A41-WP/241
EX/108
2/8/22

منظمة الطيران المدني الدولي

ورقة عمل

الجمعية العمومية – الدورة الحادية والأربعون

اللجنة التنفيذية

البند رقم ١٤: أمن الطيران–السياسة العامة

تأمين الطيران من خلال نهج الثقة الصفرية

(ورقة مقدَّمة من جنوب أفريقيا)

الموجز التنفيذي

قد يعتمد قطاع الطيران أحيانا على سلاسل توريد موسَّعة تمتد عبر قطاعات متعددة، وبالتالي تتسع رقعة التهديدات التي تتربص بالطيران. كما إن اعتماد نُظُم قائمة على بروتوكول الإنترنت (IP) لتحسين الكفاءة يتطلب بدوره اعتماد نُهُج استباقية ضرورية من أجل حماية النظم الحالية والقديمة.

تبرز "خطة عمل الإيكاو في مجال الأمن الإلكتروني" الحاجة إلى تركيز الموارد والإجراءات على التوصل إلى نهج منتظم يسمح بإدارة الأمن الإلكتروني في مجال الطيران؛ وذلك بهدف إعداد نهج من النظم يتيح للطيران التكيف مع التهديدات الجديدة في الوقت المناسب والصمود في وجهها.

تسعى ورقة العمل هذه إلى طرح مفهوم "الثقة الصفرية"، الذي يمكن للدول والجهات المعنية في قطاع الطيران أن تعتمده كأحد مبادئ التخفيف من حدة التهديدات. فإدراج مفهوم الثقة الصفرية سوف يساعد في تدعيم قدرات حماية الأمن الإلكتروني الحالية عن طريق تطبيق نُظم حماية شاملة. ومن شأن هذا المفهوم أن ينتقل بالأمن من الفكرة التقليدية القائمة على تأمين المحيط الخارجي للشبكة، وذلك من خلال وضع أدوات لتأمين بيانات المساعد الملاحي الأرضي عند عُقد الشبكات أو بالقرب من منشآت مراقبة الحركة لدى المستخدم النهائي (رادار الإمداد).

الإجراء: الجمعية العمومية مدعوة إلى القيام بالإجراءات التالية:

أ) الإقرار بفائدة تطبيق نُهُج تتسم بالسرعة والقدرة على التأقلم وهي نُهُج عمليات التقييم المستمرة والقابلة للتعديل للمخاطر والثقة (CARTA) في حماية عمليات الطيران؛

ب) الطلب إلى الإيكاو من خلال فريق خبراء أمن الطيران إعداد مواد إرشادية فنية كفيلة بدعم الدول في إدراج إطار "الثقة الصفرية" في نُظُم إدارة أمن المعلومات (ISMS) لديها؛

ج) حث الدول على النظر في إدراج مبادئ الثقة الصفرية في نُظُم إدارة أمن المعلومات لديها.

الأهداف الاستراتيجية:	ترتبط ورقة العمل هذه بالهدف الاستراتيجي: "الأمن والتسهيلات"
الآثار المالية:	لن تترتب تبعات إضافية على الميزانية، حيث سيتم ذلك في حدود الميزانية التي رصدتها الإيكاو.
المراجع:	"خطة عمل الأمن الإلكتروني" "دليل أمن الطيران" (Doc 8973)

١- المقدمة

١-١ شهد قطاع الطيران خلال السنوات الأخيرة تحوّلاً غذّته التطورات التكنولوجية، مما أدى إلى زيادة المخاطر الإلكترونية التي تستلزم مزيداً من التركيز. وفي ظل القفزات العملاقة الغير مسبوقة التي تحققت في مجال التطور التكنولوجي، تحتم الاستمرار في اعتماد نُهُج ونماذج عمليات التقييم المستمرة والقابلة للتعديل للمخاطر والثقة (CARTA).

١-٢ في الماضي، كان يُنظر إلى قطاع الطيران بمعزل عن القطاعات الأخرى، لكن الاعتماد المتبادل والتقارب بين تكنولوجيا المعلومات/التكنولوجيا التشغيلية في منظومة الطيران أدّيا إلى دخول جهات معنية مختلفة لا تحكمها آليات الامتثال لقواعد الطيران، الأمر الذي وسّع من رقعة الهجمات الإلكترونية المحتملة، وبالتالي استلزم تنقيح بعض المفاهيم التقليدية.

