

CONTRÔLE DES RISQUES • CYBER-RÉSILIENCE

La cyber-résilience n'est pas un pare-feu. C'est ce qui se passe après qu'un pare-feu a cédé.

Les chaînes d'approvisionnement de la défense et de l'aérospatiale reposent sur la même hypothèse que toute organisation moderne : que les systèmes qui font fonctionner les autres systèmes continueront de fonctionner. La plupart du temps, c'est le cas. La cyber-résilience concerne les fois où ce n'est pas le cas.



La véritable exposition

Le rapport Interpol sur les cybermenaces en Afrique a placé à plusieurs reprises l'Afrique du Sud parmi les pays les plus visés par la cybercriminalité sur le continent, un phénomène lié en partie à sa concentration de ports, d'infrastructures énergétiques et de capacités de fabrication pour la défense. Rien de tout cela ne va disparaître, et rien de tout cela ne fait de cette menace le problème de quelqu'un d'autre.

01

Les quatre phases autour desquelles s'articule chaque mission de résilience. —

La résilience, c'est maintenir les opérations, les communications et la prise de décision pendant qu'un incident est en cours, et se rétablir selon son propre calendrier plutôt que celui de l'attaquant. Une expédition retardée ou un avion cloué au sol entraîne des conséquences qui vont bien au-delà du coût, et c'est précisément là que la plupart des organisations découvrent que leur plan était resté théorique.

2021

En juillet 2021, une attaque par rançongiciel a paralysé les opérations conteneurs dans tous les grands ports sud-africains pendant plusieurs jours. Des camions faisaient la queue devant Durban et Le Cap, sans nulle part où décharger. L'attaquant n'a jamais touché une grue ni un navire. Un seul système compromis dans un bureau administratif a suffi à arrêter le fret dans tout le pays.

02

Les quatre phases autour desquelles s'articule tout engagement en matière de résilience.

01

PRÉPARER

02

DÉTECTER

03

RÉPONDRE

04

RÉTABLIR

Pourquoi c'est important au salon AAD

Les organisations de la défense et de l'aérospatiale se situent à la croisée de l'intérêt national et de la pression commerciale. Cette combinaison attire une catégorie différente d'adversaires, ce qui signifie qu'une défaillance de résilience est rarement un problème purement interne. Nous aidons les organisations de ce secteur à construire une position défendable avant d'en avoir besoin, pas après.

03

Ce que nous faisons

DISystems accompagne des organisations en Afrique du Sud, dans la région de la SADC et à l'international sur le volet concret de la cyber-résilience, pas seulement sur la paperasse qui l'entoure.



Évaluations de cyber-résilience étalonnées sur ISO 27001, NIST et King IV, construites autour de notre méthodologie G-RISE plutôt que d'une liste de contrôle générique.



Préparation aux incidents et planification de la réponse, y compris des exercices de simulation menés avec votre véritable équipe de direction, et non un scénario emprunté à un modèle standard.



Revue de risques liés aux tiers et à la chaîne d'approvisionnement, portant sur les fournisseurs et sous-traitants qui représentent autant de risque que votre propre réseau.



Conseil en gouvernance, gestion des risques et conformité, aligné sur la POPIA et les normes internationales, documenté sous une forme réellement exploitable par vos auditeurs et régulateurs.

DISYSTEMS

La plupart des organisations découvrent l'écart entre leur plan et leur réalité au moment même d'un incident. Nous préférons le détecter avec vous en amont, un mardi ordinaire, quand il reste encore le temps de le corriger.

DISystems – Conseil en cybersécurité et GRC en Afrique du Sud, dans la région de la SADC et à l'international, en partenariat avec **Cyberantix™**

CONTACTEZ-NOUS À L'ADRESSE :

tsepang@disystems.co.za

pour convenir d'un rendez-vous et en savoir plus.

