Face à la diversification des menaces, garantir productivité et sécurité en télétravail en 2021

En 2020, de nombreuses organisations ont dû procéder à de prompts ajustements de leur infrastructure IT afin de faire face à l'augmentation soudaine du nombre de télétravailleurs, alors que la COVID-19 se propageait dans le monde entier. La ruée vers la mise à niveau des concentrateurs VPN et l'augmentation des licences de communication unifiée étant désormais terminée, il est temps de se pencher sur les perspectives du travail à domicile en 2021.

Ces changements posent plusieurs questions essentielles allant des implications à long terme du travail à distance du point de vue de la sécurité IT, aux solutions que les services informatiques des entreprises peuvent apporter pour accroître la productivité et renforcer la sécurité des employés.

Les risques de sécurité inhérents au télétravail

De nombreux employés qui travaillaient auparavant dans un bureau n'ont pas vu de changements drastiques dans la façon dont ils interagissent avec les applications et les services qu'ils utilisent quotidiennement, ces dernières étant à présent en SaaS. Cependant, ils le font désormais directement, sans passer par les couches de sécurité mises en place sur les réseaux d'entreprise de leur société.

Pour ne rien arranger, il se peut que leurs terminaux ne soient pas entièrement dédiés à un usage professionnel, et qu'ils soient utilisés pour la messagerie électronique personnelle, les réseaux sociaux, etc. De plus, ils sont connectés au même réseau WiFi domestique qu'une multitude d'objets connectés qui disposent sans doute encore de mots de passe par défaut, et qu'ils le partagent avec d'autres membres de leur foyer qui appliquent très certainement des normes de cyber-hygiène plus souples que celles exigées par leur entreprise.

Dans la plupart des cas, la croissance du télétravail n'expose pas les entreprises à une série de nouveaux risques de sécurité sophistiqués et jusqu'alors inconnus - elle les expose à un grand nombre de risques connus dans un environnement en grande partie non protégé, et sur lequel elles n'ont pratiquement aucune visibilité, ni aucun contrôle.

La sécurité au prix de la visibilité

Afin de gérer les risques inhérents au travail distant, les équipes IT se tournent vers des technologies telles que les CASB (Cloud Access Security Broker) et les SASE (Secure Access Service Edge) pour étendre les contrôles et l'application des politiques de sécurité à l'ensemble de leur réseau d'utilisateurs décentralisés - et cette tendance va se poursuivre, pour probablement s'accélérer tout au long de l'année 2021. Toutefois, le choix et la mise en oeuvre de ces technologies se révèlent complexe et il subsiste des risques en termes de performances et de sécurité, qu'il est difficile de gérer sans un niveau de visibilité adéquat.

Auparavant, les équipes IT des entreprises pouvaient, métaphoriquement parlant, « voir » le trafic des utilisateurs, ce qui leur permettait d'assumer la responsabilité des performances et de la sécurité. Si c'est toujours le cas, le travail à domicile a la plupart du temps fait disparaître la visibilité qui sous-tend ces capacités. Une partie de cette visibilité peut être assurée par divers fournisseurs

de SaaS, de cloud et de CASB dans le cadre de leur offre de services, mais cette solution est très restrictive. Par exemple, si les utilisateurs signalent des problèmes concernant les performances d'un service spécifique ou constatent des comportements inhabituels qu'ils jugent suspects, dans quelle mesure l'équipe IT peut-elle se fier « uniquement » aux données de ces mêmes services pour enquêter sur un problème quelconque ? Il sera difficile, sur la base de ces seules données, de mener une discussion éclairée avec les fournisseurs de services sur les problèmes qui peuvent survenir dans leur environnement.

Pour y remédier, il devient de plus en plus nécessaire que les équipes chargées des opérations réseau et de sécurité disposent d'une visibilité de bout en bout sur l'expérience des télétravailleurs, afin qu'ils puissent mener une discussion approfondie, détaillée et factuelle avec leurs fournisseurs SD-WAN, SASE et SaaS, en cas de problème. Ce besoin ne cessera de croître en 2021, car pour de nombreuses entreprises, le télétravail est appelé à perdurer.

DDoS : version domestique

Un autre risque de sécurité négligé dans le passé, mais qui a pris de l'importance en 2020, est l'impact accru des attaques DDoS contre les concentrateurs VPN et les télétravailleurs eux-mêmes - ou plus spécifiquement les équipements des locaux des clients et les routeurs à domicile. Les cybercriminels, qui cherchent à perturber la continuité des activités, semblent privilégier les attaques contre des concentrateurs VPN d'entreprise alors que la majorité des employés travaillent depuis leur domicile, car de nombreuses applications financières, RH, techniques, etc. ne sont accessibles que via le VPN d'une organisation.

Le lancement d'attaques DDoS visant directement les télétravailleurs pourrait également se généraliser en 2021. Les attaques DDoS qui ciblent les abonnés au haut débit ne sont pas un phénomène nouveau ; la plupart des réseaux font l'objet d'une activité d'attaque de bas niveau quasiment constante. C'est un peu comme dans l'univers du gaming : c'est comme si dans la dernière manche du jeu, à un cheveu de la victoire, quelqu'un vous proposait de mettre votre concurrent hors-jeu pour cinq euros. Si vous trouvez l'idée tentante, vous n'êtes pas le seul !

Des réflexions similaires pourraient émerger parmi les cybercriminels qui s'en prennent aux grandes entreprises. L'idée que pour lancer une attaque DDoS, l'attaquant a besoin de trouver une adresse IP précise, ne serait valide que s'il se souciait des dommages collatéraux. Or, ce n'est pas le cas. Malheureusement, les attaques contre une population plus large d'abonnés, ciblant des centaines, voire des milliers d'entre eux simultanément, sont assez faciles à mettre en oeuvre et sont plutôt courantes. Ces attaques DDoS sont communément dénommées « carpet bombing », car elles consistent à inonder des centaines ou des milliers d'adresses IP au moyen de flux de trafic. Grâce à cette technique, il n'est pas nécessaire de connaître l'adresse IP exacte à attaquer, il suffit de savoir quel fournisseur d'accès Internet la victime utilise - et de l'attaquer dans son intégralité.

Sur un plan plus général, à l'heure actuelle, les cybercriminels n'ont pas encore pleinement exploité la surface d'attaque croissante associée au télétravail. Les quelques exemples susmentionnés sont non-exhaustifs, mais d'autres devraient être exploités à des fins d'attaque et utilisés à grande échelle. En 2021, il ne sera pas facile pour les équipes informatiques de garantir la productivité et la sécurité des entreprises. La période qui s'annonce sera intéressante.