ORACLE

Securing 5G Networks: What You Need to Know About the EU Toolbox

As a major enabler for future digital services, 5G will play a key role in the development of our digital economy and society in the years to come. As 5G services are geared to support countless connections with the potential for more entry points for attackers, ensuring the cybersecurity and resiliency of 5G networks will be of vital importance.

THE EU 5G TOOLBOX

In January 2020, the European Commission endorsed the joint toolbox of mitigating measures agreed by European Union member states to address security risks related to the rollout of 5G. The objective of the EU toolbox on 5G cybersecurity is to identify a coordinated approach based on a common set of measures, aimed at mitigating the main cybersecurity risks of 5G networks that were identified in the EU coordinated risk assessment report. The report highlights a number of important security challenges which are likely to appear or become more prominent in 5G networks. These security challenges are mainly linked to:

- Increasing security concerns related to the availability and integrity of the networks, in addition to the confidentiality and privacy concerns;
- Key innovations in the 5G technology (which will also bring a number of specific security improvements), in particular the increased important role of software and the wide range of services and applications enabled by 5G networks; and
- The role of suppliers in building and operating 5G networks, the complexity of the interlinkages between suppliers and operators, and the degree of dependency on individual suppliers.

The report further concludes that these challenges create a new security paradigm, making it necessary to reassess the current policy and security framework applicable

Useful Ressources:

- Oracle's Corporate Security Practices
- Oracle's Software Security Assurance
- Corporate Risk Management Resiliency Program
- Oracle's Cloud Security Practices
- Oracle's General Data Protection Regulation (GDRP) Compliance
- EU coordinated risk assessment report
- Cybersecurity of 5G networks EU Toolbox of risk mitigating measures

to the sector and its ecosystem, and making it essential for Member States to take the necessary mitigating measures.

The toolbox aims to create a robust and objective framework of security measures to ensure an adequate level of cybersecurity of 5G networks. The approach taken is a risk-based one and solely on security grounds.

The toolbox recommends a set of key actions, namely:

- Strengthen security requirements for mobile network operators.
- Ensure that each operator has an appropriate multi-vendor strategy, to avoid or limit any major dependency on a single supplier.
- Maintain a diverse and sustainable 5G supply chain in order to avoid long term dependencies.

ORACLE'S SECURITY DNA

Oracle has over 430,000 customers in 175 countries. The company operates globally in a challenging and ever-changing threat environment.

Oracle is committed to delivering secure solutions, as well as assist customers meet their security and compliance requirements using Oracle technology.

To this end, Oracle's security practices are multidimensional in order to reflect the various ways Oracle engages with its customers: e.g., by reflecting the joint security model of cloud offerings, and providing superior security documentation to help customers securely deploy technology in their data centers.

Oracle policies and standards provide global guidance for appropriate controls designed to protect the confidentiality, integrity, and availability of data per data classification.

Required mechanisms are designed to be commensurate with the nature of the data being protected. For example, security requirements are greater for data that is sensitive or valuable, such as cloud systems, source code and employment records.

Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments.

Additionally, Oracle has policies and procedures governing the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with malicious alteration of these products before installation by customers.

Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud.

ORACLE'S POSITION ON THE EU 5G SECURITY TOOLBOX

The measures presented in the EU toolbox are inline with the EU coordinated risk assessement report and concern the relevant security stakeholders in the 5G ecosystem, these being primarily Mobile Network Operators (MNOs) and their suppliers, in particular telecom equipement providers, such as Oracle, responsible for the provision of software and hardware required to operate networks. Here we have outlined some of the more relevant measures to Oracle.

Why Oracle Communications

- 40+ years of heritage in network experience meets cloud innovation to deliver highly secure, robust, and flexible cloud native 4G/5G core network solutions
- Dominance in 4G control plane category inventor for Session Border Controller & Diameter Signaling Router
- Cloud native environment based on Oracle's Cloud leadership and expertise
- Continued innovation in Cloud Native 5G Core control plane network functions
- Private Network Clous Service for reduced OPEX/CAPEX & faster time to market with a autonomous security and rich SaaS ecosystem including IoT Cloud services
- Smart Monetization Solutions

SUSTAINABILITY AND DIVERSITY OF 5G SUPPLY AND VALUE CHAIN

SM08 * - Strategic measure: Maintaining and building diversity and EU capacities in future network technologies

This area mainly addresses the risk of dependency on a single supplier and recommends a mitigation plan that ensures diversity of supply within each operator and geographical balance at national level and promote long-term sustainability of 5G supply chain.

