منظمة الطيران المدني الدولي

ورقة عمل

A41-WP/231[1]
EX/104
2/8/22

الجمعية العمومية – الدورة الحادية والأربعون

اللجنة التنفيذية

البند رقم ١٤ من جدول الأعمال: أمن الطيران – السياسة العامة

استراتيجية ثقافة الأمن السيبراني

(ورقة مقدَّمة من المملكة العربية السعودية نيابة عن دول المنظمة العربية للطيران المدني (أكاو) [٢])

الموجز التنفيذي

تزداد الهجمات السيبرانية بشكل مستمر في قطاع الطيران المدني ويؤثر هذا الهجوم المتزايد على المطارات، وشركات الطيران، والحركة الجوية، وحتى الركاب. إن الطريقة المثلى لتقليل المخاطر السيبرانية تكون عن طريق تطوير استراتيجية ثقافة الأمن السيبراني وذلك لتعزيز قدرات الموظفين، ودعم أهداف الأمن السيبراني، وحماية المنظمة من التهديدات السيبرانية الداخلية والخارجية. تشكل ثقافة "الأمن السيبراني" دوراً رئيسياً في تطبيق متطلبات الأمن السيبراني وتعزيز التعاون على مستوى المنظمة وكذلك على المستوى الوطني والدولي. تستهدف استراتيجية ثقافة الأمن السيبراني جميع موظفي المنظمة والغرض منها هو بناء ثقافة الأمن السيبراني واستمرارها لدعم الأفراد، والتقنيات، وعمليات الأمن السيبراني.

الإجراء: يرجى من الجمعية العمومية القيام بما يلي:

أ) حث الدول الأعضاء لتبني أهمية ثقافة الأمن السيبراني في مجال الطيران المدني في ظل تزايد الهجمات السيبرانية على مستوى العالم بشكل كبير؛

ب) دعوة الأمانة العامة لتبني توصية إنشاء برنامج توعية بالأمن السيبراني خاص بالعاملين في مجال الطيران المدني مماثل لبرنامج ثقافة أمن الطيران.

الأهداف الاستراتيجية:	ترتبط ورقة العمل هذه بالهدف الإستراتيجي "الأمن والتسهيلات".
الآثار المالية:	
المراجع:	

[١] قدَّمت المملكة العربية السعودية هذه الورقة باللغة العربية.

[٢] الدول الأعضاء في المنظمة العربية للطيران المدني (أكاو): الجزائر والبحرين وجزر القُمر وجيبوتي ومصر والعراق والأردن والكويت ولبنان وليبيا وموريتانيا والمغرب وعُمان وفلسطين وقطر والمملكة العربية السعودية والصومال والسودان والجمهورية العربية السورية وتونس والإمارات العربية المتحدة واليمن.

١- المقدمة

١-١ تعتبر الأخطاء البشرية السبب الرئيسي في انتهاكات واختراقات الأمن السيبراني في عام ٢٠٢١، مما يشير إلى أن الموظف هو الحلقة الأضعف في سلسلة الأمن السيبراني. بالإضافة إلى ذلك، فإن مجرمي الإنترنت قاموا بتطوير أساليب هجومية تستهدف مستخدمي الأنظمة لاستغلال نقاط ضعفهم. لذلك تحتاج المنظمات إلى بناء ثقافة الأمن السيبراني للتأكد من أن القوى العاملة لديها تتبنى السلوكيات الصحيحة للتعامل مع مجموعة مختلفة من التهديدات السيبرانية الموجَّهة إليهم أو لأدوارهم داخل المنظمة ليصبحوا خط الدفاع الأول للمنظمة.

١-٢ يرتكز الأمن السيبراني على ثلاث ركائز أساسية وهي الأشخاص، والعمليات، والتكنولوجيا. تعتمد هذه الركائز بشكل كبير على ثقافة الأمن السيبراني حيث إن التكنولوجيا بدون موظفين مدربين ستخلق نقاط ضعف، ولا جدوى من العمليات في حالة عدم اتباعها من قبل الأفراد بشكل صحيح.

١-٣ لا تقتصر الأخطاء البشرية على المستخدم العادي الذي يقوم بالنقر على روابط مشبوهة أو تحميل برامج ضارة، بل إن الأثر الأكبر يحدث عندما يخطئ مهندس غير مؤهل في تهيئة وإعداد نظام مهم أو أن يقوم بتطبيق بعض التغييرات دون اتباع إجراءات إدارة التغيير؛ مما يعرض البنية التحتية التقنية بأكملها للتهديدات السيبرانية الخارجية.

١-٤ يجب أن يكون جميع الموظفين على دراية بأدوارهم ومسؤولياتهم في تطبيق برنامج الأمن السيبراني وفهم التزاماتهم تجاه سياسة الأمن السيبراني والقانون الجنائي السيبراني الوطني إن وجد.

١-٥ يشكل مجلس الإدارة والإدارة العليا دوراً هاماً في دعم متطلبات الأمن السيبراني ومعالجة المخاطر السيبرانية. لذلك يجب أن يكونوا على دراية بأهمية الأمن السيبراني وأن يتعاملوا مع المخاطر السيبرانية على أنها مخاطر تهدد المنظمة.

٢- ثقافة الأمن السيبراني

٢-١ تعزز ثقافة الأمن السيبراني مشاركة المعلومات بين الدول الاعضاء وذلك لاكتشاف ومعالجة الثغرات والتهديدات السيبرانية الأمنية بشكل استباقي.

٢-٢ تعتبر التوعية بالأمن السيبراني والتدريب بداية التغيير. لذلك ينبغي على المنظمات أن تذهب إلى ما بعد ذلك وتبدأ في تغيير السلوك من خلال استراتيجية ثقافة الأمن السيبراني.

٢-٣ تتكون استراتيجية ثقافة الأمن السيبراني من الخطوات الثلاثة التالية:

أ) **تحديد الأهداف الاستراتيجية:** تحديد أهداف ثقافة الأمن السيبراني تمثل الخطوة الأولى. ويمكن أن تشمل هذه الأهداف على سبيل المثال لا الحصر، ضمان فهم القوى العاملة لمخاطر الأمن السيبراني التي تستهدف المنظمة، وفهم الأدوار والمسؤوليات المتعلقة بوظائفهم، وتطوير الكفاءة المعرفية والقدرات في مجال الأمن السيبراني.

ب) **تقييم الوضع الراهن:** والغرض من ذلك هو تقييم الثقافة على المستوى التنظيمي والمستوى الفردي. حيث يقيس المستوى التنظيمي دعم وحوكمة المنظمة للسلوكيات المناسبة، ويشمل ذلك السياسات والإجراءات، سياسة الاستخدام المقبول، الأدوار والمسؤوليات، برنامج التوعية والتدريب، الهيكل التنظيمي للمنظمة، هيكلة الأمن السيبراني، التسلسل الإداري للتبليغ، ووثيقة لجنة الأمن السيبراني. بينما يقيس المستوى الفردي مستوى وعي الموظفين بالأمن السيبراني من خلال استخدام نظام إدارة التعلم وتقنيات محاكاة للهجوم التصيّدي أو من خلال تطوير استبانة في حال عدم توفر التقنيات اللازمة.

ج) **بناء البرنامج:** تهدف الخطوة الأخيرة إلى تحديد الفجوة بين الوضع الراهن والوضع المستهدف وبناء البرنامج لتحقيق الأهداف الاستراتيجية.

— انتهى —