



الجمعية العمومية - الدورة الثانية والأربعون

اللجنة التنفيذية

البند رقم ١٣: أمن الطيران - السياسة العامة

خطط الطوارئ والتمارين الإلكترونية كوسيلة لزيادة القدرة على الصمود أمام التهديدات الإلكترونية

(ورقة مقدمة من البرازيل)

الموجز التنفيذي

تشدد ورقة العمل على ضرورة وضع خطط طوارئ للنظم الحيوية التي يستخدمها الطيران المدني، على النحو المبين في خطة عمل الإيكاو للأمن الإلكتروني المقابلة للركيزة ٦ لاستراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران، فضلاً عن تحسين الخطط نتيجة لتمرين التدريب بالمحاكاة على الهجمات الإلكترونية استناداً إلى الخصائص الحقيقية للنظم وإلى الحقائق التي لوحظت بالفعل والتي يمكن أن تؤدي إلى هذه الهجمات، على النحو المبين في خطة عمل الإيكاو للأمن الإلكتروني المقابلة للركيزة ٧ للاستراتيجية. وهي تسلط الضوء على تطور الهجمات الإلكترونية في الطيران المدني بالإضافة إلى أهمية المارين وخطط الطوارئ ذات الصلة.

الإجراء: الجمعية العمومية مدعوة إلى:

- أ) تعزيز إنشاء خطط لإدارة الوقائع الإلكترونية التي تتعامل مع البنية التحتية الحيوية للطيران؛
ب) إنشاء تدريبات إلكترونية منتظمة، بمشاركة الجهات المعنية من الحكومة والقطاع الخاص.

الأهداف الاستراتيجية:	ترتبط ورقة العمل هذه بالهدف الاستراتيجي: "ضمان السلامة والأمن لكل رحلة جوية"
الآثار المالية:	لا ينطبق
المراجع:	الركيزة ٦ (إدارة الحوادث والتخطيط لحالات الطوارئ) والركيزة ٧ (بناء القدرات والتدريب وثقافة الأمن الإلكتروني) في استراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران.

١- المقدمة

١-١ تمثل التهديدات الإلكترونية تحدياً كبيراً ومتزايداً لقطاع الطيران المدني، وهو نظام عالمي مترابط بطبيعته حيث يمكن لنقاط الضعف أن تساهم في الانتشار السريع للبرامج الضارة، مما يتسبب في تأثيرات عالمية واسعة النطاق. وفي حين أن التقدم التكنولوجي قد جلب العديد من الفوائد للطيران، لكنه أدخل أيضاً مشهداً متطوراً للتهديدات الإلكترونية بسبب الاعتماد العميق على البنى التحتية الرقمية. وإدراكاً لهذه الحاجة الملحة للحماية الإلكترونية وتحسين أنظمة الطيران الحيوية، تحدد استراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران مبادئ وتدابير وإجراءات تستند إلى سبع ركائز أساسية.

٢-١ وبالتالي تقترح ورقة العمل هذه تحديد بعض الإجراءات التي اتخذتها البرازيل لتحقيق قدر أكبر من تحسين الشبكة الإلكترونية في الحالات التي يمكن فيها للركبتين ٦ (إدارة الحوادث والتخطيط لحالات الطوارئ) و ٧ (بناء القدرات والتدريب وثقافة الأمن الإلكتروني) في استراتيجية الإيكاو للأمن الإلكتروني دعم الحماية الإلكترونية للأصول الهامة المستخدمة في مراقبة الحركة الجوية. ومن خلال تكامل هاتين الركبتين، يمكن للطيران المدني بناء دفاع شامل وقابل للتكيف، ليس فقط للرد على التهديدات ولكن لمنع تأثيرها والتخفيف من آثارها بشكل استباقي، مما يضمن استمرار سلامة وموثوقية السفر الجوي.

٣-١ تتضمن الركيزة ٦ إجراءات قوية للتعافي، ووجود خطط طوارئ واضحة ومختبرة للبدء الفوري في إجراءات استعادة الأنظمة والبيانات المخترقة، مما يضمن الحد الأدنى من تعطيل مراقبة الحركة الجوية والعمليات الأرضية وخدمات الركاب. ويتضمن ذلك النسخ الاحتياطية والنظم البديلة وخطوات الاستعادة التفصيلية.

