Alireza khodadoost

Cyber Security Management

Iran airports and air navigation company

Introduction

Iran airports and air navigation company (IAC)

- 54 Operational Airports
- Air navigation service provider in Iran airspace.

Big attack surface

- Wide and complicated network
- Wide range of aeronautical and airport operation systems

IAC assembled cyber security committee to develop cyber security strategy in 2018

- Senior Management Involvement

Strategies

- Increasing cyber security awareness
  - Seminars and courses about cyber security in general and IT staff specifically
- Addressing identified threats
- Focus on core functions

Strategies - *continued*

- Mitigation and Hardening
  - Network infrastructures
  - Operating systems and Databases
  - Business-critical systems

Strategies - *continued*

- SOC
  - At first limit the scope for monitoring, detection, response, recovery
  - Add airports step by step
  - 24/7 Support based on agreed SLA

Strategies - *continued*

- CERT/CSIRT
  - Forensic
  - Security assessment

SOC Center

- Identify and define business objectives
- Choose SOC models and procedures based on functional requirement
- Design technical architecture
  - Define workflow
  - Choose threat Lifecycle Management Platform

SOC Center

- Choose technology
  - Localized SIEM
- Install SIEM sensors and Integrate with systems

Challenges

- Budget
- Network structure redesign
- Geographically dispersed network around the country

Challenges - *continued*

- Legacy systems
  - Don’t generate required Logs
  - Integration with SIEM
  - No security consideration
- Lack of trained staff about cyber security in remote places

Vulnerability and threats detected (3 months duration)

HQ

Vuln. Cat.	Frequency
Critical	2
High	79
Medium	159
Info	1827
Total	2067

OIII

Vuln. Cat.	Frequency
Critical	0
High	15
Medium	30
Info	236
Total	281

OIMM

Vuln. Cat.	Frequency
Critical	6
High	61
Medium	132
Info	988
Total	1187

Current state

- About 4000 EPS
- About 75 incident per hour
- 130 ticket in last 45 days
- We have successfully detected and mitigated several attacks after our long journey.

Road map

- Extend the scope of SOC to all airports and systems
  - Addressing HA and resiliency concerns and moving towards distributed architecture
- Installation distributed firewalls everywhere with centralized control
- Providing cyber security visibility to all stakeholders about their systems

Road map

- Penetration test on our software/networks
- Centralized vulnerability detection and management
- Centralized remediation for detected vulnerability
- Deploy Red team/Blue team

CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019

ICAO MID

Thank You