منظمة الطيران المدني الدولي

ورقة عمل

A41-WP/488[1]
EX/235
2/8/22

الجمعية العمومية — الدورة الحادية والأربعون

اللجنة التنفيذية

البند رقم ١٥: برنامجا التدقيق – نهج الرصد المستمر

تعزيز أفرقة التدقيق للبرنامج العالمي لتدقيق أمن الطيران وفقا لنهج الرصد المستمر (USAP-CMA) لأغراض تقييم وتنفيذ مقتضيات الأمن السيبراني الواردة في الملحق السابع عشر

(ورقة مقدمة من فنزويلا (جمهورية – البوليفارية) بدعم من بوليفيا (جمهورية – متعددة القوميات) وكولومبيا وكوستاريكا وبنما وبيرو وأوروغواي))[2]

الموجز التنفيذي

يتضمن البرنامج العالمي لتدقيق أمن الطيران، حاليا، مبادئ توجيهية تمكن الدول من تقييم الأداء العام للنظام الوطني لمراقبة أمن الطيران. وهذا ما أتاح إعداد توصيات لتحسين الأداء بالاستناد إلى المبادئ المشتركة لأمن الطيران. ويتولى إجراء التقييم فريق من المدققين للتأكد من أن هذه الأنشطة تغطي العناصر الحاسمة لنظام مراقبة أمن الطيران علاوة على القواعد القياسية الواردة في الملحق السابع عشر — "أمن الطيران" ومدى الامتثال لها. ذلك أن هذا الملحق يحدد كيفية إعداد وتنفيذ تدابير لحماية نظم المعلومات والاتصالات فضلا عن البيانات الحاسمة المستخدمة لأغراض الطيران المدني. وبناء عليه، يتعين تعزيز أفرقة التدقيق من خلال إعداد مواد إرشادية أو تدريبية تمكنها من تقييم مقتضيات الأمن السيبراني الواردة في الملحق السابع عشر وتنفيذها.

الإجراء: الجمعية العمومية مدعوة إلى القيام بما يلي:

أ) أن تحيط علما بالمعلومات الواردة في هذه الورقة؛

ب) أن تطلب إلى المجلس إعداد أدوات أو مواد تدريبية لمد أفرقة التدقيق بتوجيهات وافية وتدريب كاف في مجال الأمن السيبراني بما يمكنها من إجراء تقييم فني وموضوعي لأسئلة البروتوكول بما يتماشى والجوانب التخصصية بهذا المجال من الطيران المدني.

الأهداف الاستراتيجية:	ترتبط ورقة العمل هذه بالهدف الاستراتيجي "الأمن والتسهيلات".
الآثار المالية:	نقترح الاضطلاع بالأنشطة المذكورة في هذه الورقة باستخدام الموارد من ميزانية البرنامج العادي للفترة الثلاثية الحالية و/أو الموارد خارج الميزانية
المراجع:	التوصية ٤-٩-١ في الملحق السابع عشر وبروتوكول البرنامج العالمي لتدقيق أمن الطيران وفقا لنهج الرصد المستمر (USAP-CMA).

[1] قدمت فنزويلا (جمهورية – البوليفارية) النسخة الإسبانية لهذه الورقة.

[2] الدول الأعضاء من إقليم أمريكا الجنوبية الأعضاء في لجنة الطيران المدني لأمريكا الجنوبية (LACAC).

١- المقدمة

١-١ يوفر البرنامج العالمي لتدقيق أمن الطيران (USAP) للدول مبادئ توجيهية تتيح تقييم الأداء العام للنظام الوطني لمراقبة أمن الطيران. وهذا ما مكن من إصدار توصيات للتحسين بالاستناد إلى المبادئ المشتركة لأمن الطيران. ويتضمن البرنامج العالمي (USAP) وبروتوكول البرنامج العالمي لتدقيق أمن الطيران وفقا لنهج الرصد المستمر (USAP-CMA) حاليا أسئلة محددة (١٣٤٥ و١٣٥٠ و١٣٦٠ و٣٢٧٨) تتصل بتقييم الجوانب العامة والأساسية لإعداد وتطبيق تدابير لحماية شبكات تكنولوجيا المعلومات والاتصالات فضلا عن البيانات الحاسمة المستخدمة لأغراض الطيران المدني.

١-٢ ويتولى إجراء هذا التقييم فريق من مدققي البرنامج العالمي (USAP) يكفلون تغطية العناصر الحاسمة من نظام مراقبة أمن الطيران إلى جانب أحكام القواعد القياسية المنصوص عليها في الملحق السابع عشر ومدى الامتثال لها. ويلزم الملحق الدول بإسناد المسؤوليات وتحديد معايير وطنية لحماية المنظومات المقترنة بعمليات الطيران من خلال تنفيذ تدابير حمائية، وتحديد النظم الحاسمة، والاضطلاع بالرصد على نحو متواصل، وضمان الكشف عن الهجمات السيبرانية وتحليلها والتصدي لها، وتقييم نوعية أنشطة المراقبة التي تضطلع بها الدولة على أساس تقييم المخاطر.

