AN-Conf/14-WP/136
30/6/24
Revision No. 1
30/7/24

منظمة الطيران المدني الدولي

ورقة عمل

المؤتمر الرابع عشر للملاحة الجوية

مونتريال، كندا، من ٢٠٢٤/٨/٢٦ إلى ٢٠٢٤/٩/٦

البند ٤ من جدول الأعمال: الترابط الفائق في شبكة الملاحة الجوية
٤-٢: الأمن الإلكتروني وقدرة نظام المعلومات على الصمود

تبادل المعلومات باستخدام منصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة ومساهمتها في تحسين الأمن الإلكتروني وتعزيز قدرة نظم المعلومات على الصمود في وجه التهديدات الإلكترونية

(مقدّمة من البرازيل، برعاية من ٢٠ دولة عضوا في لجنة الطيران المدني لأمريكا اللاتينية (LACAC)[١])

التنقيح الأول

الموجز التنفيذي

تسلّط ورقة العمل هذه الضوء على الجهود التي تبذلها البرازيل بشأن الأمن الإلكتروني في مجال الطيران فيما يتعلق بتبادل المعلومات المتعلقة بالأمن الإلكتروني من خلال منصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة، وذلك بما يتماشى مع مقترحات فريق خبراء الأمن الإلكتروني التابع للإيكاو. كما تشدد الورقة على أن هذا الحل لا يتطلب أي نفقات إضافية تتعلق بالأمن الإلكتروني، كما يعزز التعاون فيما بين الدول والمنظمات وقطاع الطيران من أجل تحسين السلامة الإلكترونية.

الإجراءات: يُرجى من المؤتمر القيام بما يلي:

أ) ملاحظة أن حالة استخدام الإدارة البرازيلية لمراقبة المجال الجوي لمنصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة بغرض تبادل معلومات المتعلقة بالأمن الإلكتروني كانت إيجابية حتى الآن؛

ب) تشجيع الدول الأعضاء على اعتماد منصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة لتبادل المعلومات المتعلقة بالأمن الإلكتروني؛

[١] الأرجنتين، أروبا (مملكة هولندا)، إكوادور، أوروغواي، باراغواي، بليز، بنما، بيرو، جامايكا، الجمهورية الدومينيكية، السلفادور، شيلي، غواتيمالا، فنزويلا (جمهورية فنزويلا البوليفارية)، كوبا، كوستاريكا، كولومبيا، المكسيك، نيكاراغوا، هندوراس.

ج) عرض موضوع هذه الورقة على فريق خبراء الأمن الإلكتروني التابع للإيكاو، وتشكيل مجموعة عمل لمعالجة مسألة توحيد عملية تبادل المعلومات المتعلقة بالأمن الإلكتروني والاستخدام المحتمل من قبل الدول الأعضاء لمنصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة.

١- المقدمة

١-١ من أجل التصدي لمشهد التهديدات العالمية التي لا تفتأ تتغير، تواصل الإيكاو تحسين قواعدها القياسية ونظمها بما يتماشى مع قرارات مجلس الأمن التابع للأمم المتحدة التي تشدد على التزام الدول بحماية الخدمات الجوية الواقعة في نطاق ولايتها. وتحث هذه القرارات جميع الدول على التعاون مع الإيكاو من أجل تقييم المعايير الأمنية الدولية وتحسينها وتنفيذها. وقد صيغت خطة عمل الأمن الإلكتروني بغرض تحقيق الأهداف المحددة في الركائز السبع لاستراتيجية الأمن الإلكتروني في مجال الطيران وإنشاء بيئة قوية للأمن الإلكتروني.

١-٢ وتشمل الواجبات الأساسية للإدارة البرازيلية لمراقبة المجال الجوي الإشراف على مراقبة المجال الجوي وحماية الطيران وتوفير خدمات البحث والإنقاذ، فضلا عن إدارة الاتصالات السلكية واللاسلكية المتعلقة بالطيران المدني البرازيلي، فضلا عن تقديم الدعم اللوجستي والحفاظ على أساسيات نظم الأمن الإلكتروني من أجل تنفيذ هذه المهام.

