63rd FITCE International Congress
26 - 28 September 2024, Kraków, Poland

The need for Cybersecurity in a Telecom Operator

Konstantina Katsampani – Senior Telecom Engineer

Cosmote S.A Telecom Operator, Greece

Abstract

In today's digital era, telecom operators are the backbone of global communication networks, handling vast amounts of sensitive data and providing critical infrastructure for businesses and individuals alike. So, they are prime targets for cyber-attacks. This presentation delves into the necessity of robust cybersecurity measures within the telecom industry, highlighting the unique threats faced by telecom operators and the potential consequences of cyber-attacks, including financial losses, operational disruptions, and reputational damage. We will explore the various types of cyber threats that specifically target the telecom sector, such as malware, ransomware, DDoS attacks, phishing, insider threats, and network intrusions. The presentation will also cover the regulatory and compliance landscape, emphasizing the importance of adhering to key regulations like GDPR and industry-specific requirements to maintain customer trust and avoid legal repercussions. Moreover, the presentation outlines a comprehensive cybersecurity strategy tailored for telecom operators, featuring essential components like risk assessment, incident response planning, continuous monitoring, employee training, and the adoption of advanced technologies such as AI and machine learning. Emerging trends and future challenges in telecom cybersecurity will be discussed, including the security implications of 5G, the Internet of Things (IoT), and the increasing sophistication of cyber threats. The Attendees will gain a deeper understanding of the critical role cybersecurity plays in the telecom sector and the actionable steps they can take to safeguard their networks and data.

.