٤-١ وتتناول الركيزة ٧ توعية وتدريب جميع المعنيين المشاركين في مراقبة الحركة الجوية، وتمكين كل فرد من مراقبي الحركة الجوية إلى موظفي الصيانة الأرضية من كيفية الاستجابة لحادث إلكتروني ودوره في الحفاظ على بيئة آمنة ومأمونة. وتعني ثقافة الأمن الإلكتروني القوية أن الجميع يدركون أنهم بمثابة خط الدفاع الأول المحتمل. وبالمثل، فإن التعلم والتكيف المستمرين أمران مهمان، مع الاعتراف بأن مشهد التهديدات الإلكترونية يتطور باستمرار ويلتزم بالتكيف مع استراتيجيات وتكنولوجيات الأمن الإلكتروني الجديدة. وهذا يعني عدم الاسترخاء والسعي دوماً للتحسين.

٥-١ هذه المبادئ ضرورية لتعزيز التعاون بين هيئات الأمن الإلكتروني في مجال الطيران المدني والمعنيين الآخرين بالاستجابة للهجمات الإلكترونية، ووضع سيناريو قوي تكون فيه خطط الطوارئ وسيلة للرد على هذه الإجراءات الضارة. وينبغي أن تتناول الوثيقة التنسيق بين جميع الجهات الفاعلة، مع إظهار جميع الآليات التي ستكون متاحة لاستعادة العمليات الطبيعية بعد التوصل إلى تسوية في كل نظام، وتسليط الضوء على المتطلبات الحيوية لتنفيذ إجراءات الاستجابة، والمساهمة في نظام إيكولوجي عالمي للطيران أكثر أماناً وتحسيناً.

٢- المناقشة

١-٢ تتحدث وسائل الإعلام كل يوم عن محاولات الهجمات الإلكترونية، بعضها ناجح والبعض الآخر لم يتم حتى الإبلاغ عنه بسبب احتوائه من خلال التدابير الوقائية المختلفة التي تطبقها الشركات والمنظمات للتعامل مع هذه الهجمات اليومية. والواقع ليس مختلفاً في قطاع الطيران. فالمهاجمون يبحثون بشكل أساسي عن نقاط الضعف التي لم يتم إصلاحها من أجل محاولة غزو وسرقة المعلومات وتعديل الأنظمة، والبحث بشكل عام عن مكاسب مالية.

٢-٢ وتعمل البرازيل، من خلال إدارة مراقبة المجال الجوي (DECEA)، على اتخاذ تدابير لجعل نظام مراقبة المجال الجوي البرازيلي أكثر تحسناً في سياق التهديدات الإلكترونية التي تتزايد يوماً بعد يوم. هكذا، وتأكيداً لفهم الإيكاو للموضوع وللتعبير عن اثنتين من الركائز المذكورة في استراتيجية الأمن الإلكتروني للمنظمة، تعمل إدارة مراقبة المجال الجوي على ترويج تمارين لتدريب أفرقة الاستجابة للحوادث التابعة لوكالات مراقبة المجال الجوي. وبالإضافة إلى المساهمة في تدريب الأفرقة، تساعد هذه التمارين أيضاً على تحديد فجوات الأمن الإلكتروني الناتجة عن مجموعات من الأنظمة والتطبيقات التي تم تطويرها لتلبية متطلبات عمليات مراقبة الحركة الجوية. تُجمع نتائج هذه التمارين في تقارير موجهة إلى الأفرقة المسؤولة عن تحسين النظم وخططة الطوارئ.

٣-٢ وفيما يتعلق بالتمارين، تكون كل محاكاة للحالة مصحوبة بتفاصيل يقدمها خبراء الصيانة في كل نظام للحصول على موثوقية الحالات التي تستند إلى أحداث حقيقية. ونتيجة لذلك، تصبح الإجراءات أقرب إلى الحالة الحقيقية وتسمح بتقييم أكثر دقة لاستخلاص تحسينات فعالة للإجراءات المعتمدة، وذلك بالنسبة لكل نظام (تحديد الثغرات) وللخطة نفسها.

