Comment moderniser son infrastructure informatique ?

L'approche Software-Defined-Perimeter permet moderniser son infrastructure informatique pour permettre la mobilité des collaborateurs. Explications.

Des mesures de sécurité « traditionnelles » de moins en moins efficaces

Les concepts de sécurité traditionnels sont fondés sur la confiance. Une fois que l'utilisateur se voit accorder l'accès au réseau d'entreprise via un système d'accès à distance VPN, il peut accéder à l'intégralité des données et des applications, pour peu que l'entreprise ait fait l'impasse sur la segmentation du réseau en raison de la complexité d'une telle opération et des efforts qu'elle exige. Cette confiance illimitée peut cependant se révéler dangereuse pour l'entreprise dans son ensemble et mettre en péril le système de sécurité.

Dans la plupart des entreprises, les utilisateurs externes continuent à passer par un VPN pour accéder au réseau interne et aux applications hébergées dans le cloud. Près de la moitié (49 %) des DSI/RSSI européens que nous avons interrogés dans le cadre d'une enquête sur la transition vers le Cloud indiquent que leur entreprise utilise des VPN pour l'accès à distance à toutes les applications métiers. L'enquête fait toutefois apparaître des inquiétudes concernant la sécurité : dans le contexte de la transformation digitale, 80 % des entreprises interrogées en Europe se déclarent préoccupées par la manière dont les employés accèdent aux applications internes. Ces inquiétudes portent principalement sur l'utilisation de réseaux non sécurisés (34 %), devant le recours à des appareils mobiles non gérés et non protégés par l'entreprise (21 %).

Le point faible de l'accès à distance classique par VPN

C'est là que réside le point faible.

La connexion au réseau est d'abord établie, avant d'être ensuite restreinte par des règles de pare-feu. Outre sa complexité, ce processus est source d'erreurs et difficile à modifier, ce qui accroît les risques pour la sécurité. Si le périphérique d'un employé venait à être compromis, des personnes non autorisées pourraient accéder à des informations sensibles ou introduire un malware dans le réseau afin de s'emparer des données.

Tant que les utilisateurs externes ont directement accès à l'intégralité du réseau interne, il existe un risque accru de violation des données ou d'infection par malware. De plus, l'installation et la gestion de l'infrastructure VPN sont des opérations onéreuses et chronophages. Une raison qui, ajoutée à une mauvaise expérience utilisateur, justifie la recherche de solutions alternatives, selon les responsables informatiques interrogés. Pour 58 % des décideurs informatiques européens, la complexité constitue un problème, suivie par une mauvaise expérience utilisateur (47 %). La latence (43 %) et les coûts (40 %) font également partie des motifs d'abandon des VPN.

Compte tenu de la dynamique de travail actuelle, les infrastructures informatiques et concepts de sécurité traditionnels s'avèrent insuffisants. Ils n'ont pas su s'adapter à l'évolution constante du marché du travail « numérique ». Or, ce que les employés veulent, c'est bénéficier au travail d'une convivialité équivalente à celle dont ils disposent dans le domaine privé lorsqu'ils accèdent à leurs

applications personnelles de réseaux sociaux ou de type Cloud. En matière de transformation digitale, les entreprises commencent à réaliser qu'elles ont besoin d'infrastructures à la fois flexibles, économiques, efficaces, simples à administrer et à exploiter, et, surtout, sécurisées. Les départements informatiques doivent optimiser les performances, tout en offrant aux employés une expérience utilisateur positive et personnalisée.

Un périmètre défini par logiciel (SDP) pour plus de contrôle

A la mode depuis quelques années, le terme « Zero Trust » est un concept générique désignant un nouveau modèle de sécurité. Son objectif : résoudre le problème d'une confiance illimitée dans les accès à distance. Cette nouvelle approche pose la simplicité en tant que postulat de base d'une connexion sécurisée des utilisateurs à leurs applications, où qu'ils se trouvent et quel que soit le réseau utilisé. Le terme peut sembler trompeur au premier abord dans la mesure où la confiance est essentielle pour connecter le bon utilisateur à l'application souhaitée. L'objectif fondamental de la l'approche SDP est précisément la mise en oeuvre du concept de « Zero Trust ». Avec son modèle CARTA (Continuous Adaptive Risk and Trust Assessment), le Gartner propose une approche basée sur un accès adaptatif qui contribue au processus. L'idée ici est de tenir compte du contexte, puis de procéder à une évaluation constante du risque, au lieu de faire d'emblée confiance à l'utilisateur ou au périphérique.

Le SDP repose sur un principe simple : l'utilisateur ne peut accéder à une application sans une autorisation d'accès préalable. Cette approche bouleverse le concept traditionnel d'accès, qui veut que l'autorisation soit accordée après l'établissement de la connexion au réseau. Le Cloud et la mobilité jouent un grand rôle dans le travail quotidien des employés. Aussi est-il de plus en plus important pour les entreprises d'assurer à ces derniers un accès sécurisé aux applications, qu'elles soient hébergées dans le datacenter ou dans le Cloud. Pour plus de convivialité, l'utilisateur ne saura même pas où résident les applications lorsqu'il y accédera à distance.

Avec un modèle Software-Defined, l'utilisateur est déconnecté du réseau. La seule chose qui compte, c'est d'établir une autorisation d'accès au niveau de l'application. Une telle approche simplifie l'accès puisque les utilisateurs n'ont plus besoin d'interagir manuellement, ni de se soucier du chemin à emprunter pour accéder aux applications. L'avantage du SDP est la possibilité d'établir des liaisons « un-à-plusieurs » vers des sites, à la différence du VPN traditionnel et de sa connexion « un-à-un » qui permet uniquement d'accéder au réseau. L'utilisateur peut ainsi se connecter simultanément à différents environnements de travail sur le réseau interne ou dans le Cloud. De plus, nul besoin pour lui de savoir à quel environnement accéder, ce qui lui facilite la tâche. Il accède directement à son application sans avoir à se connecter à un réseau. Tout le réseau reste invisible et est protégé des malwares éventuellement présents sur le périphérique de l'utilisateur.

Ce type de modèle donne accès à une application et non à l'ensemble du réseau. Les applications sont uniquement visibles aux utilisateurs autorisés et ne sont pas exposées à Internet. Il n'est plus nécessaire de procéder à une segmentation réseau complexe étant donné que la micro segmentation s'effectue au niveau de l'application, ce qui arrête automatiquement la propagation latérale d'une attaque de malware sur le réseau. Internet devient ainsi un nouveau réseau sécurisé accessible via un tunnel TLS de bout en bout et chiffré.

Le nombre d'employés mobiles ou à horaires flexibles ne cesse d'augmenter. Les entreprises subiront par conséquent toujours plus de pression pour fournir une connectivité transparente et sécurisée permettant d'accéder aux applications sans mettre en danger le réseau. Au vu du nombre croissant d'entreprises en phase de transition, une structure privilégiant le Cloud constitue la base d'un accès efficace et sécurisé aux applications. Un périmètre défini par logiciel remplace non seulement les systèmes VPN, mais aide aussi les entreprises à mettre en place une stratégie multi-Cloud. Au final, l'employé à horaires flexibles pourra se connecter à n'importe quel réseau, en

tout lieu. Et il aura uniquement accès aux applications dont il a besoin pour ses activités professionnelles.