Les rÃ©seaux 5G ont besoin dâ□□une sÃ©curitÃ© intÃ©grÃ©e
Internet
PostÃ© par : JulieM
PubliÃ©e le : 1/4/2022 15:00:00

Au Mobile World Congress Ã Barcelone, Orange a annoncÃ©, aprÃ¨s lâ□□avoir dÃ©jÃ fait pour le rÃ©seau cuivrÃ©, la fin de la 2G en 2025 et de la 3G en 2028 en France, pour laisser place Ã la 5G. Or, la sÃ©curitÃ© est devenue une prÃ©occupation majeure pour les fournisseurs de services de communication (CSP) qui procÃ¨dent au dÃ©ploiement de rÃ©seaux 5G.

Pour Daniel Crowe, Vice-PrÃ©sident France & Europe du Sud chez NETSCOUT, la sÃ©curisation de la 5G est un passage obligatoire pour les fournisseurs, sâ□□ils veulent conserver leurs parts de marchÃ© et leur compÃ©titivitÃ©.

Â« Les opÃ©rateurs prennent de plus en plus conscience que, pour monÃ©tiser les capacitÃ©s offertes par la 5G, la mise en place dâ□□une sÃ©curitÃ© approfondie dans lâ□□ensemble de leurs pratiques opÃ©rationnelles, ainsi que dans les services quâ□□ils fournissent, est cruciale. Il sâ□□agit notamment des dÃ©ploiements de la 5G autonome (5G standalone ou 5G SA), qui commencent Ã prolifÃ©rer.

Cette derniÃ¨re bouleverse considÃ©rablement le paysage de la sÃ©curitÃ©, car lâ□□architecture centrale mobile est dÃ©sormais une architecture basÃ©e sur les services (SBA). Bien que cela soit essentiel pour exploiter au maximum le potentiel de la 5G, cette nouvelle infrastructure prÃ©sente des vulnÃ©rabilitÃ©s et nÃ©cessite une approche fondamentalement novatrice de sa sÃ©curisation.

Les futurs services 5G fonctionneront sur des infrastructures de rÃ©seau multiplexÃ©es et virtualisÃ©es avec des communications Ã faible latence vers les applications et dÃ©ployÃ©es au plus prÃ¨s de lâ□□utilisateur final.

Or, Ã mesure que les services se rapprochent de ces derniers, une visibilitÃ© et un contrÃ´le accrus sont nÃ©cessaires pour garantir Ã la fois la disponibilitÃ© et la sÃ©curitÃ© des services, en particulier dans les zones du rÃ©seau oÃ¹ ils font traditionnellement dÃ©faut.

En outre, la 5G permet aux entreprises de transformer leurs processus opÃ©rationnels, et dÃ¨s lors que les services 5G qui leur sont destinÃ©s sont dÃ©ployÃ©s sur les rÃ©seaux des opÃ©rateurs tÃ©lÃ©coms, les surfaces dâ□□attaque poursuivent leur expansion.

Les organisations auront donc besoin de visibilitÃ© et de moyens de dÃ©tection des menaces pour gÃ©rer les risques liÃ©s Ã ces nouveaux rÃ©seaux mobiles, et garantir en permanence lâ□□intÃ©gritÃ© de leurs opÃ©rations et la confidentialitÃ© de leurs donnÃ©es.

De plus, les appareils IoT 5G, gÃ©nÃ¨rent Ã©galement une gigantesque surface dâ□□attaque. Dans le cas des appareils grand public, Ã lâ□□instar des rÃ©seaux filaires, les dispositifs peuvent Ãªtre compromis.

Pour lâ□□IoT dâ□□entreprise ou industriel, les consÃ©quences dâ□□une compromission peuvent aller de la rÃ©duction de la durÃ©e de vie de lâ□□appareil Ã la perte dâ□□intÃ©gritÃ© des services, en passant par la violation des donnÃ©es ou le lancement dâ□□attaques DDoS.

En effet, la fonction dâ□□exposition de rÃ©seau (NEF) donne aux applications tierces un accÃ¨s

direct aux fonctions centrales de la 5G, ce qui Ã©tend considÃ©rablement ses capacitÃ©s, mais augmente Ã©galement la probabilitÃ© quâ□□elle soit la cible dâ□□attaquants.

Toutes ces nouvelles technologies, ainsi que les nouveaux fournisseurs et services, reprÃ©sentent autant de problÃ¨mes potentiels en matiÃ¨re de performances, de disponibilitÃ© et de sÃ©curitÃ© ; liÃ©s Ã une attaque malveillante ou Ã une dÃ©faillance involontaire dans la mise en Å□uvre.

De ce fait, en intÃ©grant des capacitÃ©s de sÃ©curitÃ© au rÃ©seau mobile, les CSP bÃ©nÃ©ficient de plusieurs avantages. Cela comprend par exemple la possibilitÃ© dâ□□identifier et dâ□□attÃ©nuer les cyber-risques plus rapidement, la mise en corrÃ©lation des menaces sur plusieurs sites de surveillance, une visibilitÃ© complÃ¨te du comportement des terminaux et la garantie que les capacitÃ©s de sÃ©curitÃ© Ã©voluent avec le rÃ©seau en fonction des besoins. Â»