٢- المناقشة

٢-١ تبادل المعلومات المتعلقة بالأمن الإلكتروني

٢-١-١ لا تفتأ التهديدات العالمية تثير قلقا متزايدا. ومن أجل ضمان سلامة عمليات طيران واستمرارها، يجب حماية شبكة الملاحة الجوية والمراقبة الجوية في سياق عمليات تبادل المعلومات العالمية فيما بينها. ويكتسي تحديد هذه الأنظمة والإشراف عليها أهمية بالغة لمنع استغلال نقاط الضعف الذي يؤدي إلى تعطل الخدمة أو انقطاعها. وبالإضافة إلى ذلك، فإن ظهور أنظمة جديدة من الترابط الفائق لشبكة الملاحة الجوية سيمثل مشكلة كبيرة بحلول عام ٢٠٣٠. وفي هذا السياق، فإن معرفة التهديدات في الوقت المناسب تشكل عاملا أساسيا حتى تتمكن بنية الأمن الإلكتروني من توفير الحماية بشكل أكثر فعالية للأنظمة التي تقدم خدمات الطيران.

٢-١-٢ وبالتالي، فإن ممارسة تبادل معلومات المتعلقة بتهديد الأمن الإلكتروني تتماشى تماشيا تاما مع السياسة الوطنية البرازيلية للأمن الإلكتروني، التي أُنشئت بموجب المرسوم رقم ١١,٨٥٦ المؤرخ ٢٠٢٣/١٢/٢٦، والتي تحدد ما يلي واحدا من أهدافها:

— المادة ٣، الضميمة الحادية عشرة – "تنفيذ استراتيجيات التعاون لتطوير التعاون الدولي في مجال الأمن الإلكتروني".

٢-١-٣ وفي سياق الإيكاو، تحدد خطة عمل الأمن الإلكتروني، في إصدارها الثاني في يناير ٢٠٢٢، الملامح العامة لتبادل المعلومات المتعلقة بالأمن الإلكتروني، وتصف في فقرتها ٣-١-١ تبادل المعلومات على وجه التحديد كأحد ركائز استراتيجية الأمن الإلكتروني في مجال الطيران في إطار خطة عمل الأمن الإلكتروني.

٢-٢ منصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة.

٢-٢-١ تعد منصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة أداة هامة من أدوات الأمن الإلكتروني من أجل تبادل المعلومات المتعلقة بالتهديدات الإلكترونية. ويتزايد اعتماد هذه المنصة نظرا للفوائد العديدة التي تقدمها للمنظمات والمتخصصين في مجال الأمن الإلكتروني. وتشمل المزايا الرئيسية ما يلي:

أ) تسهل هذه المنصة التعاون بين المنظمات، مما يتيح المشاركة الآمنة للمعلومات المتعلقة بالتهديدات الإلكترونية. وذاك أمر بالغ الأهمية في مشهد لا تفتأ تتغير فيه التهديدات الإلكترونية. وتتيح القدرة على المشاركة في الوقت الفعلي للمؤشرات عن معلومات الاختراق والتهديد دفاعا أكثر قوة وفعالية؛

ب) ومن خلال مركزية المعلومات المتعلقة بالتهديدات ومشاركتها، تسمح هذه المنصة للمنظمات بالوصول في الوقت الفعلي إلى المعلومات المتعلقة بالتهديدات الإلكترونية، الأمر الذي من شأنه أن يعجل بالكشف عن الوقائع الأمنية والاستجابة لها، مما يحسن الوضع الأمني العام؛

ج) قابلية هذه المنصة بدرجة كبيرة للتعديل، مما يسمح للمنظمات بتكييفها وفقا لاحتياجاتها الخاصة. ويتضمن ذلك القدرة على إضافة سمات مخصصة وإنشاء نماذج تهديد محددة ودمج المنصة مع الأدوات الأمنية الأخرى؛

د) تربط هذه المنصة المستخدمين بأوساط الأمن الإلكتروني العالمية، مما يتيح تبادل المعلومات مع الغير من المنظمات والمهنيين، ويوسع نطاق القاعدة المعرفية المتاحة، ويعزز الدفاع ضد التهديدات الإلكترونية واسعة النطاق، ويعزز فهم التكتيكات (الأساليب) والتقنيات والإجراءات التي يتبعها الخصوم الإلكترونيون؛

هـ) وتتضمن المنصة ميزات متقدمة للتحكم في الوصول والخصوصية، مما يضمن قدرة المنظمات على مشاركة المعلومات بشكل انتقائي وآمن. وذاك أمر بالغ الأهمية لحماية البيانات الحساسة والامتثال لقواعد الخصوصية.

٢-٢-٢ وبشكل مجمل، تُعد منصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة أداة ضرورية لإدارة التهديدات الإلكترونية، حيث توفر منبرا فعالا لتبادل المعلومات المتعلقة بالأمن الإلكتروني. وباعتمادها يتعزز الدفاع التنظيمي والأمن الإلكتروني على المستويات الوطنية والإقليمية والعالمية.

