Organización de Aviación Civil Internacional

NOTA DE ESTUDIO

AN-Conf/14-WP/126[1]
29/06/24
(Nota de información)
En español únicamente

DECIMOCUARTA CONFERENCIA DE NAVEGACIÓN AÉREA

Montreal, Canadá, 26 de agosto al 6 de septiembre de 2024

Cuestión 4: Hiperconectividad del sistema de navegación aérea
4.2: Ciberseguridad y resiliencia de los sistemas de información

MODELO DE GESTIÓN DE LA CIBERSEGURIDAD

(Nota presentada por Argentina con el apoyo de 21 Estados miembros de la CLAC[2])

RESUMEN

En la presente nota se presentan consideraciones respecto al desarrollo de un modelo de gestión de la ciberseguridad que brinde lineamientos y prácticas seguras para incrementar los niveles de disponibilidad, integridad y confidencialidad de los servicios CNS/ATM.

Medidas propuestas a la Conferencia: Se invita a la Conferencia a:

a) analizar la pertinencia de desarrollar un modelo de gestión de la ciberseguridad dinámico aplicable a los servicios CNS/ATM,

b) considerar el desarrollo de un programa de prácticas de simulaciones de incidentes de ciberseguridad con el objetivo de minimizar el impacto que éstos puedan causar en los servicios CNS/ATM.

1. INTRODUCCIÓN

1.1 En materia de ciberseguridad, los referentes de la industria adoptan modelos de gestión basados en funciones (gobernar, identificar, proteger, detectar, responder, recuperar). Estos modelos sufren cambios y adaptaciones para dar respuesta a la gran diversidad de ciberataques que se producen a nivel mundial.

1.2 El avance de la conectividad sobre los sistemas hace necesaria la gestión centralizada o remota. Estos requerimientos generan nuevas superficies y vectores de ataques que pueden ser utilizados para comprometer la disponibilidad, integridad y confidencialidad de los servicios CNS/ATM.

[1] La versión en español fue proporcionada por Argentina.
[2] Aruba, Belice, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay, Venezuela.

1.3 De los últimos *ciberincidentes*, se evidencia una sofisticación creciente en técnicas, tácticas y procesos. Podemos advertir que estos ataques son dirigidos, orquestados por grupos u organizaciones amplias, y distribuidas por el planeta.

1.4 Los ciberdelincuentes se valen de nuevas técnicas y herramientas para vulnerar los sistemas sin ningún límite de tiempo. El uso de la *inteligencia artificial* (IA) para mejorar la efectividad de los ataques es una realidad. Se estima que para el 2024, los ciberataques asistidos por IA incrementarán su efectividad en un 50%.

1.5 Las evidencias muestran que los *ciberincidentes* en su gran mayoría tienen como vector de entrada a los usuarios internos. Estos, son blanco de correos maliciosos del tipo phishing logrando recolectar información del personal que posteriormente será utilizada para realizar fraudes económicos o escalamiento de privilegios.

1.6 Garantizar la disponibilidad, integridad y confidencialidad de los servicios CNS/ATM requiere de recursos tecnológicos y humanos que permitan detectar eventos de seguridad antes que estos se conviertan en incidentes. En este sentido es importante trabajar en la prevención.

1.7 Los sistemas descentralizados y extendidos generan perímetros amplios de exposición.

1.8 Se entiende que los atacantes disponen de tiempo y herramientas sofisticadas como puede ser la IA, para probar y chequear dentro y fuera de las organizaciones esperando el momento o las condiciones propicias para iniciar un ataque.

1. ANÁLISIS

2.1 En consonancia con lo anteriormente expuesto, es necesario realizar un análisis de los distintos marcos de gestión consolidados con el objetivo de diseñar un modelo de gestión de la ciberseguridad de los servicios CNS/ATM que adopte nuevas técnicas, herramientas y procedimientos que respondan eficientemente a *ciberamenazas* y *ciberataques.*

2.2 Entendiendo que los ciberataques son cada vez más sofisticados en las tácticas utilizadas, es necesario adoptar un **modelo de gestión de la ciberseguridad dinámico**, es decir, que se analice y ajuste de manera periódica y sostenible en el tiempo.

2.3 Es fundamental entender que una gestión dinámica de la ciberseguridad incluye lineamientos y buenas prácticas en materia de ciberseguridad. Estas últimas brindan claridad respecto a las acciones que se tienen que tomar ante un incidente de ciberseguridad.

2.4 Por otra parte, la implementación de prácticas de simulaciones de *ciberincidentes* resulta de vital importancia, ya que permite que los integrantes de las distintas áreas de la organización que intervienen en la recuperación de los servicios ante la ocurrencia de tales sucesos, tengan claro, entre otros aspectos, las responsabilidades y roles que cada uno ha de ejercer durante estos siniestros.

2.5 Al mismo tiempo, esta simulación mejora la toma de decisiones en condiciones de presión. Es de público conocimiento que estas situaciones son complejas en lo técnico y humano.

2.6 Es importante reducir el riesgo o la posibilidad de que un incidente se convierta en un desastre con un alto impacto en la disponibilidad, confidencialidad e integridad de los servicios CNS/ATM.

2. CONCLUSIÓN

3.1 En virtud de lo expuesto, se invita a la Conferencia a:

a) analizar la pertinencia de desarrollar un *modelo de gestión de la ciberseguridad dinámico* aplicable a los servicios CNS/ATM; y

b) considerar el desarrollo de un *programa de prácticas de simulaciones de incidentes de ciberseguridad* con el objetivo de minimizar el impacto que éstos puedan causar en los servicios CNS/ATM.

— FIN —