SecurityGen
Telecom Security. Transcending Generations.

SecurityGen identifies the cybersecurity priorities for mobile operators in 2023

Open architecture, non-standalone roaming, nation-state attacks, ransomware, and the need for more industry collaboration are among the major 5G security challenges that operators must address in the year ahead

Mobile technologies have become part of everyday life, making them an increasingly appealing target for intruders. To prevent the consequences of their attacks, operators must employ timely protection measures.

SecurityGen releases cybersecurity priorities that telecom operators should focus on in 2023. Here is what they must prepare for in the year ahead as follows:

1) 5G related challenges

- **5G is open for integration - but also open to attack**

Unlike previous mobile network generations like 3G and LTE, 5G is designed from the ground up to be flexible and open for integration with multiple external systems. However, the same open architecture that enables this flexibility and easy integration can also make 5G vulnerable and exposed to threats and hidden vulnerabilities.

The challenge for operators is to maximise 5G's advanced functionality and interoperability while also recognizing this vulnerability and minimizing the threats arising from 5G's extra openness compared to previous network generations.

- **Beware of roaming traffic from non-standalone 5G**

As operators deploy more 5G networks and more users purchase 5G smartphones, the volume of roaming traffic between 5G networks increases. But the majority of this extra roaming traffic goes through non-standalone 5G networks which still use unsecure legacy technology for their core networks, including signaling protocols such as GTP and Diameter, which have proven to be hackable in recent years.

Without proper security measures in place, 5G is vulnerable to threats originating from non-5G networks carried in non-5G network traffic – but which are able to damage and disrupt 5G services.

2) Cyberattacks from hostile states and organized crime

Telecom networks are critical national infrastructure, which makes them high-value targets for cyberattacks, especially during times of conflict and heightened geopolitical tensions. The growing use of mobile - especially 5G - for connecting and remote monitoring of everything from energy grids and automated factories to smart cities and transport systems, amplifies the damage and disruption that an attack on an operator's network could inflict. Mobile's importance also makes it a target for organized crime groups to launch financially motivated attacks of their own aimed at operators or their subscribers.

3) Operators as high-value targets for ransomware

The number and frequency of cyberattacks such as ransomware and phishing show no signs of slowing down. The threat of ransomware is already well known: however in 2023, expect the bad actors behind them to become more advanced and more selective in their attacks - including targeting mobile networks as the means to breach telecom operators and access the valuable customer data they hold.

4) New industry regulations on security but operators must do more themselves

National and pan-regional regulators are pushing the telecom industry to comply with new security requirements that address the heightened threat of cyberattack on digital infrastructure and telecom networks as part of it.

Mobile network security is still perceived as an after-thought. Rather than adopt a network-wide, security-by-design approach, many operators continue to rely on inefficient one-off security techniques which leave parts of their networks exposed to hackers.

5) Effective cybersecurity also depends on collaboration

- **Lack of knowledge sharing**

When companies and experts share their knowledge and experience, everyone benefits. But, with international cooperation undermined by current geopolitical rivalries and tensions, divisions might open between operators and other telecom industry players, regulators and national governments that make it more difficult to cooperate on collective joint efforts for better cybersecurity.

- **Cyber-security skill shortages**

Cyber-security continues to suffer an ongoing shortage of skilled workers, especially in areas that require specific expertise such as telecoms. Combined with the lack of knowledge sharing, the skills shortage makes it harder to encourage and develop new talent. The telecoms industry, led by operators, needs to step up and invest in training initiatives to attract new workers and provide them with the requisite skills needed to grow the cyber-security talent pool.

Steps to strengthen the security of 5G networks

Make the security of your 5G network as much of a commercial and operational priority as its performance in terms of speed, throughput, and coverage. The current economic conditions should not put operators off investing in proper security measures. Security is more efficient and cost-effective when it is a built-in feature across the entire system, and not just a patch on the surface.

Adopt a defence-in-depth approach based on continual network-wide assessments and monitoring. 5G networks are a step-change in complexity that are more like IT systems than legacy mobile networks. Regular security checks, continuous analysis and other established cybersecurity methods fine-tuned for the telecom environment will provide the level of detail and in-depth scrutiny that's needed to ensure a 5G network is secure.

Effective 5G security requires more than just installed software solutions and automated monitoring and testing. Extensive and ongoing training is also essential, so that operator security teams can explore and stay up to date with the latest cyberthreats - and also identify new vulnerabilities as they emerge.

Conclusion

Due to developments in automation and digitisation, mobile will continue to have a significant impact on how people live, work, and conduct business. Customers will gain from the new business opportunities and technological advancements brought about by 5G, but telco security teams must but telco security teams must be cautious and aware of the new, specific security challenges that come with 5G while also remaining vigilant against the threats inherited by reused technologies within the 5G set up.

Besides, given the crucial infrastructure role that telecommunications play, networks still remain a high-value target for attacks and rank highly among nation-state actors in the modern geopolitical environment.

Thus, telecom security cannot be addressed by a single-point solution. It needs a thorough strategic approach and collaboration with ecosystem players. Because of this, operators and their industry partners should work closely with governments and regulators to make sure cybersecurity receives the attention and funding it needs to protect users and guarantee that networks are safe, secure and resilient.