids énorme sur les VPN d'entreprise qui n'avaient pas l'habitude d'une telle charge de travail.

Le ZTNA applique les principes du Zero Trust tout en remplaçant le VPN (méthode traditionnelle pour relier les utilisateurs distants au réseau de l'entreprise) devenu problématique. Techniquement parlant, les VPN présentent trois inconvénients majeurs pour les télétravailleurs d'aujourd'hui.

Premièrement, les VPN ne sont pas conçus pour s'adapter aux exigences des grandes entreprises qui comptent un nombre relativement important d'employés à distance. Deuxièmement, les clients VPN sont souvent des logiciels anciens, négligés et complexes, et donc des cibles potentielles intéressantes pour les attaquants. Le fait qu'ils reposent sur une approche de connexion classique Nom d'utilisateur/Mot de passe présente également des failles de sécurité. Enfin, les utilisateurs accédant au réseau via un VPN gagnent une mainmise sur tout le réseau dès lors qu'ils se sont connectés. Selon les contrôles réseau en interne, cela peut poser problème.

Examinons chacun de ces problèmes et la manière dont le ZTNA les résout.

Les VPN sont mal adaptés. Parmi les limites des VPN, on peut citer la bande passante maximale qui est souvent limitée à 1 Gbit/s, les ports exposés qui peuvent être exploités, les attaques man-in-the-middle potentielles et les accès surprivilégiés. De plus, les VPN sont conçus pour gérer un volume spécifique d'utilisateurs distants et ne peuvent pas accroître ou diminuer leur capacité de manière dynamique. Si le volume est trop élevé, par exemple, certains utilisateurs ne peuvent pas accéder au VPN tant que d'autres ne se sont pas déconnectés.

Deuxièmement, les vulnérabilités des VPN ont été citées dans plusieurs avis de cybersécurité émis par l'Agence nationale de sécurité des États-Unis et, en 2019, le Centre de cybersécurité canadien a publié des recommandations indiquant que trois produits VPN populaires présentaient de multiples indicateurs de compromission pour la détection d'activités malveillantes. Il s'agissait notamment de réinitialisations d'identifiants et de protocoles VPN SSL et TLS propriétaires vulnérables.

Enfin, les VPN ne fournissent aucun filtre lorsqu'un utilisateur se connecte à un réseau. En fait, l'utilisateur dispose de tous les privilèges comme s'il était sur un poste de travail derrière le pare-feu de l'entreprise.

Il existe deux façons de réduire la menace liée aux outils d'accès à distance qui permettent à un attaquant de se déplacer sur un réseau : Premièrement, exiger que chaque entrée sur le réseau authentifie l'utilisateur, l'appareil et le logiciel uniquement sur un micro-segment spécifique du réseau. Ainsi, même si l'attaquant réussit à obtenir un accès, ses déplacements sont limités. Deuxièmement, limiter considérablement les privilèges de chaque individu sur le réseau. Ainsi, si l'attaquant ne peut pas voir le réseau à cause de privilèges limités, il ne peut pas le parcourir.

Le rapport « NewWave : Zero Trust Network Access, Q3 2021 » de Forrester mentionne que « Avec le ZTNA, les utilisateurs peuvent accéder aux applications sur site en utilisant les principes du Zero Trust, tout en permettant au trafic de visioconférence bidirectionnel de s'effectuer directement via Internet, améliorant ainsi la posture de sécurité et l'expérience des employés ». « En fin de compte, le ZTNA réduit le besoin de VPN pour les employés et permet aux équipes d'infrastructure et de sécurité d'envisager l'adoption de fonctionnalités réseau et de sécurité dans le Cloud. »

ZTNA ou la zen attitude

Du point de vue de la gouvernance d'entreprise, l'une des priorités est de gérer les personnes qui se connectent au réseau et ce qu'elles font. L'objectif de la fonction de gouvernance est d'avoir des politiques de sécurité et des procédures en place qui déterminent le mode opératoire de l'entreprise, ainsi que des pratiques commerciales éthiques et solides qui soutiennent sa viabilité financière. Or, des acteurs malveillants peuvent s'immiscer dans le réseau, compromettre ou voler des données confidentielles, installer des ransomwares et autres malwares, ou simplement rester en mode furtif en attendant un moment plus opportun pour attaquer. Non seulement ces menaces peuvent entraîner la violation des règles de conformité et coûter à l'entreprise des sommes considérables, mais elles peuvent également affecter, voire anéantir, sa valeur sur le marché.

