La Structure logicielle du système de certification cloud de l'ENISA

ENISA publie une description de la structure logicielle et un outil en ligne pour aider les consommateurs avec la sécurité en cloud lors d'achats sur de services en cloud

ENISA lance le CCSM (Cloud Certification Schemes Metaframework), « Structure logicielle du système de certification cloud ». Le CCSM est une structure logicielle qui cartographie les exigences de sécurité utilisées dans le secteur public afin d'atteindre les objectifs de sécurité dans le système de certification cloud existant. Le but du CCSM est d'offrir plus de transparence à propos des systèmes de certification et d'aider les utilisateurs avec les procédures d'utilisation des services en cloud computing.

Cette première version du CCSM est restreinte aux exigences en matière de sécurité de l'information et des réseaux (*network and information security*, NIS). Le rapport est basé sur **29 documents avec des exigences NIS** de **11 pays** (Royaume-Uni, Italie, Pays-Bas, Espagne, Suède, Allemagne, Finlande, Autriche, Slovaquie, Grèce, Danemark). Il recouvre **27 objectifs de sécurité**, qui sont cartographiés en **5 systèmes de certification cloud**.

Depuis l'an dernier l'ENISA a travaillé, en partenariat avec le Groupe des industries du secteur du cloud sur les systèmes de certification (Cloud Select Industry Group on Certification Schemes) et la Commission Européenne, et produit **deux outils** pour aider les utilisateurs à gérer la sécurité de leur cloud. Ce travail fait partie de la Stratégie Cloud de l'UE. Le premier outil, le CCSL, est une liste systèmes (existants) de certification de sécurité de l'information. Le CCSL a été lancé l'année dernière et est accessible en ligne. CCSM le deuxième outil, une extension de CCSL.

Le CCSM est déjà utilisé : la Commission Européenne a annoncé avoir ouvert un large appel d'offre de services sur le cloud (2500 cloud VM et 2500 TB de stockage sur le cloud), qui utilise les 27 objectifs de sécurité du CCSM.

Udo Helmbrecht, directeur exécutif de l'ENISA, avance *: « La sécurité du cloud est une question importante à la fois pour les clients des secteurs public et privé dans l'UE. Evidemment la certification ne règle pas tous les problèmes de sécurité, mais cela peut simplifier certaines étapes du marché. Cet outil aide les clients afin d'utiliser les systèmes de certification existant et propose également aux fournisseurs de services cloud un format pour expliquer les mesures de sécurité qu'ils prennent pour protéger leurs services. »*

Cette version du CCSM a été mis en œuvre comme un outil en ligne qui cartographie les différents systèmes de certification en une seule liste d'objectifs de sécurité. L'outil permet aux utilisateurs de choisir les objectifs de sécurité les plus pertinents pour eux, et :

1. De générer une cartographie des matrices pour différents systèmes de certification cloud et/ou,
2. De générer une liste de contrôle ou des questionnaires en version imprimé ou en tableur

Pour le rapport en entier et les outils en ligne : https://resilience.enisa.europa.eu/cloud-computing-certification

Note aux rédacteurs :

- Communiqué de presse de la Commission Européenne : L'UE lance un appel d'offre aux Entreprises de Haute Technologie à fournir des services de cloud computing pour l'UE http://ec.europa.eu/dgs/informatics/doc/newscloud.pdf

- Nouveaux programmes sur la Liste de certification cloud (CCSL) : http://www.enisa.europa.eu/media/news-items/new-schemes-on-the-cloud-certification-list-1

- Certification dans la stratégie cloud de l'UE : https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy

Pour toute demande d'interview : Dr. Marnix Dekker, expert NIS, et Dimitra Liveri, Sécurité et résilience des réseaux de communication, cloud.security@enisa.europa.eu