

Les réseaux 5G ont besoin d'une sécurité intégrée

Mobilité

Posté par : JulieM

Publié le : 4/4/2022 13:00:00

Au Mobile World Congress à Barcelone, Orange a annoncé, après l'avoir déjà fait pour le réseau cuivre, la fin de la 2G en 2025 et de la 3G en 2028 en France, pour laisser place à la 5G. Or, la sécurité est devenue une préoccupation majeure pour les fournisseurs de services de communication (CSP) qui procèdent au déploiement de réseaux 5G.

Pour Daniel Crowe, Vice-Président France & Europe du Sud chez NETSCOUT, la sécurisation de la 5G est un passage obligatoire pour les fournisseurs, s'ils veulent conserver leurs parts de marché et leur compétitivité.

« Les opérateurs prennent de plus en plus conscience que, pour maximiser les capacités offertes par la 5G, la mise en place d'une sécurité approfondie dans l'ensemble de leurs pratiques opérationnelles, ainsi que dans les services qu'ils fournissent, est cruciale.

Il s'agit notamment des déploiements de la 5G autonome (5G standalone ou 5G SA), qui commencent à proliférer. Cette dernière bouleverse considérablement le paysage de la sécurité, car l'architecture centrale mobile est désormais une architecture basée sur les services (SBA).

Bien que cela soit essentiel pour exploiter au maximum le potentiel de la 5G, cette nouvelle infrastructure présente des vulnérabilités et nécessite une approche fondamentalement novatrice de sa sécurisation.

Les futurs services 5G fonctionneront sur des infrastructures de réseau multiplexées et virtualisées avec des communications à faible latence vers les applications et déployées au plus près de l'utilisateur final.

Or, à mesure que les services se rapprochent de ces derniers, une visibilité et un contrôle accrus sont nécessaires pour garantir à la fois la disponibilité et la sécurité des services, en particulier dans les zones du réseau où ils font traditionnellement défaut.

En outre, la 5G permet aux entreprises de transformer leurs processus opérationnels, et dès lors que les services 5G qui leur sont destinés sont déployés sur les réseaux des opérateurs télécoms, les surfaces d'attaque poursuivent leur expansion.

Les organisations auront donc besoin de visibilité et de moyens de détection des menaces pour gérer les risques liés à ces nouveaux réseaux mobiles, et garantir en permanence l'intégrité de leurs opérations et la confidentialité de leurs données.

De plus, les appareils IoT 5G, génèrent également une gigantesque surface d'attaque. Dans le cas des appareils grand public, à l'instar des réseaux filaires, les dispositifs peuvent être compromis.

Pour l'IoT d'entreprise ou industriel, les conséquences d'une compromission peuvent aller de la réduction de la durée de vie de l'appareil à la perte d'intégrité des services, en passant par la violation des données ou le lancement d'attaques DDoS.

En effet, la fonction d'exposition de réseau (NEF) donne aux applications tierces un accès direct aux fonctions centrales de la 5G, ce qui étend considérablement ses capacités, mais augmente également la probabilité qu'elle soit la cible d'attaquants.

Toutes ces nouvelles technologies, ainsi que les nouveaux fournisseurs et services, représentent autant de problèmes potentiels en matière de performances, de disponibilité et de sécurité ; liés à une attaque malveillante ou à une défaillance involontaire dans la mise en œuvre.

De ce fait, en intégrant des capacités de sécurité au réseau mobile, les CSP bénéficieront de plusieurs avantages. Cela comprend par exemple la possibilité d'identifier et d'atténuer les cyber-risques plus rapidement, la mise en corrélation des menaces sur plusieurs sites de surveillance, une visibilité complète du comportement des terminaux et la garantie que les capacités de sécurité évoluent avec le réseau en fonction des besoins.

À»