Le déploiement d'un modèle réseau Zero Trust en général et d'une approche ZTNA en particulier permet, d'une part, d'identifier les intrus sur le réseau, les applications malveillantes et bénignes, et les utilisateurs non autorisés. D'autre part, il réduit considérablement la surface d'attaque du réseau, améliorant ainsi le profil de risque global de l'entreprise.

Lorsque des utilisateurs accèdent à un réseau équipé du ZTNA, leurs appareils accèdent aux ressources du réseau sur leur propre périmètre micro-segmenté qui est validé et vérifié en permanence. Avec le Zero Trust, les utilisateurs ne sont plus « sur le réseau de l'entreprise » proprement dit. La confiance et les privilèges d'accès implicitement accordés auparavant disparaissent. Ils n'ont plus accès qu'aux segments du réseau pour lesquelles eux-mêmes et leurs appareils ont été authentifiés. Ce n'est pas le cas avec les connexions VPN traditionnelles.

Dans un réseau traditionnel, le pare-feu empêche les attaques, mais peu de défenses sont véritablement en place une fois que les identifiants d'un utilisateur ont été acceptés. Les attaquants peuvent alors se déplacer librement, à la recherche d'identifiants aux privilèges supérieurs qui leur permettent d'accéder à des parties plus sécurisées du réseau, et ainsi voler, copier, corrompre des données ou les chiffrer contre une rançon.

Avec une infrastructure Zero Trust, non seulement le vol d'identifiants devient beaucoup moins intéressant, mais le pare-feu n'est plus que l'un des nombreux dispositifs de sécurité des données et des applications. Même si un employé en télétravail a son ordinateur piraté, ses identifiants ne seront pas suffisants une fois que l'attaquant aura accédé au réseau de l'entreprise.

L'approche ZTNA ne lui donne accès qu'à une partie limitée du réseau. Et cela suppose qu'il ait les identifiants pour s'authentifier lui-même, l'appareil et le logiciel pour une application ou des données approuvées.

Vaincre les ransomwares

Dans le rapport Sophos L'état des ransomwares 2021, 37 % des personnes interrogées ont déclaré avoir subi une attaque de ransomware l'année précédente, 54 % d'entre elles affirmant que les cybercriminels avaient réussi à chiffrer leurs données. En termes de perte de données, la bonne nouvelle est qu'elles étaient 96 % à avoir récupéré au moins une partie de leurs données. La mauvaise est que, en moyenne, seuls 65 % des données chiffrées ont été récupérées après le paiement de la rançon.

Selon le rapport, la rançon moyenne versée par les organisations de taille moyenne s'élevait à 170 404 dollars en 2020 (soit environ 140 000 euros). Mais cette somme ne représente qu'une partie de la facture totale. Si l'on prend la plus récente attaque de ransomware (en tenant compte des temps d'arrêt, des ressources humaines nécessaires, du coût des équipements et du réseau, du manque à gagner, de la rançon payée, etc.), le coût moyen de remédiation avoisinait les 1,85 million de dollars (env. 1,52 million d'euros), soit plus du double du coût rapporté en 2020 (761 106 $/env. 627 000 000 €).