٢- التحليل

٢-١ بالنظر إلى أهمية الأنشطة المنفذة ضمن البرنامج العالمي لتدقيق أمن الطيران وفقا لنهج الرصد المستمر (USAP-CMA)، من المهم ضمان وجود مواد إرشادية، في مجال الأمن السيبراني، تتيح لفريق التدقيق إجراء تقييم فني وموضوعي لمدى تنفيذ المعايير الدولية والاستراتيجيات وأفضل الممارسات التي تعدها وتتبعها الدول لتحديد وحماية النظم الحاسمة لتكنولوجيا المعلومات والاتصالات من أي تدخل من شأنه أن يقوض سلامة أو تشغيل منظومة الطيران المدني.

٢-٢ هناك في الوقت الراهن إطارات مرجعية وممارسات منطبقة على الصعيد العالمي أتاحت لمختلف المؤسسات إدارة المخاطر السيبرانية بشكل فعال والحد منها. ومن الأمثلة على ذلك سلسلة معايير المنظمة الدولية للتوحيد القياسي ISO/IEC-2700 الرامية إلى ترسيخ أفضل الممارسات بشأن مختلف جوانب إدارة أمن المعلومات، ومواصلة تحسينها والتخفيف من المخاطر؛ ودليل أهداف الرقابة المتعلقة بتكنولوجيا المعلومات (COBIT)؛ ومنهجية "ماغريت" لتحليل المخاطر وادارتها بالنسبة لنظم المعلومات، وغيرها من المعايير والمبادئ التوجيهية والممارسات الفضلى الدولية.

٢-٣ وتعكس الوثائق المرجعية المذكورة آنفا تقدما ملحوظا في التعاون والتكامل، على الصعيد العالمي، في مجال الأمن السيبراني، حيث أتاحت مسارات للعمل ومعالم إرشادية منطبقة ومشتركة بين جميع أنواع البنى التحتية الحاسمة. وتتصل المعالم الإرشادية تحديدا بمعايير القطاع وبالمبادئ التوجيهية والممارسات الفضلى التي تتيح إعمال الأمن السيبراني وتقييمه، ليس فحسب على مستوى المؤسسات أو من حيث الوثائق، وانما أيضا فيما يتعلق بالعمليات والتنفيذ.

٢-٤ وبناء عليه، نقترح إعداد مواد إرشادية موحدة تتيح استحداث إطار مرجعي على أساس أفضل الممارسات في القطاع ومنهجيات وتجارب الدول من أجل التوصل إلى نهج متناغم. وليس من الضروري أن تكون وثيقة الإرشادات وثيقة جامدة، وانما وثيقة تمكن فريق المدققين للبرنامج العالمي (USAP) من إجراء تقييم فني وموضوعي لمستوى الامتثال للقواعد القياسية، مع مراعاة خاصيات واحتياجات كل واحدة من الدول على النحو المبين في أسئلة البروتوكول ١٣٤٥ و١٣٥٠ و١٣٦٠ و٣٢٧٨.

٢-٥ يعرض المرفق بهذه الورقة محتوى نموذجيا لمجالات المعرفة والمواد الإرشادية. ويستند هذا المحتوى إلى المعايير المستقاة من مختلف القواعد القياسية والمبادئ التوجيهية والممارسات السارية في إدارة أمن المعلومات وتحسينها المتواصل والتخفيف من المخاطر بمختلف المؤسسات التي لديها بنية تحتية حاسمة ذات بعد دولي. ويسلط المرفق الضوء على ما يلي:

أ) مجالات المعرفة والخبرة التي يحتمل أن يكون من الضروري اكتسابها لتقييم التدابير الخاصة بالأمن السيبراني والتي تطبقها الدول (عملا بأسئلة البروتوكول)؛

ب) المحتوى المقترح لدى صياغة النصوص أو المواد الإرشادية لتمكين فريق التدقيق من تقييم وتنفيذ مقتضيات الأمن السيبراني الواردة في الملحق السابع عشر.

٣- الاستنتاج

٣-١ من الأساسي لفريق التدقيق المكلف بتنفيذ البرنامج العالمي لتدقيق أمن الطيران أن يمتلك الأدوات والمعارف اللازمة لإجراء تقييم دقيق وموضوعي لمدى وفاء الدولة بمهام الحماية، من حيث التصميم والتحديد والتنفيذ، لأغراض أمن الطيران، وفقا لمقتضيات القواعد والتوصيات الدولية الواردة في الملحق السابع عشر — أمن الطيران، الصادر عن الإيكاو.

