Les étapes « vers le Cloud » pour les gouvernements et administrations publiques

Le rapport de l'ENISA Cadre de sécurité pour les Cloud gouvernementaux décrit un guide étape par étape à l'intention des Etats Membres (EM) pour l'acquisition et l'utilisation sécurisées de services en Cloud.

Ce cadre répond au besoin d'un cadre de sécurité commun lors du déploiement de Clouds gouvernementaux et s'appuie sur les conclusions de deux études précédentes de l'ENISA. Il est recommandé de l'intégrer à la boite à outils des administrations publiques lors de la planification de la migration vers le Cloud ainsi que lors de l'évaluation des contrôles et procédures de sécurité déployés.

Le cadre suggéré est structuré en quatre (4) phases, neuf (9) activités de sécurité et quatorze (14) étapes qui détaillent l'ensemble des actions que les Etats Membres devraient suivre pour définir et mettre en œuvre un Cloud gouvernemental sécurisé. En outre, le modèle est validé de façon empirique, grâce à l'analyse de quatre (4) cas de Clouds gouvernementaux – Estonie, Grèce, Espagne et Royaume-Uni – servant aussi d'exemple à la mise en œuvre de Clouds gouvernementaux.

Le cadre se concentre sur les activités suivantes : le profilage des risques, le modèle architectural, les exigences de sécurité et de confidentialité, les contrôles de sécurité, la mise en œuvre, le déploiement, l'accréditation, le log/suivi, l'audit, la gestion du changement et la gestion de sortie.

L'étude montre que le niveau d'adoption de Clouds gouvernementaux est encore faible ou à un stade très précoce. Les questions de sécurité et de confidentialité sont les principaux obstacles, et en deviennent même temps des facteurs clés à prendre en compte lors de la migration vers les services Cloud. De plus, il y a un réel besoin de pilotes et prototypes en Cloud pour tester l'utilité et l'efficacité du modèle économique du Cloud pour l'administration publique.

Les organisations se tournent vers le Cloud, améliorant l'efficacité et l'efficience des technologies de l'information et de la communication (TIC). Pour les gouvernements, il est rentable et offre d'importantes possibilités en termes d'évolutivité, d'élasticité, de performance, de résilience et de sécurité.

Le directeur général de l'ENISA a commenté : « *Le rapport fournit aux gouvernements les outils nécessaires pour déployer les services en Cloud avec succès. Les citoyens et les entreprises bénéficient du marché unique numérique de l'UE en accédant à ces services à travers l'UE. La technologie Cloud est un pilier fondamental et un moteur de croissance et de développement à travers toute l'Europe.* »

Le rapport fait partie de la contribution de l'agence à la stratégie Cloud de l'UE, visant des experts nationaux, des organismes gouvernementaux et des administrations publiques dans l'UE, afin de définir la stratégie de sécurité nationale du Cloud, obtenant des données de bases pour analyser le déploiement du Cloud gouvernemental existant du point de vue de la sécurité ou pour les aider à remplir leurs exigences en matière de sécurité d'approvisionnement. Les décideurs européens, les fournisseurs du secteur privé de l'UE de services en Cloud (Cloud Service Providers - CSP), et les courtiers du Cloud, peuvent également bénéficier de son contenu.

En substance, le cadre sert de guide préparatoire à un achat public et peut être utilisé tout au long

du cycle de vie de l'adoption du Cloud. L'étape suivante par l'ENISA est d'offrir ce cadre comme outil de référence.

Pour le rapport complet : Cadre de sécurité pour Clouds gouvernementaux

Pour toute demande d'interview : Dimitra Liveri, Security & Résilience des réseaux de communication, cloud.security@enisa.europa.eu

Notes aux journalistes:

Précédents rapports sur le sujet:

Sécurité et résilience des Clouds gouvernementaux

Guide de bonnes pratiques pour le déploiement et la sécurité de Clouds gouvernementaux