AN-Conf/14-WP/113[1]
28/6/24

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

الأمن الإلكتروني – إدارة المخاطر وجرد أصول المعلومات الإلكترونية في خدمات الملاحة الجوية

(مقدّمة من شيلي وشاركت في رعايتها ٢٠ دولة من الدول الأعضاء في لجنة الطيران المدني لأمريكا اللاتينية)[2]

[1] قدمت شيلي هذه الورقة باللغة الإسبانية.

[2] الأرجنتين وأروبا وبليز والبرازيل وكولومبيا وكوستاريكا وكوبا والجمهورية الدومينيكية وإكوادور والسلفادور وغواتيمالا وهندوراس وجامايكا والمكسيك ونيكاراغوا وبنما وباراغواي وبيرو وأوروغواي وفنزويلا (جمهورية – البوليفارية).

الموجز التنفيذي

تعرِض ورقة العمل هذه المبادئ التوجيهية العامة للأمن الإلكتروني التي يجب أن تراعى في خدمات الملاحة الجوية من أجل التصدي للتهديدات الحالية للنظم التكنولوجية المستخدمة في هذا المجال، إذ إن التبادل المستمر للمعلومات يجعل هذه النظم أهدافاً محتملة للهجوم الإلكتروني.

وتنجم هذه الظروف عن الهيكل الوظيفي لنظام الطيران، بما في ذلك سلطات الطيران المدني ومقدمو خدمات الملاحة الجوية ومشغلو المطارات وأي منظمات أخرى معنية.

الإجراءات: يُرجى من المؤتمر القيام بما يلي:

أ) تعزيز السعي إلى وضع خطة لإدارة المخاطر في نظام خدمات الملاحة الجوية تتيح تحديد أي تهديدات للأمن الإلكتروني والتخفيف منها أثناء تصميم الشبكات والنظم المطلوبة وتركيبها وتشغيلها؛

ب) تعزيز السمات التي تيسر إدارة المخاطر، مثل تطبيق سجل واحد متكامل لكل أصل من الأصول الإلكترونية المحددة في خدمات الملاحة الجوية، والتي تمكّن من الوقوف على التهديدات، مع تحديد مستويات الأولوية للعمل والصيانة والتعافي السريع للنظم، إذا اقتضى الأمر ذلك؛

ج) تجديد الالتزام بالتحسين المستمر لمختلف العمليات، بما في ذلك العمليات المصنفة على أنها حرجة، من أجل تحقيق مستويات الأمن الإلكتروني المثلى في خدمات الملاحة الجوية.

١- المقدمة

١-١ يؤدي التغيير التكنولوجي الذي يجري تنفيذه داخل مختلف المنظمات في كل أوساط المجتمع إلى زيادة تعرض هذه المنظمات للجنوح الإلكتروني. كما أن تقديم خدمات الملاحة الجوية ليس بمنأى عن هذه المشكلة، ولذا فإن هناك ما يدفع بزخم إلى وضع استراتيجيات وإقامة حواجز للحماية من هذا التهديد الكامن والمتنامي، الذي يمكن أن يؤثر في تحقيق المستويات المثلى للأمن التشغيلي.

١-٢ وتستلزم الحاجة إلى وضع أساليب لإدارة المخاطر بغية الوقوف على أي تهديد للأمن الإلكتروني والتخفيف من آثاره على نظام خدمات الملاحة الجوية التزاماً متجدداً بضمان التحسينات المستمرة لمختلف العمليات، بما في ذلك العمليات التي تصنفها المنظمة على أنها حرجة.

١-٣ وينبغي أن تراعي سياسة الأمن الإلكتروني التي تضعها خدمات الملاحة الجوية كامل دورة حياة نظام الطيران، وأن تشمل عناصر مثل ثقافة الأمن الإلكتروني، وتعزيز الأمن من خلال التصميم، وأمن سلسلة الإمدادات لبرامج ومعدات تكنولوجيا المعلومات، وسلامة البيانات، ومراقبة الدخول المناسبة، والإدارة الاستباقية للثغرات الأمنية، وتحسين مواعيد تحديث النظم، وإدماج نظم وعمليات رصد البيانات.

٢- المناقشة

٢-١ يفترض الهدف المتمثل في تحقيق نظام ملاحة قابل للتشغيل البيني عالمياً وجود شبكات وبنى أساسية مشتركة لتكنولوجيا المعلومات وهياكل وعمليات تتمحور حول الشبكات. ولن يقتصر تبادل المعلومات في المستقبل على الاتصالات من نقطة إلى نقطة، بل سيستخدم أيضاً بنية النظم المفتوحة وتدفق المعلومات القائم على الإنترنت. وكل هذا يزيد من تعرض النظم للهجوم الإلكتروني.

٢-٢ ويجب أن يراعي تطبيق الأمن الإلكتروني في خدمات الملاحة الجوية حماية الشبكات والنظم وقدرتها على الصمود واستمراريتها التشغيلية وسريتها وسلامتها وتوافر المعلومات فيها. ويتطلب توافر المعلومات تحليل الآثار التشغيلية ودورة حياة النظم.

