PL
3Keys of Network Assurance
2022
ENTERPRISE SECURITY STRATEGY
5G SECURITY RISKS
SECURITY BREACH LESSONS LEARNED
The FUTURE of COMMUNICATIONS
CSPs & Cybersecurity
Protecting CELLULAR INFRASTRUCTURE
CYBERSECURITY a New Model
MISSION-CRITICAL SECURITY
TECHNOLOGY CAN'T SAVE YOU
SECURITY w/o PASSWORDS
SECURITY & ASSURANCE

www.pipelinepub.com
Volume 18, Issue 1

Safeguarding Against 5G Security Risks

By: Juniman Kasman

5G has long been touted as being inherently more secure than its cellular predecessors—and it is. But that doesn't mean it’s impregnable. The fact that 5G networks are much more software-based than previous cellular networks creates strengths and weaknesses. On one hand, their software basis makes 5G networks highly customizable and enhances speed, capacity, and responsiveness. On the other hand, the software that enables 5G technology makes it vulnerable in a number of worrisome ways. And this is where the real challenges and threats of 5G security come into play.

Hackers are well aware of and eagerly exploiting these vulnerabilities as 5G networks continue to roll out, and communications service providers (CSPs) are in the crosshairs. The Nexusguard Annual Threat Report 2020 showed that CSPs—especially Internet service providers (ISPs)—were among the prime targets of hackers last year, suffering more attacks than other sectors. Not only have threats increased, but they have also become increasingly complex and sophisticated.

In a world where we’re living, working, learning and more online, 5G security is essential. Here is a look at the risks facing CSPs and the measures they can take to safeguard their networks and their customers.

Hackers target the weak links

Some of the security risks stem from the nature of 5G technology. While 4G and earlier networks rely on a finite number of hardware points of contact to route traffic, 5G networks use countless dynamic software-based routing points that are challenging to monitor and secure. Also, in 5G many of the apps are run in the software or in the cloud. This makes the apps, as well as customer data, easy prey.

The proliferation of endpoints is another major vulnerability of 5G networks. The Internet of Things (IoT) is spawning billions of smart, Internet-connected devices—like car infotainment systems, smartwatches, thermostats, speakers, baby monitors, and even refrigerators, to name just a few. Many more such devices are in development or are hitting the market as the IoT rushes to capitalize on the speed and capacity of 5G. The problem is that many fledgling IoT devices, especially low-end ones, often lack any meaningful security features. They're the proverbial weak link, offering vectors into the network that hackers can easily exploit to launch attacks on CSP customers.

Compounding the problem is the fact that device manufacturers aren't the only ones that neglect security. Many CSPs don't invest enough in security-apps-related services. According to data from the Global System for Mobile Communications Association (GSMA), 48 percent of mobile network operators report that they lack the knowledge and tools to mitigate 5G network vulnerabilities. Lack of knowledge, device vulnerabilities, and increasingly complex attacks are driving a complex 5G security environment.

Know what to watch for

Cybercriminals are using various types of attacks against CSPs, including distributed denial of service (DDoS) attacks. In some cases, DDoS attacks aimed at a CSP's customers can bring down the whole network. Other complex attacks are on the rise, including sophisticated bit-and-piece (carpet bombing) attacks, which drip-feed junk traffic across a large IP pool to paralyze the target, and other UDP-based attacks that can flood target networks with traffic. They can defeat (evade) threshold-based and host-based detection/mitigation countermeasures that are widely applied to a CSP's network. Other threats include small-sized, short attacks known as "invisible killers," and extortion and ransom DDoS (RDDoS) attacks that take advantage of the surge in anonymous crypto payments. One of the most concerning issues is the growing threat of terabit attacks. Given that a 5G device can transmit more than 10Gbps, attackers must target only 100 of these poorly protected smart devices to generate a full terabit attack. Most CSPs don't have the capacity on the backend to withstand this volume of data, which will easily congest the network and eventually bring customers down. Disabling even one part of a CSP's core infrastructure can cripple a network. This hasn't happened yet, but the possibility is very real—and imminent.

This level of disruption can be devastating for CSPs, who are expected to give their customers uninterrupted connections and maximum speed for critical operations, as well as an assurance of privacy and protection against data breaches.

Strengthen your defenses

The first step in building a solid defense is to make cybersecurity a top priority rather than an afterthought, taking a native-integrated approach and investing in it as needed. Attacks are constantly refined and updated, and it's imperative to keep defenses up to date in response. Before ruling out upgrades because of the expense, calculate the cost of downtime and damage to your brand and revenue if you do fall victim.

Think twice about using threshold and signature-based detection methods, which are no longer sufficient. Organizations that rely on them may well experience major outages from newer, more evasive DDoS attacks and the emergence of small-sized attack traffic. A far more effective defense is a hybrid strategy that combines on-premises and cloud-based mitigation technologies, which can be used separately or in tandem. Platforms powered by machines with big data and deep learning capabilities can help with identifying and classifying customer traffic and with developing up-to-date defenses against ever-evolving attacks.

Many CSPs don't have the staff, the technical expertise, or the budget to protect against advanced threats on their own. It can easily take millions of dollars to build a network able to provide global DDoS protection when you factor in start-up costs, technology maintenance, and support for both internal and external users.

The best solution for many enterprises is a partnership with an experienced managed security provider that uses artificial intelligence (AI) and machine learning, with an emphasis on multi-dimensional and deep learning-based DDoS detection and mitigation. The right partner can provide the hardware, productization and operational support needed, so the organization doesn't incur the hardware barriers and upfront costs associated with typical anti-DDoS service ramp-up.

The situation is serious, with DDoS attacks up 341.21 percent in March 2020 compared to the year before, according to our research. All indications point to attacks continuing to increase and become more sophisticated, further testing the effectiveness of authentication-based mitigation. In fact, some experts predict application attacks will double in 2021-2022. Our research shows that ransom DDoS attacks will increase by 30 percent; easy access to booter and stresser service means a lower cost for bad actors to carry out ransom DDoS attacks. DDoS attacks of 10Gbps or less will account for 99 percent of all attacks, as they'll continue to be difficult to detect and economical to deploy.

This challenging outlook only reinforces the need for CSPs to bolster their security—and step up efforts to protect their networks, infrastructures and customers, especially as we move fully into a 5G world.