٢-٣ استخدام الإدارة البرازيلية لمراقبة المجال الجوي لمنصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة.

٢-٣-١ بدأت الإدارة البرازيلية لمراقبة المجال الجوي في تنفيذ منصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة في عام ٢٠٢١، وهي تستخدم هذه الأداة وتعزز استخدامها منذ ذلك الحين. ويؤكد التحسين والصقل المستمرين لاستخدام هذه المنصة على التزام الإدارة بالتصدي للتحديات المتغيرة التي تواجه الأمن الإلكتروني.

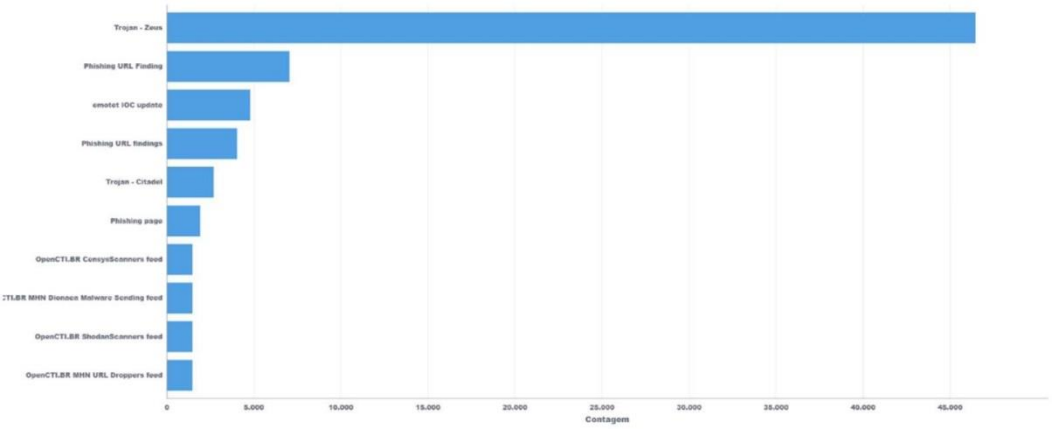
٢-٣-٢ ويجدر الإشارة إلى أن اعتماد هذه المنصة يمكن الإدارة البرازيلية لمراقبة المجال الجوي من التعاون بفعالية، بشأن تبادل المعلومات المتعلقة بالتهديدات الحرجة، مع أصحاب المصلحة البرازيليين الآخرين، بما في ذلك مركز القوات الجوية البرازيلية لمعالجة حوادث الشبكة ومؤسسة البترول البرازيلية والوكالة الوطنية للاتصالات السلكية واللاسلكية واتحاد البنوك البرازيلي.

وهذا التعاون لا يعزز آليات الدفاع الخاصة بالإدارة البرازيلية لمراقبة المجال الجوي فحسب، بل يساهم أيضا في الوضع الأمني العام للنظام البرازيلي لمراقبة المجال الجوي.

٢-٣-٣ وتجري معالجة المؤشرات والتنبيهات المتعلقة بالتهديدات، الواردة من الغير عبر هذه المنصة، كأساس لإعداد قوائم الحظر أو لصياغة قواعد جدار الحماية الإلكترونية (firewall). وتوفر هذه المؤشرات رؤى هامة حول التهديدات الأمنية المحتملة، مما يسمح للمؤسسات بحماية شبكاتها وأنظمتها بشكل استباقي من الأنشطة الضارة، والحفاظ على استباق التهديدات الناشئة وتعزيز وضع الأمن الإلكتروني لديها.

٢-٣-٤ وبمرور الوقت، يجري تحديد القواعد المرتبطة بالتهديدات في ضوء مستوى المخاطر المقترن بها. ويجري باستمرار تحديث مستوى المخاطر هذا لكل تهديد بناء على المؤشرات الواردة من خلال المنصة. ومن خلال التعديل الدينامي لمستوى المخاطر المرتبط بكل تهديد، يمكن للمنظمات ضمان بقاء قواعد جدار الحماية الإلكترونية الخاصة بها فعالة وسريعة الاستجابة لضمان بيئة إلكترونية أكثر أمانا. ويسمح هذا النهج باستخدام استراتيجيات أكثر دقة وقابلية للتكييف من أجل التخفيف من حدة التهديدات، مما يعزز مرونة الأمن الإلكتروني بشكل عام.

