Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

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

ASSEMBLÉE — 41e SESSION

COMITÉ EXÉCUTIF

Point 14 : Sûreté de l'aviation — Politique

STRATÉGIE DE CULTURE DE LA CYBERSÉCURITÉ

(Note présentée par l'Arabie saoudite, au nom des États de l'Organisation arabe de l'aviation civile [OAAC][2])

RÉSUMÉ ANALYTIQUE

Les cyberattaques sont en constante progression dans le secteur de l'aviation civile, ce qui, à son tour, a des répercussions sur les aérodromes, les compagnies aériennes, le trafic aérien et les passagers. La meilleure méthode pour réduire les cyberrisques est d'élaborer une stratégie de culture de la cybersécurité destinée à renforcer les capacités du personnel, promouvoir les objectifs de la cybersécurité et protéger les organisations contre les cybermenaces internes et externes. La stratégie de culture de la cybersécurité vise à jouer un rôle critique dans la conformité aux exigences de la cybersécurité et à renforcer la coopération aux niveaux organisationnel, national et international. Une stratégie de culture de la cybersécurité devrait prendre en compte tout le personnel d'une organisation, car elle cherche à établir et à développer une culture de la cybersécurité capable de soutenir les personnes, les technologies et les opérations de cybersécurité.

Suite à donner : L'Assemblée est invitée à :

a) demander instamment aux États membres d'adopter une stratégie de culture de la cybersécurité dans l'aviation civile, à la lumière de l'augmentation significative des cyberattaques dans le monde ;
b) à demander à l'OACI d'élaborer un programme de sensibilisation à la cybersécurité à l'intention du personnel de l'aviation civile, parallèlement au programme de culture de la sûreté de l'aviation.

Objectifs stratégiques :	La présente note de travail se rapporte à l'objectif stratégique *Sûreté et facilitation.*

[1] Version en arabe fournie par l'Arabie saoudite.
[2] *États membres de l'Organisation arabe de l'aviation civile (OAAC) : Algérie, Arabie saoudite, Bahreïn, Comores, Djibouti, Égypte, Émirats arabes unis, Irak, Jordanie, Koweït, Liban, Libye, Mauritanie. Maroc, Oman, Palestine, Qatar, République arabe de Syrie, Somalie, Soudan, Tunisie et Yémen.*

Incidences financières :	
Références :	

1. INTRODUCTION

1.1 L'erreur humaine a été citée comme la première cause des attaques et des violations de la cybersécurité en 2021, ce qui laisse entendre que le personnel constitue le maillon le plus faible de la chaine de la cybersécurité. En outre, les cybercriminels ont lancé des attaques visant les usagers du système pour exploiter leurs vulnérabilités. Les organisations doivent donc élaborer des stratégies de culture de la cybersécurité pour s'assurer que leur personnel est bien aux prises avec un vaste éventail de cybermenaces qui les visent ou qui visent leurs postes de travail. De ce fait, ils deviennent la première ligne de défense de leurs organisations.

1.2 Les personnes, les processus et les technologies constituent les trois principaux piliers de la cybersécurité. Ces trois piliers dépendent fondamentalement d'une forte culture de la cybersécurité, car la technologie, sans un personnel adéquatement formé, créera des vulnérabilités. Les processus en eux-mêmes sont également inefficaces s'ils ne sont pas correctement mis en œuvre par le personnel.

1.3 L'erreur humaine n'est pas limitée aux usagers qui cliquent sur des liens suspects ou qui téléchargent des logiciels malveillants. Le risque le plus important vient des développeurs de systèmes sous-qualifiés qui commettent une erreur en configurant ou en installant un système critique ou qui omettent de suivre des procédures de gestion des changements tout en introduisant des changements dans un système, exposant de ce fait l'ensemble de l'infrastructure technique à des cybermenaces externes.

1.4 Tous les membres du personnel doivent bien connaitre leurs rôles et responsabilités dans l'application du programme de cybersécurité de l'organisation. Ils doivent également comprendre les obligations qui leur incombent en vertu de la politique de cybersécurité et de tout code pénal national portant sur les cyberactivités.

1.5 Les cadres supérieurs et les membres du conseil d'administration jouent un rôle crucial dans la promotion des exigences relatives à la cybersécurité et dans le traitement des cyberrisques. De ce fait, ils doivent être sensibilisés à l'importance de la cybersécurité et traiter les cyberrisques comme des risques qui concernent l'ensemble de l'organisation.

2. CULTURE DE LA CYBERSÉCURITÉ

2.1 Une culture de la cybersécurité cyber promeut le partage des informations entre les États membres pour identifier proactivement et traiter des cybervulnérabilités et des cybermenaces.

2.2 Un changement efficace commence par la sensibilisation et la formation à la cybersécurité. Les organisations doivent par conséquent prendre des mesures supplémentaires pour effectuer des changements comportementaux en adoptant une culture de la cybersécurité.

2.3 Une culture de la cybersécurité comprend les trois étapes suivantes :

a) *identification des objectifs stratégiques :* L'identification des objectifs d'une culture de la cybersécurité est la première étape du processus. Ces objectifs peuvent comprendre, entre *autres,* le fait de s'assurer que les employés comprennent parfaitement les risques de la cybersécurité pour l'organisation et connaissent bien leurs rôles et responsabilités, ainsi que le fait d'améliorer les connaissances et les compétences en matière de cybersécurité ;

b) *évaluation de la situation existante :* Cet objectif consiste à évaluer la culture existante aux niveaux organisationnel et individuel. Le niveau organisationnel reflète la gouvernance de l'organisation et la promotion de ses comportements appropriés. Ceci peut comprendre les politiques et les procédures, la politique d'utilisation acceptable, les rôles et responsabilités, la sensibilisation et la formation, la structure organisationnelle, les structures de cybersécurité, les comptes rendus d'incidents et la documentation du comité de cybersécurité. D'un autre côté, au niveau individuel, on procède à des investigations sur le niveau de sensibilisation du personnel à la cybersécurité, par le biais de plates-formes d'apprentissage ou de simulations de cyberattaques. En l'absence des technologies requises, une enquête peut être lancée et diffusée pour recueillir les informations nécessaires ;

c) *élaboration du programme :* La dernière étape consiste à bien déterminer l'écart entre la situation actuelle et la situation souhaitée et établir le programme afin de réaliser les objectifs stratégiques antérieurement identifiés.

— FIN—