FORTINET

LIVRE BLANC

Sécuriser l'innovation numérique exige un modèle d'accès zero-trust

Les RSSI font face à de nouveaux risques alors que la surface d'attaque s'étend

Synthèse

Pour accélérer leur business et rester compétitives, les entreprises adoptent des projets d'innovation digitale. Il en résulte que les applications et les données d'entreprise sont désormais présentes et disséminées en dehors des sites corporate pour permettre aux travailleurs d'accéder à davantage de ressources d'entreprise, à partir de nombreux endroits. Pour cette raison, le périmètre réseau traditionnel s'estompe tandis que la surface d'attaque s'élargit. Une réelle préoccupation pour les RSSI.

En réponse à ces menaces, les entreprises doivent adopter une approche de sécurité qui consiste à ne faire confiance à aucune personne, à aucun dispositif. Plus précisément, les RSSI doivent protéger le réseau avec un accès zero-trust, autrement dit, un accès à vérification systématique. Cette stratégie s'assure que tous les utilisateurs, dispositifs et applications Web du cloud sont fiables et authentifiés, et qu'disposent de privilèges d'accès pertinents. Le zero-trust devient ainsi un levier essentiel pour sécuriser tous les projets d'innovation digitale.

81 % des dirigeants d'entreprises déclarent que les collaborateurs constituent désormais le principal risque pour la sécurité mobile.[1]

L'évolution du edge réseau

Pour toutes les entreprises, les projets d'innovation digitale sont des moteurs de croissance. Cette croissance va néanmoins multiplier les edges réseau : infrastructures cloud privées et publiques, objets connectés (IoT) et appareils mobiles, sites distants bénéficiant d'une connectivité de type Software-Defined (SD), etc. Il en résulte une croissance exponentielle du volume de données, d'applications et de workflows. Pour gérer l'accès des utilisateurs et interconnecter différents dispositifs disséminés géographiquement (sur et hors du réseau), les entreprises ont recours à de nouveaux dispositifs déployés sur les edges réseau.

Pour les RSSI, cette situation est tout sauf idéale. La démultiplication des edges réseau au fil des années récentes, jusqu'à faire disparaître le traditionnel périmètre réseau, crée un environnement ouvert… Et idéal pour les attaques ! Les cybermenaces sont de plus en plus prolifiques et s'adaptent continuellement. Dans le passé, la sécurité du périmètre réseau était basée sur une approche de « confiance et de vérification ». Mais avec autant d'utilisateurs, d'appareils et d'applications sur le réseau, reste à savoir à qui/quoi faire confiance. En détournant des identifiants et en utilisant des malware, les cybercriminels tentent d'accéder à des comptes légitimes. Une fois dans la place, ils identifient facilement les moyens de se mouvoir au sein d'un réseau interne non segmenté et défini comme étant de confiance. À partir d'un dispositif edge, ils peuvent lancer des attaques pouvant aboutir à une mise à l'arrêt opérationnelle, des vols de données, des pertes financières et des atteintes à la réputation de l'entreprise ciblée.

Pour les responsables de la sécurité, il est impossible de suivre le nombre croissant d'attaques en se contentant d'une approche traditionnelle à l'accès aux réseaux. D'où une évolution des mentalités : les évènements et les dispositifs sur le réseau ne peuvent plus être plus considérés comme étant de confiance. Avec un modèle d'accès zero-trust, les RSSI structurent leur approche en définissant des zones vulnérables spécifiques de l'edge réseau et en leur retirant toute confiance par défaut : les utilisateurs, les dispositifs et les ressources sur et hors réseau.

Savoir *qui* est connecté au réseau

Les responsables de la sécurité doivent savoir à tout moment qui se trouve sur leur réseau. Cependant, les entreprises subissent un risque supplémentaire lorsque les collaborateurs utilisent des mots de passe faibles pour se connecter au réseau. De nombreux comptes exigent désormais une identification, mais les mots de passe restent encore souvent trop faibles et donc faciles à pirater, via une attaque de phishing par exemple. Il est essentiel pour les entreprises de connaître chaque utilisateur et le rôle qu'il joue dans l'entreprise. C'est sur cette base qu'elles peuvent accorder en toute sécurité l'accès aux ressources nécessaires pour chaque rôle ou poste, avec la possibilité de fournir des accès supplémentaires au cas par cas.

Le BYOD, à savoir l'utilisation de dispositifs personnels dans un cadre professionnel est une pratique courante parmi les collaborateurs et les managers. Mais certains RSSI en négligent les dangers. La surface d'attaque élargie permet aux menaces en évolution de percer plus facilement les défenses sur la périphérie réseau traditionnelle, puis de se mouvoir au sein du réseau interne. Ce type d'intrusion peut passer inaperçu pendant de longues périodes. Certaines des intrusions les plus préjudiciables ont pour origine des utilisateurs non autorisés qui ont accédé au réseau ou des niveaux d'accès inappropriés accordés à des utilisateurs de confiance. Le BYOD devient omniprésent dans les entreprises, et 83 % des responsables de la sécurité affirment que leur entreprise est confrontée à des menaces mobiles.[2]