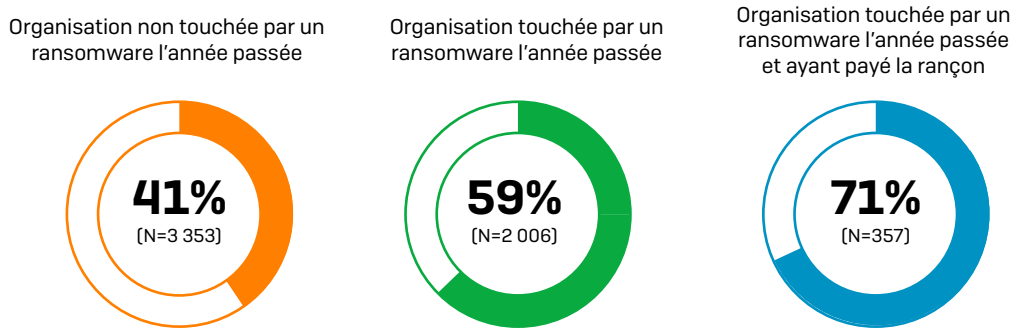
Dans une récente enquête menée par Vanson Bourne et commanditée par Sophos auprès de 5 400 professionnels de l'informatique dans le monde, 20 % des répondants ont déclaré avoir déjà implémenté une approche Zero Trust ; 41 % ont déclaré avoir déjà commencé à la mettre en œuvre en espérant qu'elle soit terminée début 2022. Enfin, 20 % espèrent l'avoir en place pour début 2023.

Les solutions ZTNA éliminent un vecteur d'attaque courant des ransomwares et d'autres attaques d'infiltration de réseau. Puisque les utilisateurs ne sont plus « sur le réseau » mais plutôt sur un micro-segment du réseau de l'entreprise, les menaces qui auparavant pouvaient s'immiscer avec le VPN n'ont nulle part où aller avec le ZTNA.

Les attaques de ransomware encouragent l'adoption du ZTNA

L'enquête révèle que les professionnels IT des organisations victimes de ransomware au cours de l'année précédente sont près de 50 % à bien connaître l'approche ZTNA par rapport à ceux dont les organisations n'ont pas connu d'incident (59 % contre 39 %). Ce pourcentage passe à 71 % pour les entreprises qui ont été touchées et qui ont payé la rançon.

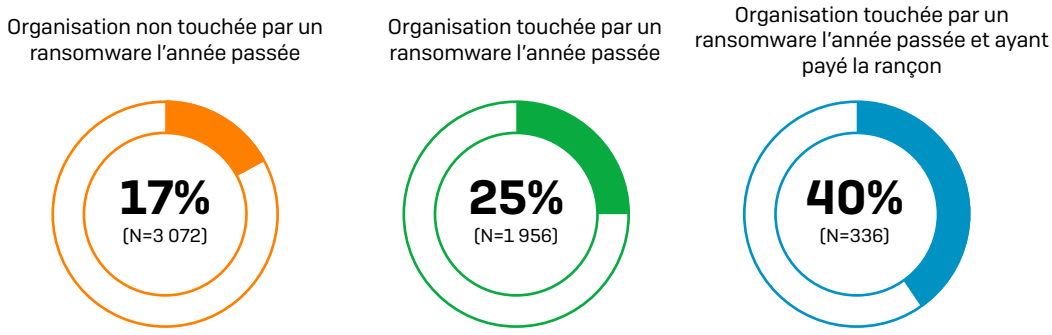
Pourcentage des personnes interrogées considérant « très bien connaître » l'approche ZTNA (Zero Trust Network Access).



Pour illustrer davantage ce point, seulement 10 % des victimes de ransomware connaissent peu ou pas du tout l'approche ZTNA, contre 21 % pour les organisations n'ayant pas été victimes.

L'enquête a également montré que les victimes de ransomwares sont plus avancées dans leur adoption du Zero Trust. Un quart (25 %) des personnes dont l'organisation a été victime d'une attaque de ransomware l'année passée a déjà pleinement adopté une approche Zero Trust, contre 40 % pour les organisations ayant été touchées et ayant payé la rançon. En comparaison, seulement 17 % (une sur six) des entreprises n'ayant pas subi d'attaque ont déjà totalement migré vers cette approche.

Pourcentage des répondants dont l'organisation a déjà adopté une approche Zero Trust



Par ailleurs, les victimes de ransomware semblent avoir des motivations différentes dans leur adoption du ZTNA.

