सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF HOUSING AND URBAN AFFAIRS

ACHIEVING CYBER SECURITY IN MOBILITY ECOSYSTEM

15th Urban Mobility India Conference & Expo2022

GAP ANALYSIS

- Protection mechanisms/processes taken to ensure Confidentiality, Integrity, Availability, and Privacy of the user data

- Adequacy of the Technical security practices present, as on date

AREAS OF CONCERN

1. Security status of sensitive installations and strategic assets, which includes
   i. IT infrastructure,
   ii. Network,
   iii. Software applications including mobile apps
   iv. Sensors/End point devices/IOT devices/Wearables and the various services.
2. Security issues arising out of critical telecom and IT products, sourced from outside of India.

SUGGESTED APPROACH

- Vulnerability Assessment / Penetration Testing (VA/PT)
- End Point Security
- Sourcing of critical telecom and IT products from Trusted sources
- Process Audit

VULNERABILITY ASSESSMENT / PENETRATION TESTING (VA/PT)

- Cybersecurity status of servers and network devices
- Cybersecurity status of the Software Applications
- Security status of the Mobile Applications, if any
- Security measures, taken during API integration
- Overall Network Architecture
- Security robustness of Internet facing IPs /URLs , through Penetration Testing

END POINT SECURITY

- Security status of End point devices, like smart cameras .
- Overall Network Architecture (for deployment of end point devices) from security point of view

SOURCING OF CRITICAL TELECOM AND IT PRODUCTS

Compliance status of ‘Trusted Electronics Value Chain’ (TEVC), while acquiring ICT components , with special attention towards the possible security issues, arising out of sourcing of critical telecom and IT products from border sharing countries

PROCESS AUDIT

Information Security Management System (ISMS) to be established in line with ISO 27001 standard covering Cyber security policy, procedures, and guidelines

- Co-ordinate with respective stakeholders to perform the risk assessment and implementation of security requirements
- Provide security awareness trainings
- Facilitate the internal review
- Support during certification audit by an external agency

WAY FORWARD

- All web-based applications shall be tested and hardened as per the requirements of OWASP ASVS
- All Mobile Apps shall be tested and hardened as per the requirements of OWASP MASVS
- All servers and network devices including endpoint devices shall be hardened before deployment and regularly patched

WAY FORWARD …

- The various agencies involved to come out with an action plan for implementation of Information Security Management system, adhering to the requirements of ISO/IEC 27002.
- The service providers should ensure compliance with the requirements of ‘Trusted Electronics Value Chain’, while sourcing the components (Hardware /software /service) form overseas suppliers.
- Cyber Security Model Framework for Smart Cities’, issued by MoHUA to be referred in future RPFs