La dissémination géographique des collaborateurs est un autre défi pour les entreprises, puisque ces collaborateurs travaillent en différents endroits : siège social de l'entreprise, sites distants et, de plus en plus, leur domicile. Avec autant d'utilisateurs accédant à distance au réseau, la surface d'attaque est plus encline à s'élargir. Par exemple, les collaborateurs se connectent souvent à des hotspots ou des réseaux Wi-Fi publics dans les cafés, les aéroports, les voitures ou dans les transports publics. Cette connectivité présente des risques majeurs de sécurité. Des tiers peuvent capter les informations qui transitent entre l'utilisateur et le réseau de l'entreprise. Les assaillants peuvent exploiter des vulnérabilités logicielles non corrigées pour injecter des logiciels malveillants dans le terminal, et ainsi accéder à des informations locales et au réseau d'entreprise via le terminal.

Nombre des attaques les plus dommageables pour les entreprises sur ces dernières années sont issues de dispositifs réseau présents sur l'edge.[3]

Ces défis sont d'autant plus critiques que le télétravail se généralise. C'est précisément ce que constatent les entreprises lors de la pandémie de COVID-19. La plupart des entreprises, qui avaient prévu que moins de 15 % de leurs effectifs seraient basés à distance, ont soudain dû s'assurer qu'elles disposaient de l'infrastructure de sécurité adéquate pour 90 % de leur effectif, voire plus.

Ces besoins expliquent en partie l'importance d'un accès zero-trust. Étant donné que les dispositifs se déplacent constamment sur et hors du réseau, les responsables de la sécurité doivent connaître les utilisateurs sur le réseau et s'assurer qu'ils disposent de niveaux d'accès pertinents. D'autre part, lorsqu'un salarié évolue d'un poste à un autre, il n'a peut-être pas besoin d'accéder aux mêmes ressources que dans son rôle précédent, et les équipes de sécurité doivent pouvoir mettre à jour son accès en douceur.

Identifier *ce qui* est connecté au réseau

Si connaître les utilisateurs présents sur le réseau s'impose, les responsables de la sécurité également savoir à tout moment les dispositifs qui y sont connectés. La prolifération des appareils mobiles et des objets connectés a décliné le périmètre réseau traditionnel en de nombreux micro-edges, qui sont autant de vecteurs d'attaque. Chaque micro-edge est associé à un dispositif utilisateur, faisant ainsi des terminaux des cibles privilégiées pour les logiciels malveillants et les exploits sophistiqués.

En raison de cette prolifération des terminaux et de l'élargissement de la surface d'attaque, de nombreuses organisations perdent intrinsèquement le contrôle de leur réseau : ils ne savent plus quels sont les appareils qui s'y connectent. En fait, il n'existe pratiquement aucune configuration normalisée pour les dispositifs BYOD ou les objets connectés. En ce qui concerne le BYOD, les appareils mobiles sont des vecteurs de risques pour les réseaux. Ces risques portent sur des fuites de données, un Wi-Fi non sécurisé, le spoofing du réseau, le phishing, les logiciels espions, un chiffrement défectueux ou de mauvaise gestion des sessions. Cependant, le principal moteur d'expansion de la surface d'attaque des terminaux reste l'explosion des dispositifs IoT.

Les cyberattaques contre les appareils IoT sont en plein essor, car les organisations connectent de plus en plus d'appareils « intelligents ». Les acteurs malveillants tirent parti de ces appareils pour mener des attaques par déni de service distribué (DDoS), ainsi que de nombreux autres types d'actions malveillantes.

Afin de sécuriser totalement les terminaux BYOD et les objets connectés, les entreprises doivent avoir une visibilité sur l'emplacement de chaque appareil, sur son activité et sur la façon dont il se connecte aux autres appareils via le réseau. Toute carence de visibilité rend l'organisation vulnérable à des risques fortuits. Les responsables de la sécurité doivent être en mesure de suivre les appareils en périphérie du réseau. Pourtant, près de la moitié des professionnels de la cybersécurité déclarent ne pas avoir planifié la prise en charge des attaques sur les objets connectés de l'IoT, même si neuf sur dix expriment des inquiétudes quant aux menaces futures.[4]

La segmentation traditionnelle des réseaux est utilisée par certaines entreprises, mais il est difficile de définir des segments sécurisés qui seraient ouverts à tous les utilisateurs et applications autorisées, mais en même temps, totalement inaccessibles à toutes les autres. Même une segmentation de type « best-effort » laisse des failles dans les défenses du réseau (des méthodes d'accès non anticipés par les architectes réseau), des failles que les assaillants tenteront d'exploiter.

En outre, les organisations restent vulnérables aux attaques si les autorisations d'accès sont définies sur la base d'une confiance par défaut dans les appareils contrôlés. De nombreuses entreprises ont été surprises par des attaques émanant de collaborateurs et de sous-traitants qui étaient considérés comme étant de confiance. Un dispositif égaré ou dérobé peut révéler des mots de passe qui favoriseront de futures attaques sur le réseau. D'où la criticité d'une approche zero-trust. Les cybercriminels s'efforcent de pirater un vaste panel de dispositifs réseau et les responsables de la sécurité ont d'autant plus besoin d'identifier chaque dispositif qui se connecte au réseau.

