Security by design : le rôle de la 5G quant à la définition d'une stratégie de cybersécurité à long terme

En termes de potentiel révolutionnaire de la 5G, nous avons passé depuis longtemps la phase de la conjecture, de la spéculation et de la prédiction. Bel et bien installée, la 5G offre aux entreprises du monde entier une foule d'opportunités, et nous observons déjà sa puissance en action grâce aux nombreuses villes et sociétés prenant part à son inexorable croissance.

Comme pour toute innovation ou évolution technologique, des questions inévitables viendront cependant à se poser quant à sa capacité de protection contre le cybercrime.

Nous aborderons ici le rôle que jouera la 5G en matière d'élaboration de nouvelles stratégies de sécurité, les mesures pouvant être prises par les RSSI pour assurer la sécurité à long terme de leur entreprise, ainsi que la signification du nouveau modèle hybride télétravail-bureau en termes de security by desing 5G.

Une stratégie à long terme axée sur la sécurité

En matière de stratégie opérationnelle, la cybersécurité ne s'est jamais révélée prioritaire face aux autres aspects fondamentaux. Imaginons par exemple qu'une entreprise souhaite accéder à un nouveau marché dans un délai donné. Son attitude générale consistera à établir une stratégie lui permettant d'y parvenir le plus rapidement possible en laissant de côté l'optimisation et les enjeux de sécurité à plus tard. Trop souvent, la sécurité est intégrée à la dernière minute et à l'arrivée des problèmes, ce qui ne correspond aucunement à une approche durable à long terme.

Les RSSI doivent garder à l'esprit que l'arrivée de la 5G apporte une immense opportunité, mais également une toute nouvelle surface d'attaque exploitable par les cybercriminels. C'est pourquoi, quelles que soient les nouvelles stratégies, innovations ou mises à jour de produit, la 5G doit occuper une place centrale. La stratégie doit être sécurisée par nature et axée sur la 5G, et non l'inverse.

De surcroît, il n'existe aucun problème qui ne puisse être résolu par des optimisations et des corrections mineures. Il est vrai que nous devons utiliser les bases des normes 4G et appliquer les enseignements tirés de l'exploitation de ces environnements, mais il est essentiel que les sociétés redéfinissent entièrement leur stratégie de sécurité en l'axant sur la 5G.

L'objectif consiste à obtenir des stratégies de sécurité dynamiques et capables d'évoluer en permanence de manière à assurer la durabilité des réseaux eux-mêmes en constante transformation. Voici les trois mesures devant être prises par les RSSI pour assurer la future sécurité des environnements 5G :

1. Des accélérateurs réseau de sécurité visant à renforcer l'efficacité opérationnelle

Afin de faire face à la complexité infiniment croissante des opérations réseau liée au débarquement de la 5G, il est essentiel que les RSSI déploient des équipements spécialisés supplémentaires prenant en charge des fonctions de sécurité de type pare-feux, IDS, DDoS, sondes et « packet brokers ». Cette mesure améliore la latence, mais ouvre également la voie à une meilleure

maintenance du réseau et à une identification plus simple des points de vulnérabilité.

2. IA et apprentissage machine (AM) pour des couches de protection supplémentaires

Toute stratégie de sécurité digne de ce nom emploiera proactivement des technologies d'intelligence artificielle et d'apprentissage machine pour identifier les comportements suspicieux, détecter les motifs et cartographier les activités criminelles en temps réel afin de fournir une couche supplémentaire vitale à la protection de votre réseau.

Pour aller encore plus loin, les RSSI doivent toutefois envisager d'adopter des cadres spécifiques offrant une protection aux modèles d'IA et d'AM employés pour exploiter le réseau. Après tout, même le protecteur doit parfois être sous protection. Ce cadre de sécurité IA/AM doit permettre de contrôler l'exactitude des informations siphonnées dans les algorithmes d'AM, mais également garantir que les modèles d'IA fonctionnent convenablement et transmettent les informations collectées aux personnes adéquates.

3. Confidentialité et intégrité des données au coeur du réseau

En cas de piratage, il s'avère souvent fastidieux et lourd en ressources d'identifier l'attaque et de déterminer si l'intégrité des données a été compromise. C'est pourquoi il est très important que les stratégies de sécurité modernes soient conçues de manière à pouvoir identifier rapidement les modifications apportées aux données. À cet effet, les équipes de sécurité prévoyantes adoptent des technologies apportant des preuves irréfutables en temps réel en cas d'altération du réseau ou des machines. Ces équipes prennent une mesure préventive supplémentaire, à savoir le recours croissant aux fonctions sécurisées cryptographiquement pour générer les empreintes numériques des données à l'aide d'une blockchain qui les stocke et leur évite d'être modifiées.

Le télétravail à base de 5G : une révolution pour l'avenir du travail ?

La migration massive des bureaux vers un environnement de télétravail a généralement été bien accueillie par les employeurs comme les employés. Ainsi, bien qu'il apporte de nombreux avantages en termes de bien-être, de productivité et de flexibilité, il offre également aux cybercriminels une vaste gamme de possibilités d'attaque. En effet, 97 % des entreprises considèrent que les télétravailleurs courent plus de risques que le personnel de bureau.

De nombreux employés utilisent désormais plusieurs périphériques sur différents réseaux, souvent en l'absence de protection de sécurité assurée par l'équipe informatique ou de sécurité sur site. Il n'est donc pas surprenant que près de la moitié (46 %) des entreprises britanniques aient subi un piratage en 2020. Pour compliquer la situation, 54 % des sociétés ayant souffert d'un piratage l'ont attribué au moins partiellement au comportement des utilisateurs, ce qui soulève des questions sur le rôle que jouera la 5G quant à l'évolution de la conception de sécurité afin de l'adapter au nouveau modèle de télétravail hybride.

L'infrastructure haut débit britannique a plutôt bien résisté à la recrudescence de foyers recourant à environnement de télétravail. C'est pourquoi les employés eux-mêmes n'utiliseront probablement pas la 5G dans le cadre de leur environnement de télétravail. Cependant, la 5G excelle dans d'autres domaines, par exemple en permettant aux entreprises de déployer des services Cloud avancés capables de prendre en charge des applications mobiles gourmandes en données aidant les sociétés à assurer leur continuité d'activité, qui affirment effectivement à 75 % recourir de manière croissante aux applications Cloud.

Enfin, bien que les vitesses de téléchargement de pointe de la 5G ne permettent pas de répondre plus rapidement à un e-mail, cette technologie marquera l'apparition d'une nouvelle ère

d'expériences immersives telles que l'apprentissage en RA/RV pour les étudiants, les visites d'usine interactives à 360 degrés destinées aux potentiels investisseurs, ou les schémas de produits en 3D permettant aux commerciaux de disposer de ressources plus attrayantes pour obtenir des marchés.

Cependant, les entreprises désirant sérieusement mettre à disposition un télétravail plus flexible doivent clairement placer la sécurité au coeur de leur infrastructure de base et adopter une vision à long terme. Le retour rapide (voire le retour tout court) de la semaine de cinq jours de bureau est improbable. C'est pourquoi les entreprises ne doivent pas traiter la sécurité du télétravail comme une préoccupation à court terme.

Les employés doivent ainsi être formés aux dangers des cyberattaques, mais également de manière systématique à l'identification proactive des activités suspicieuses, notamment à leurs indices fréquents mais souvent négligés, et à leur signalement aux personnes adéquates en temps opportun.