١-٣ وفي السابق، كان يمكن إدارة معدات وبرمجيات الطيران وصيانتها من خلال شبكة افتراضية خاصة (VPN) مأمونة وموثوقة بها يمكن الدخول إليها عن بُعد، والتي أدت في عالمنا اليوم إلى اختراق أمن النُظم عبر هذه الاتصالات.

١-٤ وتفشت التهديدات الإلكترونية مثل فيروسات الفدية وسرقة البيانات وهجمات الانتحال في قطاع الطيران، وبذلك خلّفت أثراً على تكنولوجيا المعلومات (الوصول إلى خطط موارد المؤسسات والخدمات التعاونية وخدمات البريد الإلكتروني)، وبيئات التكنولوجيا التشغيلية (نظم "SCADA" و"PLC") التي تستهدف مناطق المراقبة في المطارات ومراكز البيانات وما حولها.

٢- المناقشة

٢-١ يمكن لسلاسل التوريد الموسعة في الطيران أن تطرح مخاطر إلكترونية، وبالتالي، تزيد الحاجة إلى اتباع نُهُج مبتكرة وجديدة لمعالجة هذه المخاطر على النحو اللازم. ويرجع ذلك إلى أنّ الطيران يعتمد على عدة جهات معنية لديها نُظُم وتطبيقات وتكنولوجيات مختلفة يجب أن تندمج مع بعضها البعض.

٢-٢ والجدير بالذكر أنّ إتاحة هذه العمليات قد يستلزم دعماً عن بُعد من جهات مقرها داخل حدود الدولة أو خارجها، الأمر الذي يعرض سلسلة القيمة الخاصة بالنقل الجوي لمزيد من التهديدات الإلكترونية.

٢-٣ أما الأساليب القديمة للأمن القائمة على تأمين المحيط الخارجي للشبكة والتي كانت تُستخدم لمعالجة الأمن المطلوب فقد أثبتت أنها غير فعالة، ويتضح ذلك جلياً من ازدياد الأحداث الإلكترونية في مجال الطيران. فما إن ينجح المهاجمون في اختراق محيط الشبكة، ليس هناك ما يمنعهم من القيام بمزيد من التحركات الأفقية.

٢-٤ بإمكان مفاهيم مثل "الثقة الصفرية" أن تتصدى للجيل القادم من التهديدات، إلى جانب التهديدات المتقدمة السائدة في وقتنا الحالي، مما يسمح لأي طلب للموارد أن تنشأ عنه عملية تقييم للوضع الأمني والتحقق من الوضع الأمني ومنح الموارد إمكانية الوصول إلى الشبكات وذلك في إطار ضوابط أمنية مدروسة وفعالة.

٢-٥ يوفر نهج "الثقة الصفرية" مجموعة من المبادئ التوجيهية لسير العمل وتصميم النُظُم والعمليات التي يمكن استخدامها بغية تحسين الوضع الأمني للأنشطة الحرجة والحساسة، وذلك بهدف منع اختراق البيانات والحد من التحركات الأفقية الداخلية.

٢-٦ يفترض مفهوم "الثقة الصفرية" أنه لا يمكن الوثوق بأي أحد سواء داخل أو خارج المنظمة. ويسعى هذا النهج إلى التقليل من مسطح الهجوم استناداً إلى الأفكار التالية:

أ) ليس هناك محيط خارجي للشبكة: من خلال التخلص من افتراض إمكانية الوثوق بالأشخاص لمجرد أنهم دخلوا إلى شبكة شركة ما؛

ب) ضمان التحقق من المستخدمين قبل منحهم إمكانية الوصول، والتحقق من سلامة الأجهزة المستخدمة قبل توصيلها بالشبكة؛

ج) التخلص من افتراض أنّ المستخدمين سيقومون بالتصرف الصحيح. وعوضاً عن ذلك، التحقق من حقوق الوصول المُعتمدة لكل طلب للحصول على خدمة؛

د) عوضاً عن ملاحقة المخالفين، وضع معوقات تبطئ من أدائهم.

