29.01.2015
EPR05/2015
www.enisa.europa.eu

ENISA Meta-Rahmen für Cloud-Zertifizierungsprogramme

ENISA veröffentlicht einen Meta-Rahmen sowie ein Online-Tool, um Kunden beim Kauf von Cloud-Services mit Cloud-Security zu unterstützen.

ENISA führt den „Meta-Rahmen für Cloud-Zertifizierungsprogramme“ („Cloud Certification Schemes Metaframework“) CCSM ein. CCSM ist ein Meta-Rahmen, in dem detaillierte Sicherheitsanforderungen dargestellt werden, die im öffentlichen Sektor für Sicherheitsziele in bestehenden Cloud-Zertifizierungsprogrammen verwendet werden. Das Ziel des CCSM besteht darin, mehr Transparenz für Zertifizierungsprogramme zu erreichen und Kunden bei der Beschaffung von Cloud-Computing-Services zu unterstützen.

Die erste Version des CCSM ist auf Netzwerk- und Informationssicherheitsanforderungen beschränkt. Sie beruht auf **29 Dokumenten mit NIS-Anforderungen** aus **11 Ländern** (Großbritannien, Italien, Niederlande, Spanien, Schweden, Deutschland, Finnland, Österreich, Slowakei, Griechenland, Dänemark). Dabei werden **27 Sicherheitsziele** abgedeckt, die **5 Cloud-Zertifizierungsprogrammen** zugeordnet sind.

ENISA arbeitet seit letztem Jahr mit der Cloud Select Industry Group on Certification Schemes und der Europäischen Kommission zusammen und hat **2 Tools** entwickelt, die Kunden im Bereich Cloud Security unterstützen. Diese Arbeit ist Teil der EU-Cloud-Strategie. Das erste Tool, CCSL, ist eine Liste (bestehender) Informationssicherheitszertifizierungsprogramme. Es wurde letztes Jahr eingeführt und ist online verfügbar. CCSM ist das zweite Tool und stellt eine Erweiterung von CCSL dar.

CCSM ist bereits im Einsatz: Die EU-Kommission gab bekannt, dass sie eine große Ausschreibung zur Beschaffung von Cloud Services (2500 Cloud VMs und 2500 TB Cloud-Storage) eröffnet hat, wobei die 27 Sicherheitsziele des CCSM verwendet werden.

Der geschäftsführende Direktor der ENISA, Professor Udo Helmbrecht, erklärte: „Cloud-Security ist sowohl für Kunden aus dem privaten als auch dem öffentlichen Sektor in der EU von großer Bedeutung. Natürlich löst die Zertifizierung nicht alle Sicherheitsprobleme, sie kann jedoch einige der Beschaffungsmaßnahmen vereinfachen. Dieses Tool unterstützt Kunden bei der Verwendung bestehender Zertifizierungsprogramme und bietet den Anbietern von Cloud-Services ein Format, mit dem sie die Sicherheitsmaßnahmen zum Schutz ihrer Dienste erklären können.“

Diese Version von CCSM wurde als Online-Tool ausgeführt. Das Tool bildet verschiedene Zertifizierungsprogramme auf einer einzigen Liste mit Sicherheitszielen ab. Das Tool gestattet es dem Kunden, die für ihn wichtigsten Sicherheitsziele auszuwählen und

1. ein Matrix-Mapping zu verschiedenen Cloud-Zertifizierungsprogrammen zu erstellen und/oder
2. Beschaffungs-Checklisten oder Fragebögen als Ausdrucke oder Tabellen zu erstellen.

Im nächsten Schritt würden bei CCSM die NIS-Anforderungen aus anderen Ländern integriert und der

Umfang des CCSM so erweitert, dass auch NIS-Anforderungen für den Schutz personenbezogener Daten enthalten sind.

Der vollständige Bericht (in englischer Sprache) und das Online-Tool sind hier abrufbar: https://resilience.enisa.europa.eu/cloud-computing-certification

Hinweise für Redakteure:

- Pressemitteilung der EU-Kommission: EU-Technologieunternehmen aufgefordert, ein Angebot über die Bereitstellung von Cloud-Services für die EU abzugeben http://ec.europa.eu/dgs/informatics/doc/newscloud.pdf
- Neue Programme auf der Cloud-Zertifizierungsliste (CCSL) : http://www.enisa.europa.eu/media/news-items/new-schemes-on-the-cloud-certification-list-1
- Zertifizierung in der EU-Cloud-Strategie: https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy

Für Interviews: Dr. Marnix Dekker, NIS-Experte, und Dimitra Liveri, Sicherheit & Resilienz von Kommunikationsnetzwerken, unter cloud.security@enisa.europa.eu