٢-٣-٥ وعلى سبيل المثال، يوضح الشكل رقم ١ بعضا من أهم عشرة أنواع من التهديدات من بين أكثر التهديدات التي تلقتها الإدارة البرازيلية لمراقبة المجال الجوي عبر المنصة خلال العام الماضي، ومنها طروادة زيوس (Trojan Zeus)، والعثور على عنوان URL من أجل التصيد الاحتيالي، وتحديث emotet IOC، وقلعة طروادة (Trojan Citadel)، وصفحات التصيد الاحتيالي.



الشكل ١ – أهم عشرة أنواع من التهديدات التي تلقتها الإدارة البرازيلية لمراقبة المجال الجوي

٢-٣-٦ بينما يعرض الشكل رقم ٢ الكمية اليومية لكتل البرامج الخبيثة من المؤشرات التي تتلقاها منصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة على مدار أسبوع واحد. ومن الشكل البياني الموضح، يمكن ملاحظة أن هذه المنصة تساهم فيما يقرب من ٤٠ ٠٠٠ ٠٠٠ عملية حظر للبرامج الخبيثة سنويا.

الشكل ٢ – البرامجيات الخبيثة التي تمكنت مؤشرات منصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة من حظرها

٢-٣-٧ واليوم، تساعد منصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة على الإخطار عن و/أو تلقي أي حدث ضار مؤكد أو مشتبه به يتعلق بأمن أنظمة الحاسوب أو شبكات الحاسوب، وذلك من أجل المساهمة في أمن المعلومات في النظام البرازيلي لمراقبة المجال الجوي.

٣- الاستنتاجات

٣-١ وفي الختام، فإن استخدام الإدارة البرازيلية لمراقبة المجال الجوي لمنصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة يعزز بشكل كبير من الأمن الإلكتروني للطيران في البرازيل. ويتماشى ذلك النهج الاستباقي مع المعايير الدولية مثل خطة عمل الإيكاو للأمن الإلكتروني. كما تدعم الإدارة البرازيلية لمراقبة المجال الجوي الوكالة الوطنية للطيران المدني في البرازيل بشأن استخدام منصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة من أجل تحسين تبادل المعلومات المتعلقة بالتهديد الإلكتروني للطيران المدني البرازيلي، والاستفادة من قدرات هذه المنصة لتبادل المعلومات في الوقت الفعلي والالتزام بالمعايير المفتوحة.

٣-٢ وتؤكد البرازيل من جديد التزامها بالمساهمة في أمن الطيران الدولي، ولا سيما في مجال الأمن الإلكتروني، متبعة نهجها التعاوني الذي يعزز سلامة الطيران العالمية. ونظرا لأن الترابط الفائق يزيد من مساحة تعرض شبكة الملاحة الجوية للهجمات الإلكترونية، فإن البرازيل مكرسة لتبني أفضل الاستراتيجيات والتقنيات لحماية بنيتها التحتية الحيوية للطيران من التهديدات الإلكترونية المتطورة.

٣-٣ وتعتزم البرازيل تشجيع استخدام منصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة فيما بين أعضاء إقليم الكاريبي وأمريكا الجنوبية لاستكشاف مبادرة تبادل المعلومات المتعلقة بالتهديدات الإلكترونية والمشاركة فيها بنشاط، وبالتالي تعزيز استخدام المنصة كمنبر قوي للتعاون. والهدف من ذلك هو تعزيز القدرة على الصمود في وجه التهديدات الإلكترونية في مجال الطيران على المستوى الإقليمي بحيث يكون هناك تكامل عالمي في المستقبل بما يتماشى مع توصيات الإيكاو.

٣-٤ وفي ضوء ما تقدّم، يُرجى من المؤتمر الموافقة على التوصية التالية:

التوصية ٤-٢/x – الأمن الإلكتروني وقدرة نظام المعلومات على الصمود في وجه التهديدات الإلكترونية

أ) ملاحظة أن حالة استخدام الإدارة البرازيلية لمراقبة المجال الجوي لمنصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة بغرض تبادل معلومات المتعلقة بالأمن الإلكتروني كانت إيجابية حتى الآن؛

ب) تشجيع الدول الأعضاء على اعتماد منصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة لتبادل المعلومات المتعلقة بالأمن الإلكتروني؛

ج) عرض موضوع هذه الورقة على فريق خبراء الأمن الإلكتروني التابع للإيكاو، وتشكيل مجموعة عمل لمعالجة مسألة توحيد عملية تبادل المعلومات المتعلقة بالأمن الإلكتروني والاستخدام المحتمل من قبل الدول الأعضاء لمنصة تبادل المعلومات المتعلقة بالبرامجيات الخبيثة.

— انتهى —