TECHNICAL AND COMPLIANCE COMMITTEE
Twentieth Regular Session
25 September to 1 October 2024
Pohnpei, Federated States of Micronesia (Hybrid)

WCPFC Information and Network Security

WCPFC-TCC20-2024-31
30 August 2024

Submitted by the Secretariat

Purpose

1. The purpose of this paper is to provide an update to TCC20 on activities undertaken by the Secretariat since TCC19 to secure the Commission's online databases and other information management systems. This paper will also provide information on the Secretariat's plans over the next 12-18 months to develop a cyber and information security governance framework that is relevant for the WCPFC and aimed at minimizing and mitigating risks to WCPFC data and information security in the future.

Background

1. The Secretariat provided updates to TCC19 on efforts since TCC18 to secure WCPFC's IT systems managed by the Secretariat. TCC18 supported the Secretariat's plans to expand security review activities in 2024, including development of an IT Systems Risk Register and the conduct of routine security reviews, including penetration (PEN) testing. On the recommendation of TCC19, the Commission at WCPFC20 supported a budget of USD15,000 for the Secretariat to carry out PEN testing in 2024 on the Commission's online databases and Secretariat IT infrastructure. The purpose of the PEN tests was to identify any security risks as well as determine the current state of the Secretariat's "security posture".

2024 Updates

2. Noting the intention expressed by the Secretariat at TCC19 to shift away from an annual, limited-in-scope security audit to a continuous, systems security mindset, the Secretariat completed two distinct PEN tests in late 2023[1] and early 2024, focused on the Secretariat's external facing systems (2023) followed by a focus on the Secretariat's internal IT infrastructure (2024).

[1] The results of the 2023 penetration test were not available until early 2024.

2. In late 2023, the Secretariat contracted the services of DEFEND[2] to perform a security review of the Secretariat's public facing web applications. The goal of the review was to assess and identify any technical security vulnerabilities pertaining to the reviewed applications and provide assurance that the level of security is suitable for the WCPFC, adheres to applicable security standards, and adheres to good security practice.

3. The security assessment focused on good security practices related to web application security and found that major security hardening practices are followed which indicates a level of maturity.

4. Six inconsistencies were identified and detailed in the assessment report[3]. Of the six findings identified through the PEN test of the Secretariat's external facing systems, two were subsequently confirmed to be "false positives", two were resolved immediately following the PEN test, and two are being addressed by the main website upgrade that is currently underway.[4]

5. In 2024, the Secretariat contracted the services of BPM[5] to conduct an internal PEN test to identify potential security vulnerabilities in the Secretariat's on-premises IT infrastructure. The internal testing was supplemented with targeted social engineering tests.

6. The findings of the internal penetration tests were classified on the following four levels: low; low-medium; medium; high. Of the findings, one was classified as high risk and was related to the social engineering tests. Work to mitigate these risks is underway through additional staff training and improved internal standard operating procedures. Three findings were considered medium-risk and have been addressed or are in progress. Three findings were classified as low-medium and are being further assessed on the basis of a cost versus risk benefit analysis. Five low risk issues are also being considered by the Secretariat.

7. In addition to routine PEN testing, the Secretariat is continuing to review its IT and database structures with a view to future-proofing the Commission's systems. The heavy reliance on online systems, coupled with the continuous advancements in technology, necessitates staying current and, whenever possible, anticipating technological and web-based application changes that could affect the Commission's interactions with its data holdings. This ongoing internal review is being undertaken as part of a longer term effort to ensure that the Secretariat is implementing best practice cybersecurity measures that are appropriate for an organization like the WCPFC.

8. As part of the Secretariat's ongoing security review, targeted online training courses and phishing campaigns have been implemented for Secretariat staff on a regular basis using the

[2] https://defend.co.nz/

[3] The report is classified as CONFIDENTIAL to protect sensitive information relating to the Secretariat's current cybersecurity framework.

[4] Two findings related to the outdated hosting platform of the WCPFC website, which in the process of being resolved through the migration from the older Drupal 7 platform to the updated Drupal 10 platform.

[5] https://www.bpm.com/

KnowBe4[6] platform to teach new skills as well as refresh users on the cyber threats that might be encountered in the course of their work.

Conclusions and Next Steps

9. Overall, the findings from the two PEN tests suggest that the Secretariat's security posture is robust. Continuous efforts by the Secretariat's ICT team to identify and resolve issues before they arise have contributed to this relatively strong security posture.

3. The risk score from the online training places the WCPFC above industry average, for a similar organization type and size, however the high-risk findings from the internal PEN test prove the need to constantly evolve and assess the training effectiveness.

10. The expanded security audit of the Commission's online databases and IT infrastructure will form part of a larger security governance framework that the Secretariat envisions as necessary for the organization. In early 2025, the Secretariat will focus on the development of a security risk register through an exercise to identify and assess the potential security risks that might apply to an organization such as the WCPFC. The outcome of this exercise is expected to inform the nature of an organizational framework for information and cybersecurity that is relevant to the WCPFC.

11. The cybersecurity landscape is constantly evolving. The TCC's support for a broader and more continuous approach to cybersecurity has improved the Secretariat's security posture, and it will continue to improve through the development of the information security governance framework. The framework will allow the Secretariat to systematically classify risks, and document its approach to mitigate or accept them.

[6] https://www.knowbe4.com/