In the Name of GOD



Expert Group Meeting of UESCAP on
Transport Connectivity and Logistics:
Emerging opportunities and challenges for enhancing rail connectivity along the Trans-Asian Railway network

Cyber Security Measures in Iranian Railways (RAI)

Iranian Railways connection Neighbor Countries



Security Experience

Due to the extensive network of the Islamic Republic of Iran Railways throughout the country and the multitude of services provided, the network of this organization is constantly exposed to various cyber attacks from both domestic and foreign sources. Therefore, maintaining the availability and security of these services is of paramount importance. The set of measures taken to ensure security is outlined below:



Iran Railways
www.rai.ir

Security Experience

- ISO/IEC 27001(information security management systems (ISMS))
- Pentest
- SOC
- CSIRT
- MSSP
- Access Control



Iran Railways
www.rai.ir

Lessons learned from attacks

In recent years, various attacks have been carried out on the network of the Islamic Republic of Iran Railways, with one of the most significant occurring in the year 2021, resulting in the partial disruption of applications and network infrastructure. According to assessments, the source of this attack was a vulnerability in one of the network devices, which unfortunately, due to sanctions-related issues, could not receive security updates. The recovery process following this attack has provided valuable lessons for the organization, which will be shared with you below:

Lessons learned from attacks

- Patch Management
- Backup Policy
- Backup Site
- APT Detection
- Forensic
- Threat Intelligence



Iran Railways
www.rai.ir

THANKS FOR YOUR ATTENTION