٢-٣ يُعرّف الحادث الإلكتروني بأنه أي حدث يضر بتوافر أو موثوقية أو سلامة أو سرية النظم أو البيانات المخزنة أو المنقولة أو المعالجة أو الخدمات المناظرة التي تقدمها نظم المعلومات وبنيتها الأساسية، مما قد يؤثر في تشغيلها العادي.

٢-٤ وتتعرض نظم الأمن الإلكتروني لمجموعة من التهديدات الإلكترونية مثل فيض المعلومات، والاعتراض السلبي للمعلومات، والاعتراض النشط للمعلومات، وتعديل ترتيبات النظم أو بياناتها، وتدمير ترتيبات النظم، وهجمات انقطاع الخدمة أو هجمات الحرمان من الخدمة، وغير ذلك من الأمور.

٢-٥ وينبغي لمقدمي خدمات الملاحة الجوية تحديد الدعائم المنطقية والمادية لنظم المعلومات الحرجة المستخدمة في عملياتهم والنظر في درجة تأثرها في حال تعرضها للتلف أو الانقطاع.

٢-٦ وينبغي تنفيذ تدابير لحماية نظم المعلومات الحرجة في أقرب وقت ممكن خلال مرحلة التصميم لضمان قدرتها على الصمود أمام الهجمات الإلكترونية قدر الإمكان.

٢-٧ وينبغي لتدابير أمن البنية الأساسية أن تراعي الأمن من خلال التصميم، وفصل الشبكة والوصول إليها عن بعد.

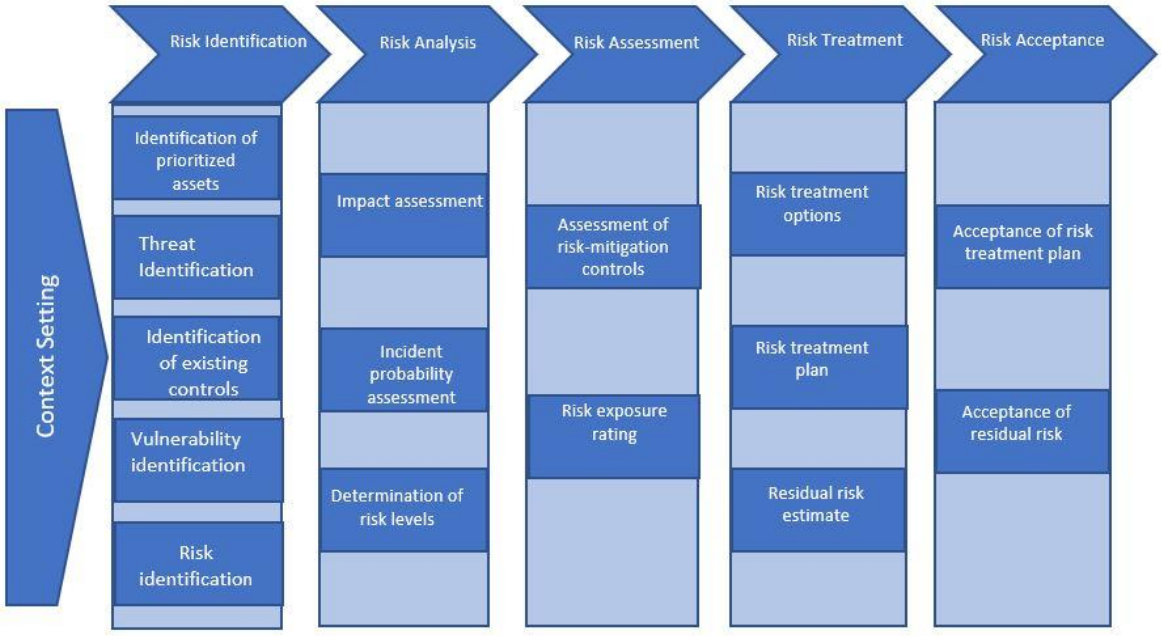
٢-٨ وينبغي للتدابير الأمنية في سلسلة الإمداد الخاصة بالدعائم المادية والمنطقية أن تراعي التحديث الدوري المطلوب لنظم تكنولوجيا المعلومات والاتصالات الخاصة بالطيران بسبب التغييرات في المتطلبات التشغيلية وتحديث الدعائم المنطقية.

٢-٩ ويتطلب تنفيذ خطة إدارة المخاطر الخاصة بخدمات الملاحة الجوية، في الحد الأدنى، الوقوف على الأصول الإلكترونية لإدارة الحركة الجوية وتحديد مستويات تصنيف الحوادث والأخطار والآثار على النظم.

