ASTech Paris Region

LES CAHIERS d'ASTech

CYBERSÉCURITÉ

Les chefs d'entreprises doivent faire face à une offre de dispositifs d'accompagnement de plus en plus conséquente.

Aussi, ils doivent redoubler de vigilance pour adhérer aux bons dispositifs :

- les plus pertinents pour leur activité,
- répondants parfaitement aux règles établies par la profession.

Pour mieux vous aider à comprendre les offres qui vous sont proposées **ASTech présente ses cahiers thématiques pour aider les PME/ETI de la filière ASD** à choisir le dispositif le plus adapté pour répondre notamment aux attentes des Grands Donneurs d'ordre de la filière ASD.

Document réalisé avec la collaboration

BOOST AEROSPACE DGA

CYBERSÉCURITÉ

PME de la filière ASD !! êtes-vous suffisamment informées ?

L'évolution numérique et la multiplication des interconnexions transforment en profondeur les secteurs de l'aéronautique et de la défense.

Alors que ces industries sont historiquement associées à des technologies de pointe, elles se trouvent désormais confrontées à des menaces cyber d'une complexité et d'une ampleur inédites.

Cela concernant différents domaines de cette industrie, de la sécurisation des électroniques embarquées jusqu'à la surveillance de leur chaîne d'approvisionnement.

Un simple phishing de la messagerie d'un sous-traitant peut constituer, pour un hacker, un moyen de cartographier la supply chain des donneurs d'ordre, ce qui expose tout particulièrement les PME de notre filière ASD.

PME de la filière ASD !! êtes-vous réellement préparées ?

- la cyber sécurité n'est plus une option mais une condition d'accès au marché,
- les grands donneurs d'ordres de l'ASD renforcent leurs exigences en matière de sécurité,
- un simple maillon faible dans la supply chain peut compromettre l'ensemble d'un programme industriel,
- ne pas se structurer sa démarche cyber c'est prendre le risque de perdre un marché, d'être déférencé, de subir une attaque impactant la production, d'engager plus globalement sa responsabilité contractuelle.

Les menaces cyber dans un contexte global

Les secteurs de l'aéronautique et de la défense font face à une mutation rapide des cybermenaces.

En 2024, un rapport du Ministère des Armées a révélé une **augmentation de 35 %** des tentatives d'intrusion visant les systèmes de contrôle des aéronefs et les infrastructures de défense stratégique.

Ces attaques, souvent perpétrées par des groupes étatiques ou des cybercriminels organisés, exploitent les vulnérabilités des réseaux interconnectés et des systèmes embarqués.

La digitalisation accrue des processus opérationnels expose également ces secteurs à de nouveaux risques, notamment via les **attaques par ransomware*** et les intrusions dans **les systèmes IoT****. Par ailleurs, l'essor des **technologies d'intelligence artificielle (IA)** offre aux hackers des outils sophistiqués pour contourner les dispositifs de sécurité traditionnels. Ces évolutions imposent une vigilance constante et une adaptation permanente des stratégies de défense.

* **Un rançongiciel ou ransomware** en anglais est un code malveillant qui bloque l'accès à votre appareil ou à des fichiers en les chiffrant et qui vous réclame le paiement d'une rançon pour obtenir le déchiffrement de vos données. L'appareil peut être infecté de différentes façons :

- après l'ouverture d'une pièce-jointe frauduleuse ou d'un lien malveillant reçu par email ;
- lors d'une navigation sur des sites compromis ;
- suite à une intrusion informatique sur le système de la victime.

Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

** **Réseau d'objets physiques connectés à Internet**

LES SOLUTIONS PRINCIPALES POUR LA FILIÈRE ASD

Deux solutions s'offrent à vous, indépendantes pour l'instant :

- **Vous travaillez pour les filières Aéronautique et spatiale :** AIRCYBER (BoostAerospace)
- **Vous avez des activités pour la défense :** Référentiel de maturité Cyber (RMC) (Ministère des Armées et des anciens combattants, DGA)
- **Vous travaillez pour les filières Aéronautique, spatiale et défense :** AIRCYBER & Référentiel de maturité Cyber (RMC)

AIRCYBER

AirCyber est le standard de maturité CyberSécurité de la filière que BoostAeroSpace gouverne pour fixer les niveaux de protection adaptés aux problématiques de cybersécurité de la Supply Chain.
Afin de déployer ce standard en collaboration entre donneurs d'ordres et fournisseurs, BoostAeroSpace déploie un programme (dispositif d'aide) qui se base sur le questionnaire RMC fondamental*. Cela permet aux fournisseurs d'être aussi résilients que les OEMs** face aux attaques cyber dans l'objectif ultime de standardiser et d'homogénéiser le niveau de protection de toute l'industrie.

* *Le référentiel de Maturité Cyber Fondamental (RMC) est un outil pour évaluer la maturité cyber d'une organisation. Il permet de répondre à 21 exigences fondamentales qui sont essentielles pour garantir la continuité des activités industrielles.*

Adhérer au service permet aux fournisseurs de bénéficier de l'intelligence collective de la communauté facilitant ainsi la mise en place de leur plan d'action et également de rendre leurs engagements et réalisations visibles et reconnus par les OEMs via les outils mis en place par et pour la filière.

Ce dispositif est opéré par BoostAerospace.
BoostAerospace a été créé en 2011 par de grands acteurs aérospatiaux – Airbus, Dassault Aviation, Safran et Thales.

** *Fabricant d'équipement d'origine*

Le dispositif

1. Auto diagnostic : Remplir le questionnaire AirCyber et sélectionner le "maturity assessor"* de votre choix pour planifier le rendez-vous sur site.
Durée de l'intervention : 2 heures.

* *Évaluateur de maturité certifié*

2. Analyse du niveau de maturité sur site : Revue sur site de votre niveau de maturité avec l'expert.
Durée de l'intervention : 1 jour + 1 mois (réception du rapport).

3. Déploiement du plan d'actions : Plan d'actions trié par criticité. Mettre en place les différentes actions pour augmenter son niveau de maturité.
Durée de l'intervention : 1 niveau/an (bronze/silver/ gold).

4. Mise à jour du plan d'actions : Revue annuelle en visio, conférence avec un expert. Utiliser les outils en ligne AirCyber (outil de maturité, catalogue, communauté)
Durée de l'intervention : 2 heures/an.

Tarifs :

- A partir* de **5 100€HT** la première année
- **1 000€HT/an** les années suivantes

* *Tarification adaptée à la taille de l'entreprise (entreprises <50 salariés 5 000€HT)*

CONTACT :
aircyber@boostaerospace.com

INFORMATION :
www.boostaerospace.com

DIAG CYBER

Le Diag Cyber DGA est un dispositif d'aide à la cybersécurisation destiné aux PME et ETI de l'industrie de la défense pour réduire les vulnérabilités numériques et financer les frais de cybersécurisation.
Ce dispositif consiste en une prestation d'audit et de conseil (phase A).

Le dispositif

Audit et analyse de risque, suivi par un expert référencé par l'ANSSI.

- Identifier et analyser les risques numériques et de cybersécurité de votre entreprise,
- Déterminer les mesures de sécurité adaptées à différents scénarios de menace,
- Évaluer à dire d'expert le niveau de maturité cyber de votre entreprise vis-à-vis du référentiel de maturité cyber de la DGA

Durée de l'intervention : 8 jours.

Tarifs :

Phase A :

- forfaitairement fixé à un maximum de **8 800 €HT** (selon éligibilité subvention de 50 % du montant de la prestation d'expertise),

Durée de l'intervention : 8 jours.

CONTACT :
dga-did-pme-cyber.contact@intradef.gouv.fr

INFORMATION :
https://www.armement.defense.gouv.fr

ASTech Paris Region

1-3 allée de Bruxelles
Aéroport de Paris Le Bourget
93350 Le Bourget
sebastien.courrech@pole-astech.org
www.pole-astech.org