Oracle believes in a fair and equitable competitive market. It is our view that a multi-supplier network provides operators with the most flexibility and highest security. Oracle Communications develops to industry standards, ensuring our ability to interface with other suppliers. Indeed, our network products are already deployed in multi-supplier networks, interoperating with other vendors who are compliant with industry standards.

NETWORK SECURITY, BASELINE MEASURES

TM02* - Technical Measure: Ensuring and evaluating the implementation of security measures in existing 5G standards

There are several risks factors to be considered in this approach, as per the table below:

RISK FACTOR	MITIGATION PLAN
Misconfiguration of network	Increase network security and resilience
Lack of access controls	Increase network security, in particular strengthen rules on access to network by suppliers and on use of Managed Service Providers and third line support
Low equipement quality	Apply pressure or incentives on suppliers to increase product quality and increase network security and resilience
Exploitation of 5G networks by organized crime	Increase network security and raise quality of supplier's processes and equipement
Significant distruption of critical infrastructure or services	Increase network security, ensure resilience and continuity and raise quality of supplier's processes and equipement
IoT exploitation	Increase network security, ensure resilience and continuity and raise quality of supplier's processes and equipement

Oracle takes security very seriously. Our software development processes include stringent audits and reviews by our corporate security team. All products must align with Oracle's Software Security Assurance (OSSA) program which requires secure design, architectural risk analysis with threat modeling, secure coding standards, secure configuration, supply chain security, and comprehensive static and dynamic

security testing. Oracle also provides features that allow the Operator to control the access to their network equipment. Oracle products and the delivery process ensures that customers control all security credentials such as passwords, certificates and encryption keys.

Our software development process ensures that all shipped products have completed stringent auditing and testing and are of the highest quality possible. Oracle does not allow "ad hoc" development in the field as this approach introduces too many vulnerabilities and cannot be properly audited and tested.

REQUIREMENTS RELATED TO SUPPLIERS' PROCESSES AND EQUIPEMENT

TM08* - Technical Measure: Raising the security standards in suppliers' processes through robust procurement conditions

This mitigation plan addresses the risk of low equipement quality and ensures that MNOs demand specific security standards from equipement suppliers in the procurement process. An example would be specific security improvements and demonstrating quality levels, security maintenance of the equipement throughout its lifetime and built-in security during the product' development processes.

Oracle Communications Global Business Unit (CGBU) is TL-9000 certified for quality and ISO-27001 certified for Information Security. Combined, these two 3rd party audited programs ensure quality and security are not only maintained but continuously improved. Certificates are available upon request.

TM11* - Reinforcing resilience and continuity plans

In order to address the risks around significant distruption of critical infrastructure or services, MNOs must reinforce t their resilience and continuity plans. An example would be to have adequate plans in place in case of disaster affecting the ongoing operation of their network, and to ensure any critical dependencies are mapped and mitigated as required. MNOs should request similar arrangements within their suppliers and only use suppliers who demonstrate sufficient levels of long-term resilience.

Oracle has a Corporate Risk Management Resiliency Program (RMRP) that establishes a business-resiliency framework providing response to business interruption that may impact Oracle's operation. The program is implemented and managed locally, regionally and globally. CGBU's program is externally audited as part of the TL-9000 and IS)-27001 certifications.

STANDARDIZATION

SUPPORTING ACTION: SUPPORTING AND SHAPING 5G STANDARDIZATION

All revelant actors including operators and suppliers are encouraged to increase their engagements in relevant standardization bodies, in particular through reinforced coordination at EU level in order to increase ability to shape standardization according to identified needs, by setting up a forum or group of national regulatory authorities and other relevant competent authorities of Member states, reporting to the NIS Cooperation Group and the EECG, in particular tasked to:

- Contribute to achieving an appropriate level of convergence as regards technical measures relying on standardisation and certification, in line with existing legislation, such as but not limited to the Cybersecurity Act;
- Promote standardisation of interfaces to facilitate diversity of suppliers;

*: Reference: Cybersecuruty of 5G networks EU Toolbox of risk mitigating measures

- Ensure liaison between the NIS Cooperation Group and relevant European and/or international standardisation bodies;
- Ensure full participation by EU industry and improve the dialogue between the industry and the MS.

While the EU Toolbox does not show risks for this supporting action, we at Oracle strongly believe that the lack of standardization and open interfaces represents the highest security risk. This is why Oracle participates in over 400 standards organizations today, including the 3GPP, GSMA, and IET.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle