ECASEC
European Competent Authorities for Secure Electronic Communications
powered by ENISA

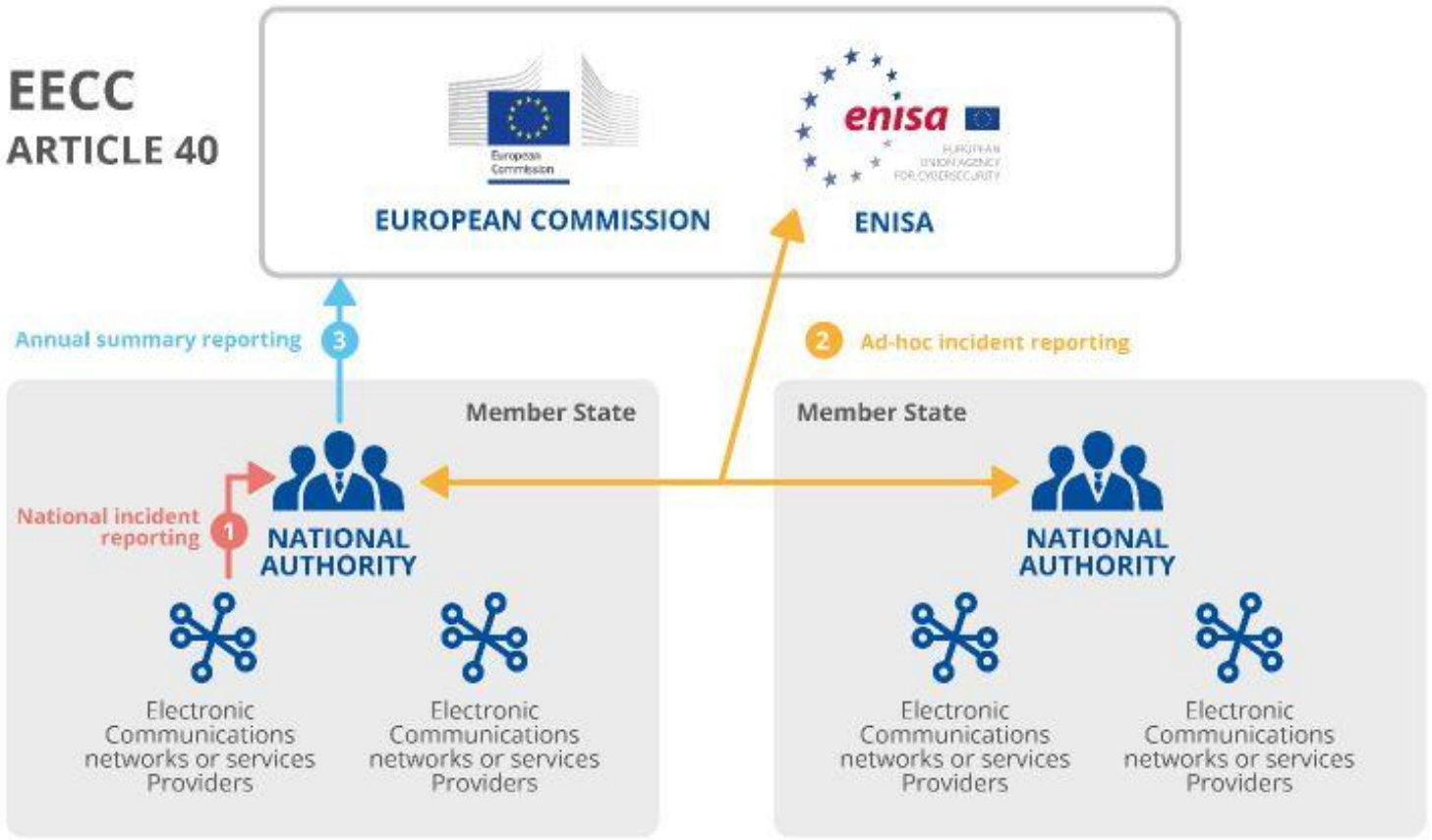
NIS COOPERATION GROUP

THE EU CYBERSECURITY AGENCY

ENISA – OVERVIEW OF ACTIVITIES IN TELECOM

Georgia Bafoutsou, Cybersecurity Expert
Policy Development and Implementation Unit, ENISA

ANNUAL INCIDENT REPORTING



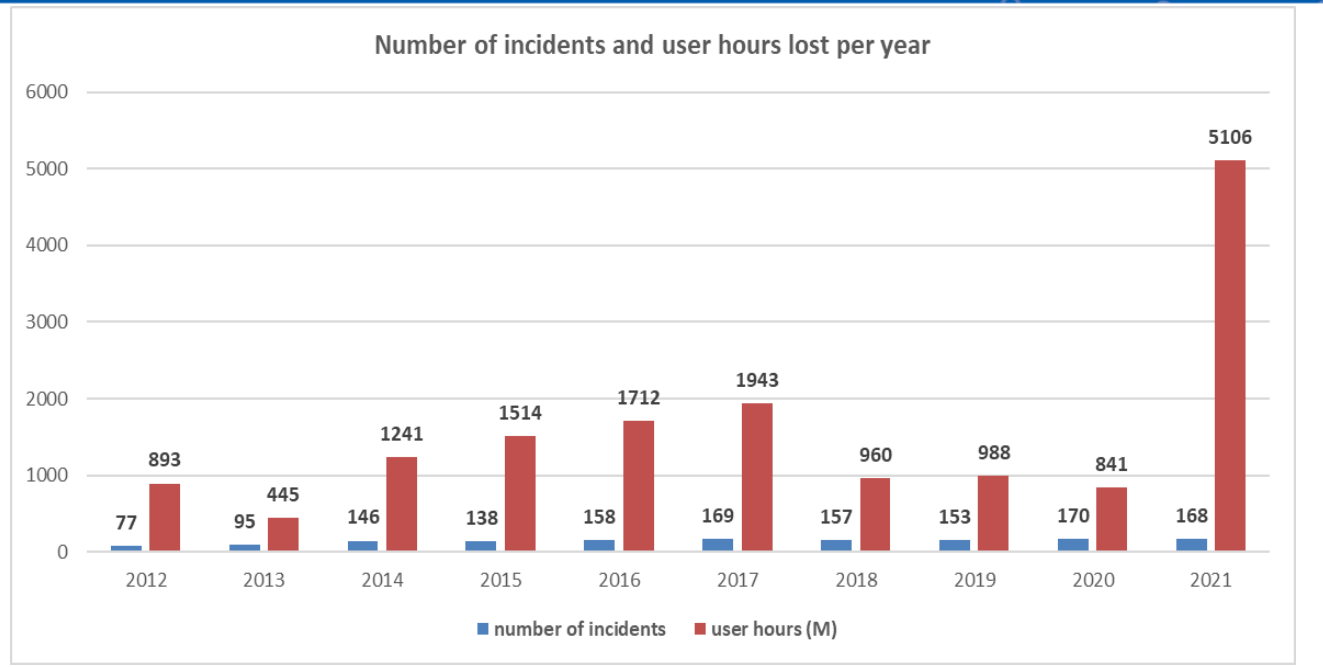
CIRAS

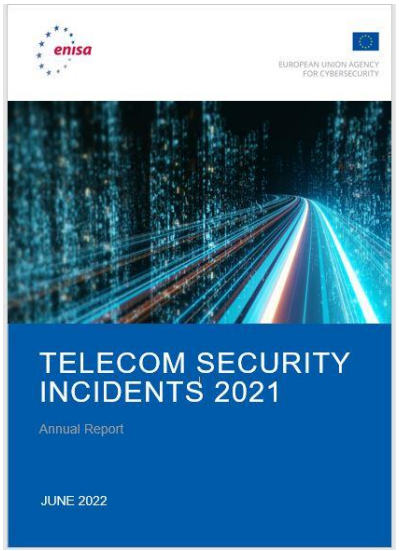
is a free online tool where ENISA stores reported incidents and provides annual and multiannual statistics.

ANNUAL INCIDENT REPORTING

https://ciras.enisa.europa.eu/

ANNUAL INCIDENT REPORT 2021 – SNEAK PREVIEW

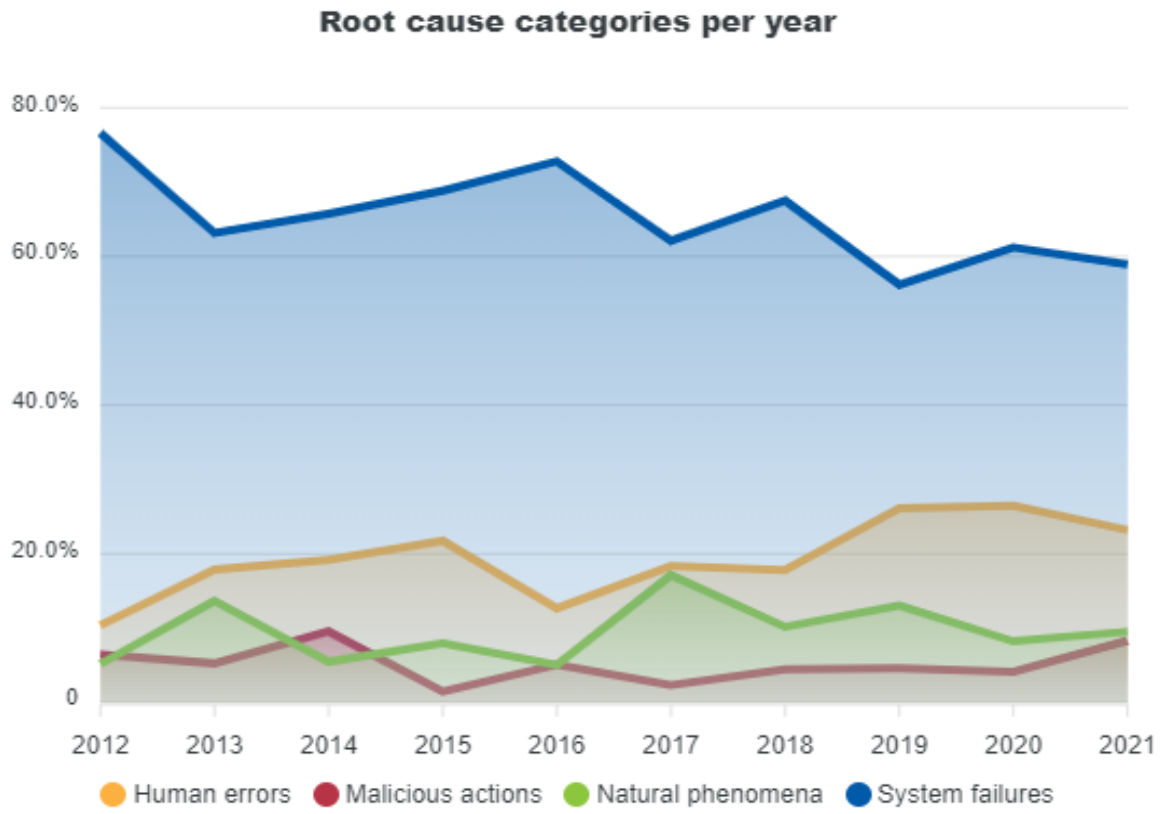




- Reports of 168 incidents submitted by national authorities from 26 EU Member States (MS) and 2 EFTA countries
- The total user hours lost, was 5106 million user hours, a huge increase compared to the 841 million user hours lost in 2021

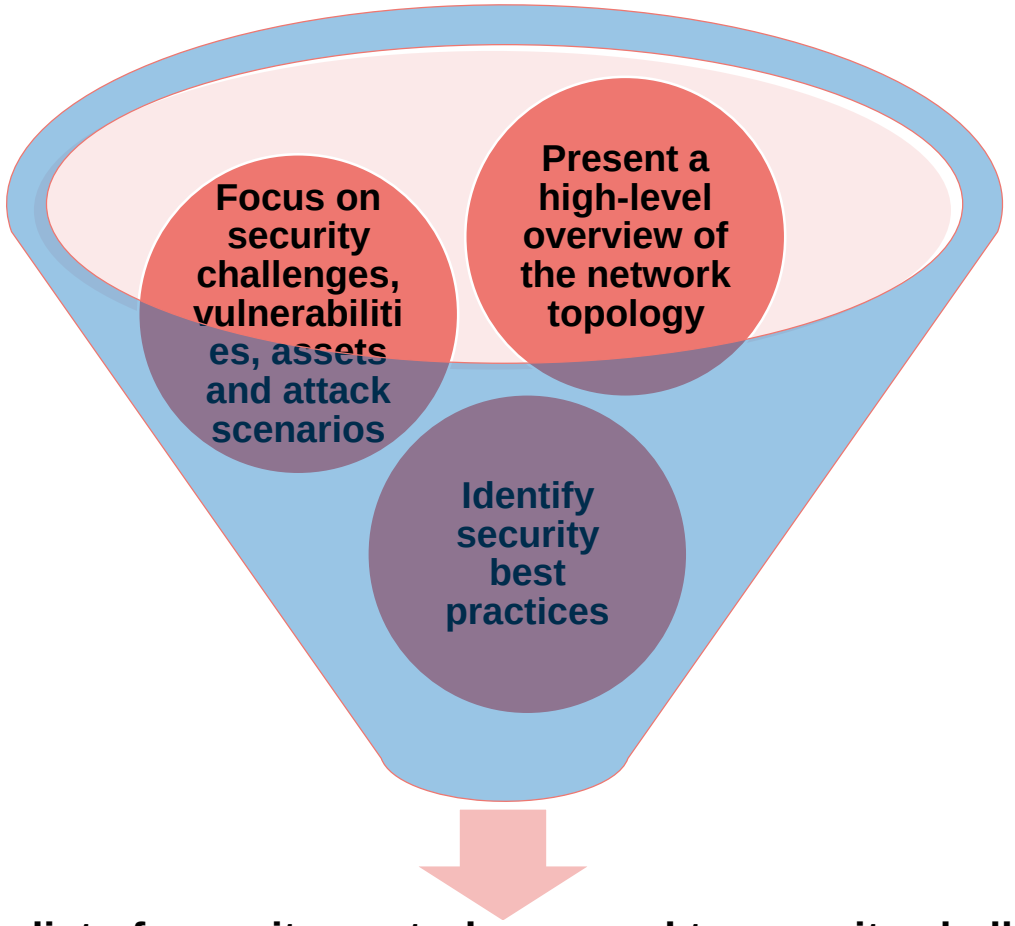
ANNUAL INCIDENT REPORTING

- Reporting of incidents related to NI-ICS services requires further attention
- For the first time, incidents concerning confidentiality and authenticity were reported.
- Malicious actions doubled in 2021 (noticed a spike of 8%), though they continue to be the cause of the minority of incidents
- System failures continue to dominate in terms of impact, but the downward trend continues
- Incidents caused by human errors remain at the same level as in 2020.
- In 2021, we observed a noteworthy decrease in incidents that were flagged as third-party failures



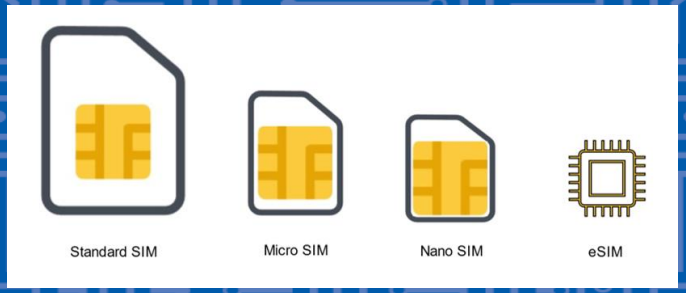
SECURITY CHALLENGES IN FIXED-LINE NETWORKS

- Work split in three sections
  - ✓ Fixed-line core and access network
  - ✓ Customer Premises Equipment (CPEs)
  - ✓ Sub-sea cables

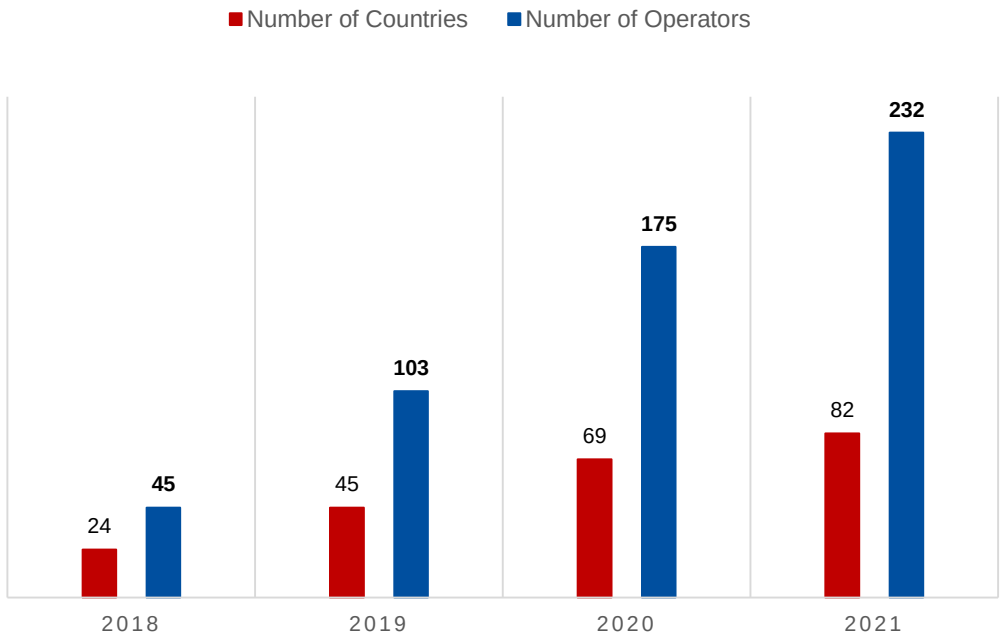


Create a list of security controls mapped to security challenges and corresponding evidence that can be used for security reviews either by Authorities or by operators themselves

EMBEDDED SIM DEEP DIVE



- The global market for eSIM is currently estimated at € 622.7M
- Projections suggest, that the global eSIM market will reach approximately € 1.7B by the year 2026, thus growing at a Compound annual growth rate of 28%

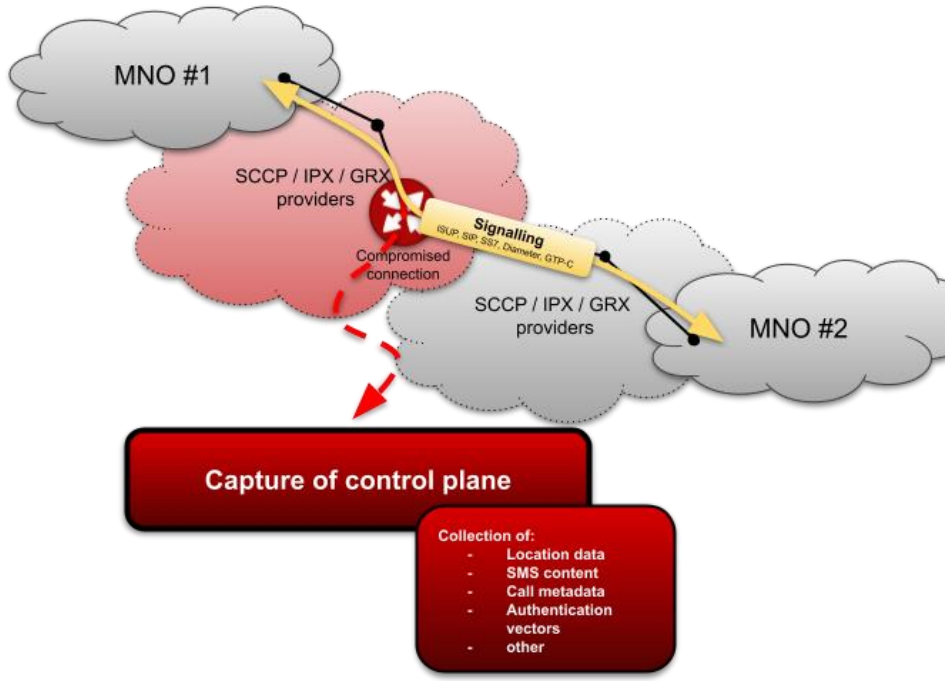


- Our report will
  - ✓ Present the eSIM ecosystem and usage in Europe
  - ✓ Analyze the eSIM technology and security aspects in different setups (Consumer and M2M)
  - ✓ Focus on security challenges
  - ✓ Provide security good practices
  - ✓ Provide recommendations for security reviews
- Planned to be published by end 2022

SIGNALING SECURITY CHECKLIST

- Give an overview of signalling protocol vulnerabilities, threat actors and their TTPs,
- Analyse real incidents
- Provide a security measures checklist

- Explain the roaming signalisation protocols and their evolution towards 5G
- Analyse common signalling attacks
- Present security controls to efficiently mitigate attacks

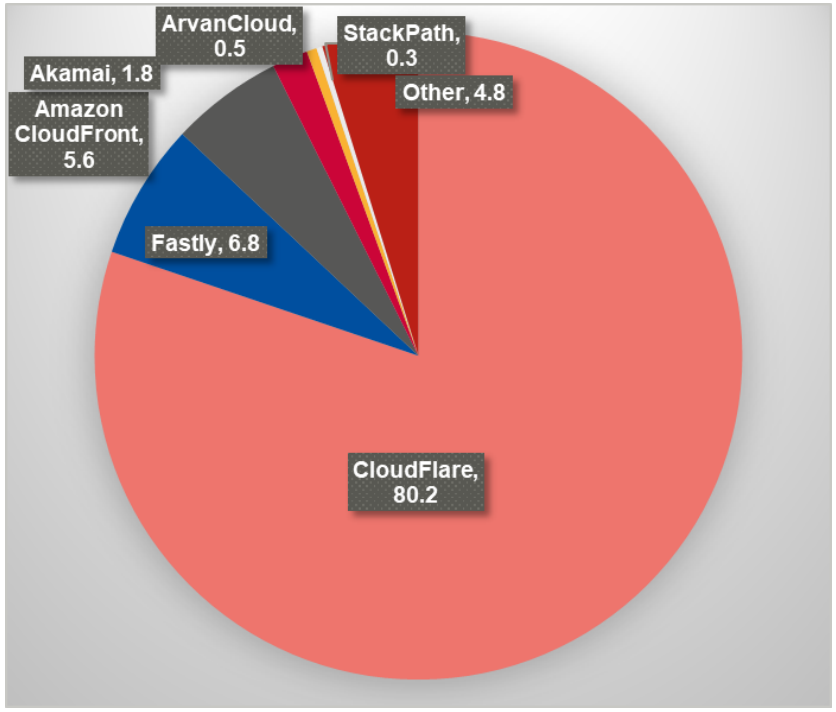


Compromised connection of signalling between two MNOs

CLOUD, FOG AND EDGE COMPUTING IN 5G: SECURITY OPPORTUNITIES AND CHALLENGES

- Analyse solutions and approaches related to cloud, fog and edge computing for 5G networks
- Present an overview of the standardisation landscape for the above areas
- Explain some basic usage scenario and how the approaches support Internet of Things and other emerging applications over future wireless network architectures
- Analyse the opportunities and security challenges

CONTENT DELIVERY NETWORKS (CDN)



Market share by the customer base

Source: W3Tech

https://w3techs.com/technologies/overview/proxy

- A CDN offers better security and performance compared to a single site
  - Due to consolidation a small outage is amplified by the amount and importance of content leading to significant impact

- Content providers should spread risks
  - Multi-CDN set up
    - Distributing content using multiple CDNs
    - Also a strategy to achieve higher performance
  - Diversity in DNS providers
    - Do not rely on a single providers
    - Various approaches for using different CDNs can be applied

VERIFICATION AND IDENTIFICATION OF DOMAIN NAME OWNERS

Study is intended to research, identify and capture initiatives, good practices and case studies

- Mapping of the process and relevant stakeholders with their roles and responsibilities
- Identifying challenges, vulnerabilities, assets involved, as well as relevant attack scenarios;
- Assessing the associated risks for the process;
- Exploring good practices and security measures

WE VALUE YOUR FEEDBACK

Connect with ENISA