Protéger les ressources présentes sur et hors du réseau

Les responsables de la sécurité sont aussi confrontés à une utilisation croissante des dispositifs mobiles hors du réseau corporate ou sur d'autres réseaux. Ceci présente des menaces de sécurité (logiciels malveillants, botnets, etc.) lorsque ces appareils se reconnectent au réseau d'entreprise. Par exemple, de nombreux collaborateurs utilisent leurs appareils BYOD à la fois pour leurs besoins personnels et professionnels. Ils naviguent sur Internet, interagissent avec des tiers sur les médias sociaux et reçoivent des e-mails personnels. Mais lorsqu'ils rejoignent le réseau par la suite, les collaborateurs peuvent fortuitement exposer leurs appareils, et les ressources de l'entreprise, à des virus, logiciels malveillants et autres exploits.

63 % des entreprises ne sont pas en mesure de surveiller les terminaux lorsqu'ils se déconnectent du réseau d'entreprise, et 53 % révèlent que le nombre de terminaux infectés par des logiciels malveillants a progressé sur les 12 derniers mois.[6]

Cette utilisation à la fois personnelle et professionnelle des dispositifs est une réalité. Et pourtant, la plupart des entreprises sont incapables de tracer le nombre de terminaux qui se connectent et se déconnectent du réseau corporate. Dans un récent rapport du Ponemon Institute, 63 % des entreprises déclarent ne pas pouvoir surveiller les terminaux hors du réseau, et plus de la moitié d'entre elles ne peuvent pas déterminer le niveau de conformité des terminaux.[5] Le volume important de dispositifs connectés au réseau ne permet pas de disposer d'une visibilité sur l'ensemble d'entre eux. Il en résulte que les RSSI et les équipes de sécurité ont du mal à gérer les nombreux risques qui en découlent.

Avec un framework zero-trust qui identifie, segmente et surveille en permanence tous les dispositifs, les entreprises disposent d'une alternative à des réseaux plats à risque, pour garantir la sécurité des ressources internes, des données, des applications et des éléments de propriété intellectuelle. Cette stratégie permet de maîtriser les risques résultant d'une stratégie de sécurité centrée sur le périmètre réseau. Et elle dope la visibilité et le contrôle sur les dispositifs hors réseau, tout en simplifiant la gestion globale du réseau et de la sécurité.

Conclusion : un accès réseau zero-trust devient un impératif

L'innovation digitale permet d'atteindre plus rapidement les objectifs métier. Elle met néanmoins à rude épreuve les RSSI, leurs équipes et leurs ressources, compte tenu d'une surface d'attaque qui s'étend et de l'émergence de nouveaux vecteurs d'attaque. Les exactions des cybercriminels deviennent plus sophistiquées et l'approche traditionnelle qui consiste à sécuriser le périmètre réseau n'est plus suffisante. Selon la nature et la sophistication de la menace, il n'est pas possible de voir tous les aspects d'une menace. Mais avec un accès zero-trust, les RSSI peuvent se concentrer sur les utilisateurs et les appareils qui se connectent au réseau, en confirmant leur identité et en s'assurant qu'ils disposent du niveau d'accès et de confiance adéquat.

La prolifération de l'IoT et des appareils intelligents sur le réseau explique, en grande partie, l'expansion de la surface d'attaque. Les professionnels de la sécurité n'ont souvent pas une visibilité totale sur le flot d'appareils qui accèdent au réseau, et les RSSI ont bien compris que ce qu'ils ne peuvent pas voir pourrait bien leur nuire. Pour sécuriser tous ces terminaux, les entreprises ont besoin d'un accès zero-trust actif sur l'ensemble du réseau d'entreprise, pour savoir la localisation de chaque terminal, son activité, comment il se connecte à d'autres terminaux sur le réseau. Cette surveillance continue permet de détecter toute anomalie de comportement susceptible d'indiquer une menace.

Alors que les responsables de la sécurité doivent gérer des collaborateurs opérant à partir de différents endroits et utilisant des appareils personnels et professionnels pour accéder au réseau, ils ont besoin d'un moyen de protéger tous les terminaux sur la périphérie du réseau. Avec une approche d'accès zero-trust, les entreprises disposent d'une visibilité sur tous les dispositifs sur et hors du réseau, ce qui favorise une protection avancée, un contrôle d'accès dynamique et la réduction de la surface d'attaque.

[1] « Mobile Security Index 2019 », Verizon, 2019.

[2] Idem.

[3] Neil Jenkins and Natasha Cohen, « Living on the Edge », Cyber Threat Alliance, 30 avril 2019.

[4] « Only 47% of cybersecurity pros are prepared to deal with attacks on their IoT devices », Help Net Security, 8 novembre 2019.

[5] « The Cost of Insecure Endpoints, » Ponemon Institute, 2020.

[6] Idem.

FORTINET

www.fortinet.fr

décembre 7, 2020 11:37 AM

696181-A-1-FR