- En effet, on a demandé aux interrogés ce qui les motivait à adopter une approche Zero Trust et, bien qu'il y avait des dénominateurs communs, on a également noté des différences claires. « Améliorer notre posture globale de cybersécurité » était la motivation la plus courante aussi bien pour les victimes que les non-victimes.
- La deuxième motivation la plus fréquente chez les victimes de ransomware était le souhait de « simplifier nos opérations de cybersécurité » (43 %), impliquant qu'une sécurité trop complexe avait peut-être contribué à leur dernière attaque.
- Un autre facteur clé était de « passer d'un modèle CAPEX à un modèle OPEX » (27 % contre 16 %, et jusqu'à 34 % parmi les organisations ayant été touchées et ayant la rançon).
- Enfin, la volonté de « soutenir notre évolution vers une utilisation accrue du Cloud » (42 %) a également été citée comme une motivation importante. Ce chiffre tombe à 30 % pour les organisations n'ayant pas subi d'attaque récente.

Perspectives pour l'avenir

Les avantages d'un environnement Zero Trust peuvent être difficiles à expliquer aux équipes dirigeantes et aux actionnaires, dans la mesure où il n'est pas facile de prouver qu'une attaque a échoué ou qu'elle n'a tout simplement jamais eu lieu parce que l'attaquant a été bloqué avant de pouvoir injecter son malware. Néanmoins, il est possible de démontrer que le Zero Trust réduit considérablement les risques et cet avantage peut être monétisé par l'entreprise.

Par exemple, il peut se traduire par une baisse des primes et de meilleures conditions d'assurance, et éventuellement une valorisation de l'entreprise sur le marché. Les courtiers et les spécialistes en cyberassurance reconnaissent qu'un risque plus faible entraîne une diminution des incidents, et donc des indemnités moins élevées. De ce fait, l'industrie de la cyberassurance procède actuellement à une réévaluation et à une modification des conditions de souscription des polices d'assurance cyber afin d'offrir de meilleures conditions aux entreprises qui réduisent leurs risques de manière proactive.

En mai 2021, le décret présidentiel américain sur l'amélioration de la cybersécurité du pays émis par Joe Biden a stipulé que le gouvernement fédéral devait « adopter les meilleures pratiques en matière de sécurité [et] progresser vers une architecture Zero Trust… ». L'adoption d'une approche Zero Trust par le plus grand employeur du pays montre à quel point ce modèle est considéré comme la voie à suivre pour minimiser les risques.

Pour Gartner, le Zero Trust est l'avenir de la cybersécurité. « La protection des données doit être une priorité absolue pour les grandes entreprises, qu'elles soient novices ou bien avancées dans leur transition vers le Cloud », a déclaré le cabinet. Selon Gartner, 82 % des entreprises prévoient de laisser leurs employés travailler à distance pendant un certain temps. « Avec le télétravail qui se généralise à long terme, la sécurité est devenue une priorité pour les entreprises. Cependant, beaucoup commencent à se rendre compte que leur approche traditionnelle de la sécurité n'est pas adaptée à leurs employés distants du Cloud-native », écrit Gartner.

Forrester appuie cette affirmation, notant que le Zero Trust sécurise les ressources plutôt que le réseau physique. « Dans ses formes les plus simples, le modèle Zero Trust déplace le focus des différents types d'authentification et de contrôles d'accès vers des contrôles ciblés portant sur les bases de données, les applications, les systèmes et les réseaux sensibles », rapporte le cabinet. « Ces contrôles exploitent les identités, activent ou désactivent les utilisateurs et déterminent leur accès en fonction de rôles définis. »

Si l'avenir est au Zero Trust, tout commence par le contrôle des personnes qui sont sur le réseau, des ressources auxquelles elles peuvent accéder et comment. C'est la *raison d'être* du ZTNA et pourquoi il est essentiel pour l'avenir de la cybersécurité.

Plus d'informations sur la page
Sophos.fr/ztna

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

22-02-06 FR(MP)

SOPHOS