٤-٢ وهناك ركيزة أخرى لاستراتيجية الإيكاو للأمن الإلكتروني، تتعلق بإدارة الحوادث وخطط الطوارئ، وهي بمثابة أساس لإعداد خطط الطوارئ المرتبطة بكل نظام حيوي يستخدم في مراقبة المجال الجوي البرازيلي. ويرد في الوثيقة وصف لجميع المعلومات الضرورية لتوجيه الإجراءات نحو إعادة إرساء الوظائف التي يوفرها كل نظام على مستويات مختلفة من مراقبة الحركة الجوية، فضلاً عن مختلف الجهات الفاعلة المشاركة في الاستجابات بالتنسيق المطلوب للتقليل إلى أدنى حد من عدم التوافر والأثر الذي يلحق بمستخدمي النقل الجوي.

٥-٢ يتم إعداد خطط الطوارئ بناءً على معايير دولية، مثل المعيار ISO/IEC 27031، ويتم تعديلها وفقاً لخصوصيات كل موقع. يتيح ذلك تجميع تفاصيل وظائف الأنظمة في كل موقع للحفاظ على هذه الوظائف حتى في حالة الهجمات الإلكترونية، مما يحافظ على تحسين البيئة والتحكم فيها.

٦-٢ ومن المهم التوضيح بأن إدارة مراقبة المجال الجوي تشارك أيضاً في تمرين الأمن الإلكتروني الوطني البرازيلي، تحت مسؤولية وزارة الدفاع، الذي يهدف إلى حماية الأنظمة الحيوية في البلاد. وفي هذا التمرين الوطني، تساهم إدارة مراقبة المجال الجويين مزودة الخبرة المكتسبة داخل وحداتها، في أمن النقل الجوي وتلقى المعلومات من مناطق أخرى لديها أيضاً أنظمة حيوية وتتطلب تدابير للحماية والتحصين. وتساعد الأنشطة التي وضعت في هذا التمرين الوطني الكبير على تأكيد وتحسين خطط الطوارئ، التي تحتاج إلى تحديث مستمر في مواجهة التهديدات الجديدة اليومية.

٧-٢ وتدعو البرازيل الدول الأعضاء في الإيكاو وصناعة الطيران إلى دعم وتنظيم تمارين الأمن الإلكتروني للجمع بين الخبراء الحكوميين والصناعيين من أجل تبادل أفضل الممارسات والمعارف لدى تدريب خبراء الإنترنت على التصدي للهجمات الإلكترونية وبناء خطط طوارئ إلكترونية أكثر موثوقية لحماية البنية التحتية والأنظمة الحيوية للطيران.

٣- الاستنتاج

٣-١ تشكل التهديدات الإلكترونية تحدياً دائماً، وقطاع الطيران المدني، بشبكته العالمية المعقدة، معرض للخطر أيضاً. ويتمشى موقف البرازيل الاستباقي، كما يتضح من مبادرات إدارة مراقبة المجال الجوي، مع استراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران، ولا سيما الركيزتان ٦ و٧. ومن شأن التركيز على خطط الطوارئ القوية، المستندة بالمعايير الدولية مثل المعيار ISO/IEC 27031، والمصممة وفق الخصوصيات المحلية، إلى جانب التمارين الإلكترونية المنتظمة والواقعية، أن يعزز بشكل كبير التحصين الإلكتروني. ولا تقتصر هذه الجهود على تدريب أفرقة الاستجابة للحوادث وتحديد نقاط الضعف فحسب، بل تعزز أيضاً ثقافة قوية للأمن الإلكتروني بين جميع المعنيين. ومن خلال تبادل الخبرات والتعاون في التمارين الوطنية والدولية، تؤكد البرازيل على الحاجة الماسة للتكيف المستمر والعمل الجماعي لحماية المنظومة العالمية للطيران من المخاطر الإلكترونية.

— انتهى —