International Civil Aviation Organization

Twenty Eighth Meeting of the Communications/ Navigation and Surveillance Sub-group (CNS SG/28) of APANPIRG

Bangkok, Thailand, 01-05 July 2024

Agenda Item 12: Cybersecurity of CNS/ATM systems

12.2 Other Cybersecurity related matters

STRENGTHENING AVIATION CYBERSECURITY THROUGH ORGANIZING ATTACK-WITH-DEFENCE EXERCISE

(Presented by Hong Kong, China)

SUMMARY

In the ever-changing landscape in aviation cybersecurity, traditional training may not provide cybersecurity personnel with real-world experience in handling actual cyber-attacks. Organizing an Attack-with-Defence exercise under simulated and controlled environment is beneficial in strengthening cybersecurity personnel's understanding on attacker's mindset and skills, while enhancing awareness and preparedness to respond to cyber-attacks.

1. INTRODUCTION

1.1 In alignment with the ICAO Aviation Cybersecurity Strategy, particularly one of the pillars of "Capacity Building, Training and Cybersecurity Culture", it is essential to raise awareness and emphasize that building cybersecurity culture is everyone's responsibility. In coping with the ever-changing cyber-attacks in aviation landscape, it is crucial to continuously enhance the skills of cybersecurity personnel to respond to cyber-attacks. The Attack-with-Defence (AWD) exercise is a vital part of cybersecurity training and preparedness, where participants simulate cyber-attacks and defend their systems against simulated threats. The main goal is to enhance the skills and readiness of cybersecurity professionals, incident responders, and network defenders.

1.2 AWD exercise provides a realistic environment for testing an organization's cybersecurity readiness. Traditional classroom-based training may not give cybersecurity teams the real-world experience of dealing with actual cyber-attacks. AWD exercise bridges this gap by simulating different cyber-attack scenarios.

1.3 AWD exercise involves team-based Capture-the-Flag (CTF) competition, promoting active participation and collaboration. Teams combine their skills and knowledge, fostering problem-solving and creativity. The competitive atmosphere encourages quick actions and decisive decision-making. Participants are engaged more enthusiastically, leading to a positive and productive learning process.

2. DISCUSSION

Overview of AWD Exercise

2.1 In March 2024, the Hong Kong Civil Aviation Department (HKCAD) organized the inaugural AWD exercise in collaboration with cybersecurity consultants. The exercise aimed to strengthen the HKCAD personnel's ability to detect, respond and recover from simulated network attacks, while providing insights into hacker's mindset and skills.

2.2 Participants, including operation, technical and management staff, were divided into teams with a good mix and competed to earn points. Prior to the competition, a training session was arranged to get the participants familiarized with cyber-attacks and network hardening. All these practical sessions were conducted with an online platform using different tools.

2.3 AWD exercise strengthened participants' technical abilities in attack and defence, teamwork, and real-time strategy. In the attack and defence mode, each team defended one or more virtual machines with identical configurations. Within limited time, teams also needed to identify and exploit vulnerabilities of virtual machines of other teams to capture a "flag" or piece of information, thereby earning points.

Competition Question Types

2.4 The competition featured two main types of challenges. The first challenge focused on finding and exploiting security weaknesses in websites. Participants tackled issues like code injection, file upload vulnerabilities, and deserialization problems. The second challenge involved manipulating computer programs (usually written in PHP, Java, or Python) to gain control over them.

2.5 Additional question types like cryptography and reverse engineering could be considered, but due to limited time, only the above two challenges were used in the exercise. In fact, questions or challenges can be customised to match with participants' skill levels, enhancing the effectiveness of learning.

Competition Stages

2.6 The competition was divided into two stages: the "Reinforcement" stage and the "Attack and Defence" stage, each occurring in iterations one after the other. During the "Reinforcement" stage, the target network of each team was not connected to others, allowing each team to perform activities such as data backup, code auditing, and vulnerability repair. In the "Attack and Defence" stage, teams were free to attack other teams or defend their own environment. Effective coordination among team members was crucial, with segregated duties between attack and defence to maximize points gained and minimize points lost.

Competition Visualization

2.7 A virtual platform was provided to visualize real-time competition status, scoreboard and time remaining, creating an engaging environment for participants and audience.

Conclusion

2.8 In the light of the encouraging results, HKCAD plans to organize similar AWD exercise for (1) professional cybersecurity personnel, and (2) general staff, through exercises with different levels of complexity on a regular basis.

2.9 Based on the subsequent feedback from participants and HKCAD's observation, AWD exercise bridges theory and practice, preparing cybersecurity professionals for the evolving threat landscape. By simulating real-world scenarios, participants could enhance their skills, adaptability, and teamwork. In sum, staying proactive in combating cyber threats is crucial in the dynamic world of cybersecurity.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) acknowledge the commendable efforts of Hong Kong, China in organizing the Attack-with-Defence (AWD) exercise in collaboration with cybersecurity consultants, to actively engage aviation professionals in offensive and defensive activities, helping participants develop critical skills, enhance incident response capabilities, and contribute to overall cybersecurity resilience;

b) seek assistance from ICAO APAC Office in organizing seminars/workshops, bundled with similar AWD exercise, that facilitate the acquiring and sharing of experience in cybersecurity among States/Administrations and industry partners; and

c) encourage States/Administrations to collaborate effectively in addressing cybersecurity threats.

– – – – – – – – – – – –