	DESCRIPTION OF PROCESSES							
Strategic product	Process	Sub-process	Asset name	Identifier or Code	Type	Location	Person responsible / Owner	Support

				CRITICALITY ANALYSIS			
Storage medium	Retention time	Disposal	Search criterion	Confidentiality	Integrity	Availability	Criticality

الشكل ١- جدول تحديد وجرد الأصول الإلكترونية لإدارة الحركة الجوية



الشكل ٢– مخطط إدارة المخاطر

		Susceptibility						Risk																		
								Probability of occurrence									Impact									
								Threat agent factors				Vulnerability factors					Technical factors					Business fac				
ASSET ID	Vulnerability	Identity fraud (Authenticity)	Manipulation (Integrity)	Rejection (No Rejection)	Information disclosure (Confidentiality)	Denial of service (Availability)	Privilege escalation (Authorization)	Skill level	Motivation	Opportunity	Size	Ease of discovery	Ease of exploitation	Awareness	Intrusion detection	**Total probability of occurrence**	Loss of confidentiality	Loss of integrity	Loss of availability	Loss of responsibility	Overall technical impact	Financial loss	Reputational damage	Non-compliance	
ASST 17	Description of vulnerability	S	T	R	I		E	9	4	4	3	4	3	3	4	**4.25**	2	2	2	2	**2**	6	3	3	
ASST 17		S	T		I	D	E	4	4	7	4	4	4	7	4	**4.75**	4	4	3	3	**3.5**	3	4	4	
ASST 17		S	T	R	I	D	E	4	4	7	9	9	9	9	3	**6.75**	7	7	0	0	**3.5**	0	0	0	
ASST 16 & 17		S	T	R	I	D	E	4	4	7	9	9	9	9	3	**6.75**	2	2	2	2	**2**	2	2	2	
ASST 17		S	T		I	D	E	0	0	0	0	0	0	0	0	**0**	0	0	0	0	**0**	0	0	0	
ASST 16 & 17		S	T		I	D	E	0	0	0	0	0	0	0	0	**0**	0	0	0	0	**0**	0	0	0	

الشكل ٣– جدول تحليل المخاطر والثغرة الأمنية للأصول المحددة

٢–١٠ ينبغي أن تتيح صياغة خطة إدارة المخاطر إمكانية توقع العواقب الناشئة عن التهديدات مثل الهجمات الإلكترونية والوقائع الإلكترونية غير العدائية بناءً على تحليل وتقييم المخاطر التي تتعرض لها الشبكات والنظم، وذلك لتجنب هذه الوقائع أو تقليل عددها. ويمكن التخفيف من الآثار المحتملة من خلال تحديد الإجراءات الفورية وتدابير التحسين التدريجي مع المؤشرات والضوابط والتوثيق الخاصة بكل منها.

٢–١١ وأحد العناصر التي ينبغي النظر فيها لتسهيل إدارة المخاطر هو وضع سجل واحد لكل أصل جرى تحديده من الأصول الإلكترونية لإدارة الحركة الجوية. وسيتيح هذا الأمر القيام بما يلي:

أ) تجميع الأصول الإلكترونية التي تتماثل في النوع و/أو في دورة الحياة؛

ب) ضمان سلامة البيانات؛

ج) تعزيز نجاح إجراءات الحفاظ على قدرة النظم على الصمود؛

د) منع ازدواجية العناصر أو تقادمها؛

هـ) تقليل الجهد المطلوب للتحليل واتخاذ القرارات.

٣- الاستنتاجات

٣-١ إن الحاجة إلى تنفيذ استراتيجيات الأمن الإلكتروني لمواجهة التهديدات الرقمية التي يتعرض لها توفير خدمات الملاحة الجوية تتطلب من مقدمي هذه الخدمات وضع خطط وبروتوكولات عمل من أجل حماية النظم والبنية الأساسية المرتبطة بها، وضمان تمتُّعها بما يكفي من القدرة على الصمود للحفاظ على سرية المعلومات وسلامتها وتوافرها.

٣-٢ وبناءً على ما تقدم، وفي سياق خطة عمل الإيكاو للأمن الإلكتروني، يرجى من المؤتمر الموافقة على:

أنه ينبغي لمقدمي خدمات الملاحة الجوية الاضطلاع بما يلي:

أ) وضع خطة لإدارة مخاطر التهديدات الإلكترونية، على أن يراعى في الحد الأدنى تحديد الأصول الإلكترونية لإدارة الحركة الجوية، وتصنيف الوقائع، وتصنيف مستويات الخطر، ودرجة التأثير في النظم، وبروتوكولات تعافي النظم؛

ب) النظر في العوامل الميسِّرة ضمن إطار إدارة المخاطر، مثل تصميم سجل واحد لكل أصل إلكتروني قابل للتشغيل البيني من أصول إدارة الحركة الجوية؛

ج) تجديد الالتزام بالتحسين المستمر لمختلف العمليات، بما في ذلك العمليات المصنفة على أنها حرجة، من أجل تحقيق مستويات الأمن الإلكتروني المثلى في خدمات الملاحة الجوية.

— انتهى —