BIZCOMMUNITY

Telcos are preparing to secure the new wave of 5G connectivity, survey finds

According to a global survey of service provider employees by Heavy Reading, telcos will implement a wide array of measures in 2021 to secure the next wave of 5G connectivity.

Photo by Steve Halama on Unsplash

As operators begin to rollout standalone 5G networks, they are moving swiftly to secure core network configuration services, such as slice management, which enable 5G operators to provide highly customised connectivity.

By the end of 2021, 71% of respondents expect to have implemented security measures for their core network configuration services and 75% plan to have secured the radio access network (RAN).

Most telcos are also taking steps to secure other key aspects of their 5G networks, with approximately two-thirds of respondents planning to implement security measures for roaming network signalling, network slicing, application programming interfaces (APIs), the Internet of Things (IoT) and edge computing (MEC) by the end of 2021. Not far behind are container security to support microservices - 61% of respondents - and enterprise mobility (58%).

Bart Salaets, senior director of solutions engineering at F5, said: “It is heartening to see the speed and urgency with which service providers are moving to secure the many different facets of their 5G networks. These measures will be critical to the credibility and success of 5G, particularly in the enterprise market, where businesses across a wide variety of industry verticals are looking for 5G connectivity and services that are ubiquitous, flexible and highly secure.”

What needs to be done before commercial launch?

One of the key attributes of 5G networks will be their ability to expose various capabilities to third parties using APIs.

Although the availability of APIs opens up new avenues of attack for malicious actors, there are a number of measures telcos can implement to protect their network. One-third of respondents said they will implement network DDoS before commercial launch, while 28% plan to implement identity and access management systems and 22% next-generation firewalls (NG-FWs) before going live.

Within a year of commercial launch, the top three priorities are web application firewalls (44% of respondents), NG-FWs (38%) and application delivery controllers (35%). A significant group (31%) also plan to deploy a dedicated API gateway within this 12-month window.

5G and fibre - why we need both to drive connectivity

Steve Briggs 30 Mar 2021

The research also indicates that it will be important for telcos to fully secure the control plane in their new 5G core networks. In this respect, the top priorities are to implement a network repository function (NRF), which maintains a repository of available network service elements, and a secure edge protection proxy (SEPP), which secures and filters internetwork messaging.

Among the respondents, 27% plan to implement an NRF and a SEPP before commercial launch. The next most popular measure is to implement a network exposure function (NEF) to secure the interactions between network functions and application functions – 22% of respondents said they would implement a NEF before a commercial launch.

Mixing and matching security platforms

Pragmatically, many telcos plan to employ multiple platforms to implement their 5G security measures. One of the most popular approaches among the survey respondents is to use a mixture of vendor appliances, virtual network functions (VNFs) and cloud-native network functions (CNFs). Some 28% selected this option as their preferred approach.

The same number of respondents said they prefer to employ VNFs, while CNFs - the most futuristic option - are the preferred approach for 19%. Some 12% chose vendor appliances and 8% SmartNIC-based VNFs/CNFs.

Talking 5G with Avishai Sharlin, president of Amdocs Technology

Imran Salie 26 Feb 2021

However, all five approaches attracted strong support as “viable secondary options” reflecting a sense of realism among operators: they need to quickly employ the most cost-effective measures to protect each element of their network, rather than taking a one-size-fits-all approach.

The survey also found that the concept of a secure access service edge (SASE) is gaining traction among 5G operators. Some 43% of respondents now view SASE as an integral part of their 5G security strategy. The other half are still either formulating a SASE strategy (25% of respondents) or view SASE as independent of their 5G security strategy (24%).

This enthusiasm reflects the position of SASE as the first cloud-native software implementation to combine a number of existing capabilities, such as WAN support, with security capabilities, such as firewall-as-a-service and content inspection.