٢-٧ يساعد إدراج نهج "الثقة الصفرية" في إمكانية تدعيم قدرات حماية الأمن الإلكتروني الحالية عن طريق تطبيق نُظُم حماية شاملة. ومن شأن هذا النهج أن ينتقل بالأمن من الفكرة التقليدية القائمة على تأمين المحيط الخارجي للشبكة، وذلك من خلال وضع أدوات لتأمين بيانات المساعد الملاحي الأرضي عند عُقد الشبكات أو بالقرب من منشآت مراقبة الحركة لدى المستخدم النهائي (رادار الإمداد).

٢-٨ هناك مختلف التكنولوجيات التي تدعم تنفيذ نهج "الثقة الصفرية" والتي يمكن الارتكاز عليها لتقديم الحماية على عدة جبهات:

أ) التقسيم الدقيق، وهو أحد أول مفاهيم "الثقة الصفرية"، المصمم أساساً للحماية من التحركات الأفقية بهدف التخفيف من أثر أي اختراق يقع. فالتحركات الأفقية داخل مراكز البيانات للحصول على معلومات من الأصول الرئيسية يشكل عنصراً رئيسياً في العديد من الهجمات. ويسعى هذا النهج إلى الحد من الاتصالات غير المصرح بها بين العمليات ما لم يكن هناك دواعٍ تشغيلية للقيام بذلك، وبذلك يتسنى

التقليل من أثر الاختراق. خلافاً للحماية الرأسية (شمال–جنوب) التقليدية التي تؤمنها الجدران النارية، تهتم تقنية التقسيم الدقيق بالأمن الأفقي (شرق–غرب) للعمليات؛

ب) تنشأ عن الدخول عبر شبكات "الثقة الصفرية" حدود منطقية للوصول إلى التطبيقات تستند إلى السياق. والهدف من ذلك هو التقليل من الوصول وإساءة استخدام الوصول إلى التطبيقات الموجَّهة بحسب سياق المستخدم والجهاز، مما يخالف افتراض أنّ موقع كيان ما (أي مثلاً داخل الشبكة) يعني الوثوق به تلقائياً؛

ج) تقوم تقنية "الثقة الصفرية" بحجب كافة التطبيقات على الشبكة، وتسمح بإمكانية الوصول إليها بناء على عوامل مثل هوية المستخِدم والجهاز المستخدم والموقع الجغرافي والوضع الأمني، مما يعني أنّ المستخدمين يُمنحون إمكانية الوصول إلى التطبيقات التي يحتاجونها فقط، ولكن لا يمكنهم أي شيء آخر على الشبكة؛

د) تعمل تقنية عزل المتصفح المشغل عن بُعد على أساس مبدأ أنّ المستخدمين النهائيين يشكلون الحلقة الأضعف في أي منظمة، ويظل الوصول إلى شبكة الإنترنت إحدى أكبر رقعات الهجمات التي تنطلق منها عمليات الاختراق. فبالتالي، فإحدى أكثر الطرق فعاليةً في التخفيف من حدة الاختراق عبر النقطة النهائية/المستخدم النهائي هي عزل الوصول الشبكي من أجل التخلص من عمليات الاستغلال والتهديدات عبر المتصفح مثل فيروسات الفدية والبرمجيات الخبيثة المخبأة وهجمات الانتحال.

٣- الخلاصة

٣-١ يمكن استخدام مبادئ "الثقة الصفرية" من أجل ضمان أنّ يكون الطيران المدني قادراً على تقوية نفسه بنفسه من خلال اعتماد نهج "الأمن المدمج". فضمان أمن العناصر والعمليات الحرجة حتماً يغير مفهوم الأمن من أمن تفاعلي (يستجيب عند الهجوم) إلى أمن استباقي، كما يعزز من تطوير منظومة طيران مدني قادرة على التقوية الذاتية، مما يتيح للطيران التطور ويسمح بتحسين قدرته على الصمود بصورة آلية، حيث أثبتت هذه النُهُج فعاليتها.

— انتهى —