The 5G era is near, but are security procedures ready?

The new 5G mobile network generation is beginning to be gradually deployed in leading countries like the United States and Europe, bringing promises of the future of a seamless and seamless connection standard among all. technology world gadgets, from sensors, software systems, to robots and IoT platforms.

The new 5G mobile network generation is beginning to be gradually deployed in leading countries like the United States and Europe, bringing promises of the future of a seamless and seamless connection standard among all. technology world gadgets, from sensors, software systems, to robots and IoT platforms. With reliability, high stability, large capacity and especially unprecedented low latency. 5G is contributing to forming the foundation of a comprehensive automated control system, operating in an important global environment.

However, in addition to the obvious benefits mentioned above, this new generation connectivity standard also brings many risks of information security and security. These can be more sophisticated, new, difficult to control threats, related to things we already know even in recent times.

For many years, telecommunications networks are basically isolated networks built on proprietary telecommunications protocols. However, today, they are tending to gradually shift to internet-facing mode, all-IP network with standardized protocols. By automation and virtualization, a major change in this technology has contributed to significantly shortening the development and deployment cycle and giving the bad guys a broader perspective, more opportunities in grasping. Catch the holes.

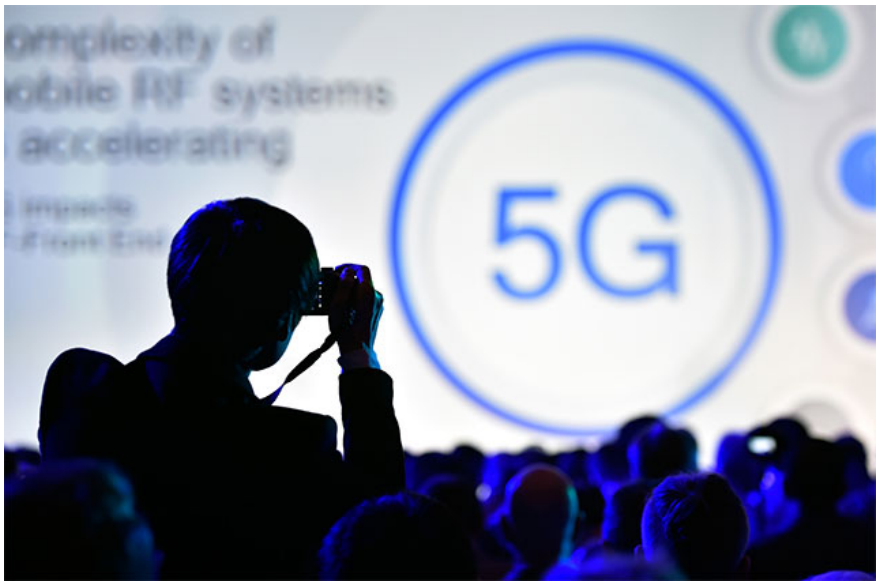
From service providers, regulatory agencies to consumers, this technological change can be seen as a huge challenge for us to access security and risk reduction issues. .

1. The first areas benefit from the development of 5G

Security: Important platform for network systems

Ensuring security for critical networks is a sector-wide task and has long been an explanation of customer confidence in the service.

Despite this, learning efforts in learning and improving security never stop, providing great challenges in maintaining strong product and service security in the context. The technology scene is developing rapidly like today. Owning only control and distribution measures for the process, along with the required technical requirements, is not enough to ensure that everything is maintained stable and safe.



Thus, it can be seen that holding a security development process and establishing strict new technical security requirements is a beginning that can bring about high efficiency. However, this goal will not be achieved if you do not provide measures to monitor, evaluate and observe the level of implementation of the process, and more importantly, commitment, synchronization in maintaining policies and enforcing strict security throughout the system.

The lesson here is that security measures should be designed and focused on starting from the beginning, from the initial development stage to address today's security challenges, and from today. to deal with issues that we may encounter tomorrow.

1. Post-MWC 2019: 5G has a long and tough road ahead

Security design

Acting as a proactive design approach, security standards, tools, and processes must ensure that privacy is implemented before the product is integrated and deployed on an enterprise scale. .

Over time, it can be seen that one of the most important things here is that the telecommunications industry must build a list of security requirements, sorted by priority and severity. , and at the same time this is a mandatory element in each product. This constitutes an active core factor in the security process, which includes external

participation from industry forums, such as 3GPP, and both customers and regulatory agencies. In general, all of these factors should be combined and included as a mandatory security requirement of the company.

The following products also need to be evaluated to establish a 'baseline security boundary', and define a roadmap for security, privacy and interoperability, and then undergo many rigorous tests with both internal and commercial tools. If feasible, companies must use both static and dynamic code analysis, as well as strong cryptography to ensure product integrity throughout the development cycle.

1. Will Qualcomm's 5G CPU be available in the market in 2020?

In fact, even the best software, refined and tested many times, still has the potential to contain exploitable vulnerabilities. Therefore, companies must constantly monitor public and private sources to indicate that their software or third-party software is embedded in products that ensure safety.

Security holes, if any, should be classified according to the scale of the conditions, the actual characteristics of each product, and the R&D groups will also have to implement many different plans to fix this problem. In addition, plans must be applied across all R&D groups, who in turn are responsible for complying with the highest security standards while monitoring this process.

In addition, automation is also an essential element for security development and implementation. Companies should aim to provide developers with automated feedback on potential security issues in their code at the earliest stage of development, as well as find ways to automate the hole scanning process. Network vulnerabilities and various application security tests to ensure they are implemented regularly and consistently. When this process is applied, early-stage and more comprehensive product testing should also be monitored by the R&D and security management teams, allowing quick intervention when needed. In the event that the above process is not followed, security departments should also give veto power over the product, because the cost of security and remediation when problems occur will be extremely high, seriously affecting to the existence of a business.

1. The way that 5G will change Internet connection in your home

Looking at the future of 5G

There is a sad fact that we still have to accept that the current security processes and measures are still being implemented too passively, always following the security trend as well as potential threats. At the present time, we are taking the first steps to the 5G era, the systems must be carefully designed in order to optimize the safety inspection efficiency, provide the right kind of product. reliable and protected that customers expect long ago. Take slow, steady steps!