1st Aviation Cyber Security Exercise in Turkey

The Interregional Aviation Security and Facilitation Seminar,
Cairo, Egypt 13-15 November 2018

Demet ÇITIR

Outline

- Cyber Security Structure in Turkey
- Cyber Security Exercise
  - Aim and Scope of Cyber Security Exercise
  - Methodology of the Exercise
  - Results and Lessons Learned From Cyber Security Exercise

Cyber Security Structure in Turkey

- National Cyber Security Action Plan and Strategy
  - National Cyber Events Response Center (USOM)
  - Critical Infrastructures
  - Sectoral and Corporate CERTs

Corporate CERTs

- 26 Corporate CERTs with 107 employees
  - 12 Airline Companies
  - 3 Ground Handling Companies
  - 10 Airport and Terminal Operators
  - 1 Air Navigation Service Provider

- MRO, RAs, Airport Suppliers (Fuel)

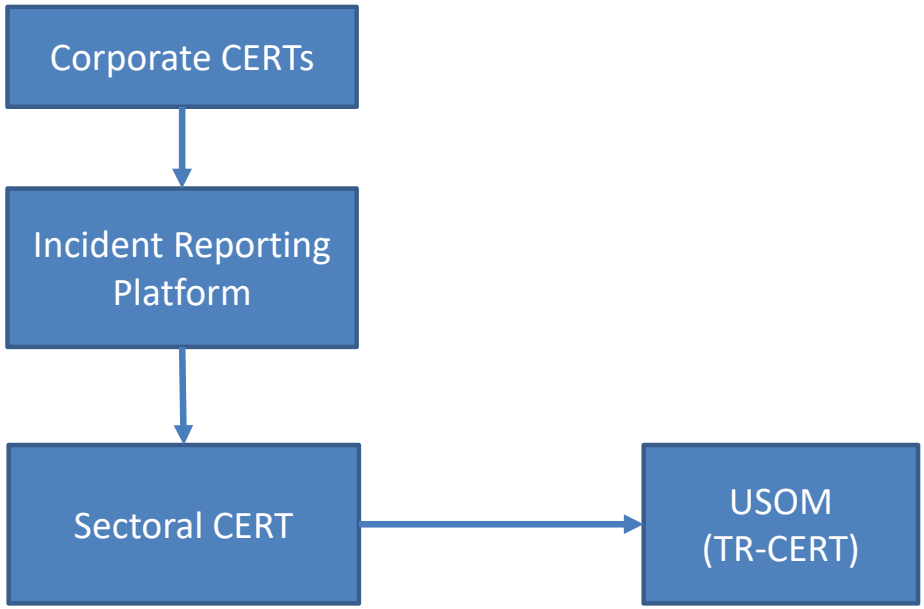
Responsibilities of CERTs

- Establishing and managing Corporate CERT
- Incident response management and coordination
- Continuous system testing and inspection
- Enhance cyber security culture

Responsibilities of CERTs

- Cyber security risk assessment and mitigation process
- Log management
- Cyber security intelligence related to their operations and business reputation
- The disaster recovery center for critical systems

Incident response management and



The Aim of Cyber Security Exercise

- To determine
  - effectiveness of the preventive measures
  - effect of a possible cyberattack on aviation entities
  - identify vulnerabilities
  - cyber security awareness level
  - effectiveness of reporting mechanisms

The Scope of Cyber Security Exercise

Type of Operation	Companies Included(%)	Total Operation(%)
Airlines	35	80
Airport/Terminal Operators	30	75
Ground Handling Companies	66	60
ANSPs	100	100

Methodology

- Blackbox/Greybox Penetration Tests
- Social Engineering Tests
- Denial of Service Tests

Blackbox/Greybox Penetration Tests

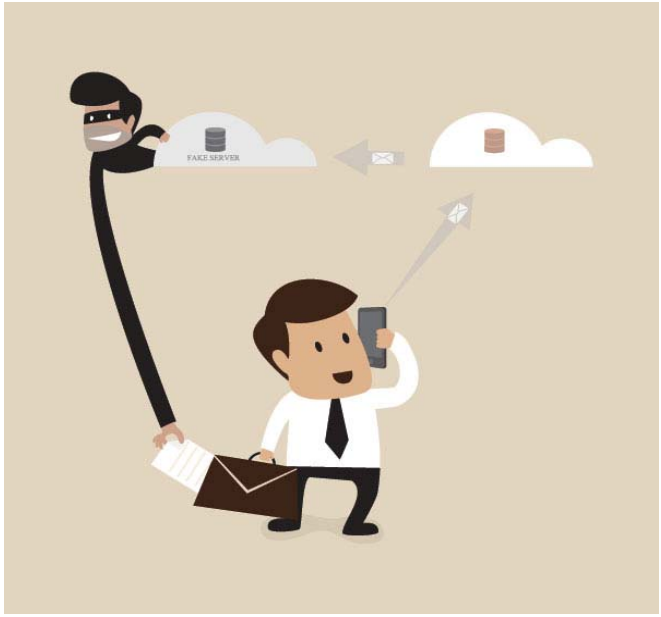
- Gathering cyber intelligence
- Sector related previous cyber attacks
- Attacks that damage reputation
- Exfiltration of sensitive information
- Testing cooperation and escalation procedures

Social Engineering Tests

Phishing Mails

@VectorStock.com

Methods of Social Engineering Tests



Phone (Voice) Phishing

Denial of Service Tests on Critical Infrastructures

- DoS/DDoS Test
  - On IT Systems
  - On Operational Systems

@securityintelligence.com

Outcomes of Blackbox/Graybox Penetration Tests

Results	Actions
Configuration quality of the cyber security systems are lacking in several cases and needed to be improved to deal with these types of attacks.	To increase staff quality among corporate CERTs the technical training requirements increased significantly and globally recognised cyber security certificates made mandatory
We have found a couple of IT System vulnerabilities that can affect operational systems and business continuity.	To identify risks and mitigate them before a possible cyber attack Turkish DGCA stricten its regulations by increasing system testing requirements.

Outcomes of Social Engineering Tests

Results	Actions
Phishing mail success rate among participant aviation entities are a little bit below accepted threshold.	We deducted from our results aviation entities in Turkey somewhat capable with coping phishing mail related attacks such as petya, notpetya.
Phone phishing test results showed us participant aviation entities need to significantly improve themselves in this particular area.	In order to enhance cyber security culture among aviation entities and ensure a high level of staff awareness, the training content requirements were reviewed and mandatory cyber security training requirements were increased significantly. Entities were also required to carry out quarterly cyber security awareness testing among their employees.

Outcomes of DoS/DDoS Tests

Results	Actions
DoS/DDoS tests on many participating companies were not satisfactory because companies majorly rely on configurations made by ISPs.	To rectify this commonly shared probable vulnerability, a requirement was introduced into regulation for Dos/DDoS tests on critical systems to be carried out by accredited companies annually.

Incident Reporting Mechanism

Results	Actions
Late response by corporate CERT's representatives.	Incident reporting mechanisms are reminded.
Using reporting mechanisms that do not comply with our regulations such as phone calls, emails, etc.	Incident reporting mechanisms are reminded.

THANK YOU

Demet ÇITIR
00903122036052
sektorelsome@shgm.gov.tr