— — — — — — — —

المرفق

المضمون المقترح لمجالات المعرفة والمواد الإرشادية

أ) مجالات المعرفة والخبرة اللازمين لتقييم ما تنفذه الدول من تدابير الأمن السيبراني

الإلمام بإجراءات وتقنيات إدارة الأصول والعمليات الحاسمة؛ تحديد وتقدير الأصول أو المعلومات التكنولوجية المتعلقة بالطيران؛ سياسات واجراءات وتدابير أمن المعلومات؛ إدارة المخاطر والحوادث؛ الضوابط أو الضمانات الإدارية التي تيسر التحفيف من آثار الاستنتاجات في مجال الأمن السيبراني؛ التدقيق في المجال الجنائي وتدقيق الشبكات والرموز والهشاشة والتدقيق المادي، وتحليل محتوى الشبكة الإلكترونية وغيرها.

القدرة الفنية على تقييم التدابير الحمائية من خلال إجراء التجارب، على غرار ما يلي: تجميع الأصول وتصنيفها وتحديدها، تفقد الخدمات، تحليل مواطن الهشاشة والتحقق؛ إجراء اختبارات تشغيلية لفحص شبكة الإمداد الكهربائي والمعدات والمصادر أو النظم المستقلة لدى تعطل الشبكة؛ اختبار المعدات لأغراض إدارة نظم المعلومات ومنصات تكنولوجيا المعلومات؛ اختبار التجهيزات وبرمجيات التشغيل والبنية التحتية و/أو تطبيقات البرمجيات؛ إجراء اختبارات أداء منصة تكنولوجيا المعلومات (في ظروف التوقف الكامل)؛ اختبار خدمات الدعم في مجال الإنترنت (الفصل عن الشبكة الرئيسية، التحقق من الربط مع الشبكة الثانوية، موازنة الحمل (أو الشحنة) وما إلى ذلك؛ اختبارات استرداد المعلومات وغيرها.

ب) المضمون المقترح لدى صياغة النصوص أو إعداد المواد الإرشادية تيسيرا لتقييم وتنفيذ المقتضيات الخاصة بالأمن السيبراني، المنصوص عليها في الملحق السابع عشر

١- دليل بشأن العمليات الحاسمة في قطاع الطيران المدني، موجهة لشركات الطيران (إدارة تدفقات الركاب والأمتعة والبضائع والمساعدة الأرضية وتحويل الطائرات وصيانة الطائرات، في جملة أمور)؛ العمليات الحاسمة في المطارات (أمن المطار، العمليات، والبنية التحتية للمطارات، الإدارة والطوارئ في المطارات، فضلا عن أمور أخرى)؛ العمليات الحاسمة في إدارة النقل الجوي (الاتصالات الصوتية، تبادل الرسائل وبيانات الرادارات الخاصة بالطيران، الملاحة الجوية، وما إلى ذلك).

٢- منهجية موحدة لتقييم المخاطر في قطاع الطيران تشمل تحديد السياق والسياسات والمسؤوليات، وتحديد الإجراءات التشغيلية، وجرد الأصول وتقديرها، والكشف عن مواطن الهشاشة ومصادر التهديد واحتمالات تحول هذه التهديدات إلى واقع وتقييم آثارها (تبعاتها).

٣- دليل بشأن الضوابط أو الضمانات بما في ذلك إدارة تجهيزات الشبكة، إدارة البرمجيات المرخصة وغير المرخصة، الشكل العام للأجهزة المتنقلة، الحواسيب الشخصية، الحواسيب المكتبية، الخواديم، استمرار عملية تحديد مواطن الهشاشة والتقويم، عمليات وأدوات تحديد الامتيازات الإدارية ومنعها وتصحيح سبل استخدامها (الشبكات/التطبيقات)، تحديث ورصد وتحليل نتائج التدقيق واجراءات حماية الرسائل الإلكترونية واجراءات حماية محركات البحث الإلكتروني، إدارة مخازن البيانات والبروتوكولات والخدمات في أجهزة الشبكة؛ الإجراءات القائمة على المنهجيات والأدوات المناسبة لتيسير الاختبارات الخاصة باسترجاع المعلومات؛ إجراءات تصميم أجهزة الشبكة بشكل مأمون (جدار الصد، والموجهات والأزرار)، الدفاعات المحيطة؛ إجراءات وأدوات حماية البيانات لمنع فقدان المعلومات والتخفيف من آثار الحوادث والاستجابة لها وغير ذلك من الضوابط.

— انتهى —