5G and cybersecurity: A new approach for next-generation networks

Prysmian General Cable Draka

Introduction

5G is the wireless fabric that will connect everything. From the self-driving vehicles on our roads, to surgeons performing remote, real-time surgery, to the smooth day-to-day running of smart factories, smart homes, and smart cities.

However, with increasing importance must come increased security. There are still security issues which need to be considered and addressed before 5G can truly begin to power our lives.

Recently, the European Commission has endorsed a joint toolbox of mitigating measures agreed by EU Member States to address security risks related to the rollout of 5G. The objectives of this toolbox are to identify a possible common set of measures which are able to mitigate the main cybersecurity risks of 5G networks, and to provide guidance for the selection of measures which should be prioritised in mitigation plans at national and at Union level.[1]

Security considerations across 5G networks

Network architecture

5G networks are based on a software-defined network. Its activities are pushed towards routers spread throughout the entire network, making it impossible to identify or deploy chokepoints for security inspection and control.

Virtualisation

With 5G, most activities are developed and performed based on the Internet Protocol (IP) as well as popular operating systems. As a result, it will be easier to attack the software and manipulate it.

IoT proliferation

IoT has grown even without the support of 5G technology. It's already being used effectively in sectors such as military and public defence, transportation, public safety, healthcare, and smart urban centres. Devices on the IoT network allow individuals and organisations alike to run critical processes. But the addition of billions of IoT devices to the 5G network could also expose it to additional risks, and increase the network's vulnerability.

[1] www.ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

Mitigating cyber risk in 5G networks

Cyberattacks on 5G will overwhelmingly take the form of software-based attacks. Likewise, they must be combatted with software protections. Defence solutions powered by Artificial Intelligence (AI) are the most powerful defence against these virtual attacks. Once built into the network, AI-powered software security products will continue to evolve, to increase a network's defence-levels via self-learning, and will continue to adapt to an ever-changing environment.

But we cannot rely on retrospectively added defence products. To develop robust cybersecurity solutions, security should be considered at every stage of the network development lifecycle – not just incorporated into an already finished product. It's essential that security is integrated within the network's hardware, firmware and software development, in order to protect its integrity. In fact, it's likely that regulatory bodies will enforce minimum security requirements for all 5G hardware and software.

Given that the cyber threat to the nation comes through commercial networks, devices, and applications, the 5G cyber focus must begin with those companies involved in the new network, its components, devices and applications.

Conclusion

With potentially vulnerable software operations, and a distributed infrastructure that avoids the centralised chokepoint afforded by earlier networks, 5G networks will be a prime target for attacks.

Increasingly, businesses and consumers alike will expect the companies who provide their network services to demonstrate sufficient cybersecurity defences that can sustain 5G network security.

Whether they're small, local ISPs, or renowned multi-national giants, every network service provider must implement successful and robust cybersecurity programmes.

Source: www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity

Prysmian Group

Prysmian Group
Via Chiese 6, 20126 – Milan, Italy
T +39 02 64491
dh@prysmiangroup.com
prysmiangroup.com