29/01/2015
EPR05/2015
www.enisa.europa.eu

Μετα-πλαίσιο συστημάτων πιστοποίησης του ENISA για το υπολογιστικό νέφος

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) δημοσιεύει ένα μετα-πλαίσιο και ένα διαδικτυακό εργαλείο για να βοηθήσει τους πελάτες με την ασφάλεια στο υπολογιστικό νέφος, όταν αγοράζουν υπηρεσίες υπολογιστικού νέφους.

Ο ENISA ξεκινά το CCSM, το «Μετα-πλαίσιο συστημάτων πιστοποίησης για το υπολογιστικό νέφος». Το CCSM είναι ένα μετα-πλαίσιο που αντιστοιχίζει τις λεπτομερείς απαιτήσεις ασφαλείας που χρησιμοποιούνται στο δημόσιο τομέα με τους στόχους ασφάλειας στα υπάρχοντα συστήματα πιστοποίησης για το υπολογιστικό νέφος. Στόχος του CCSM είναι να παράσχει περισσότερη διαφάνεια για τα συστήματα πιστοποίησης και να βοηθήσει τους πελάτες με την προμήθεια υπηρεσιών υπολογιστικού νέφους.

Αυτή η πρώτη έκδοση του CCSM περιορίζεται στις απαιτήσεις ασφάλειας δικτύων και πληροφοριών. Βασίζεται σε **29 έγγραφα με απαιτήσεις ασφάλειας δικτύων και πληροφοριών (NIS)** από **11 χώρες** (Ηνωμένο Βασίλειο, Ιταλία, Ολλανδία, Ισπανία, Σουηδία, Γερμανία, Φινλανδία, Αυστρία, Σλοβακία, Ελλάδα, Δανία). Καλύπτει **27 στόχους ασφάλειας**, και τους αντιστοιχίζει με **5 συστήματα πιστοποίησης για το υπολογιστικό νέφος**.

Από πέρυσι, ο ENISA συνεργάζεται με την Επίλεκτη ομάδα του κλάδου για τα συστήματα πιστοποίησης και την Ευρωπαϊκή Επιτροπή, δημιουργώντας **2 εργαλεία** για να βοηθήσουν τους πελάτες με την ασφάλεια του υπολογιστικού νέφους. Αυτό το έργο είναι μέρος της Στρατηγικής της ΕΕ για το υπολογιστικό νέφος. Το πρώτο εργαλείο, το CCSL, αποτελεί λίστα (υπαρχόντων) συστημάτων πιστοποίησης ασφάλειας των πληροφοριών. Το CCSL ξεκίνησε πέρυσι και είναι προσβάσιμο στο διαδίκτυο. Το CCSM είναι το δεύτερο εργαλείο και αποτελεί προέκταση του CCSL.

Το CCSM χρησιμοποιείται ήδη: η Ευρωπαϊκή Επιτροπή ανακοίνωσε ότι προκήρυξε μεγάλο διαγωνισμό με πρόσκληση υποβολής προσφορών για την προμήθεια υπηρεσιών υπολογιστικού νέφους (2.500 υπερβατικών μηχανών υπολογιστικού νέφους και 2.500 TB αποθηκευτικού χώρου στο νέφος), η οποία χρησιμοποιεί τους 27 στόχους ασφάλειας του CCSM.

Ο Udo Helmbrecht, εκτελεστικός διευθυντής του ENISA, δήλωσε: «Η ασφάλεια του υπολογιστικού νέφους αποτελεί σημαντικό ζήτημα για τους πελάτες του ιδιωτικού αλλά και του δημόσιου τομέα στην ΕΕ. Προφανώς, η πιστοποίηση δεν επιλύει όλα τα ζητήματα ασφάλειας, ωστόσο μπορεί να απλουστεύσει μερικά από τα βήματα της προμήθειας. Το εργαλείο αυτό βοηθά τους πελάτες να χρησιμοποιήσουν τα υπάρχοντα συστήματα πιστοποίησης, ενώ συγχρόνως προσφέρει στους παρόχους υπηρεσιών υπολογιστικού νέφους ένα μορφότυπο για να εξηγήσουν τα μέτρα ασφάλειας που λαμβάνουν για να προστατεύσουν τις υπηρεσίες τους».

Αυτή η έκδοση του CCSM έχει εφαρμοστεί ως διαδικτυακό εργαλείο. Το εργαλείο αντιστοιχίζει διαφορετικά συστήματα πιστοποίησης σε ενιαίο κατάλογο στόχων ασφάλειας. Το εργαλείο επιτρέπει στους πελάτες να επιλέξουν τους στόχους ασφάλειας που έχουν μεγαλύτερη σημασία γι' αυτούς, και

1. να δημιουργήσουν μια μήτρα που αντιστοιχίζεται σε διάφορα συστήματα πιστοποίησης για το υπολογιστικό νέφος, ή/και
2. να δημιουργήσουν λίστες ελέγχου προμηθειών ή ερωτηματολόγια ως εκτυπώσεις ή υπολογιστικά φύλλα.

Τα επόμενα βήματα για το CCSM θα είναι να συμπεριληφθούν οι απαιτήσεις NIS άλλων χωρών και να διευρυνθεί το πεδίο εφαρμογής του CCSM ώστε να περιλαμβάνει και τις απαιτήσεις NIS που αφορούν συγκεκριμένα στην προστασία των προσωπικών δεδομένων.

Για την πλήρη έκθεση και το διαδικτυακό εργαλείο: https://resilience.enisa.europa.eu/cloud-computing-certification

Σημειώσεις προς τους συντάκτες:

- Δελτίο Τύπου της Ευρωπαϊκής Επιτροπής: Πρόσκληση υποβολής προσφορών προς τις εταιρείες τεχνολογίας της ΕΕ για την παροχή υπηρεσιών υπολογιστικού νέφους για την ΕΕ http://ec.europa.eu/dgs/informatics/doc/newscloud.pdf
- Νέα λίστα συστημάτων πιστοποίησης για το υπολογιστικό νέφος (CCSL) : http://www.enisa.europa.eu/media/news-items/new-schemes-on-the-cloud-certification-list-1
- Πιστοποίηση στο πλαίσιο της Στρατηγικής της ΕΕ για το υπολογιστικό νέφος: https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy

Για συνεντεύξεις: Δρ. Marnix Dekker, Εμπειρογνώμων στην Ασφάλεια δικτύων και πληροφοριών, και Δήμητρα Λιβέρη, Υπεύθυνη ασφάλειας & ανθεκτικότητας δικτύων επικοινωνίας, στη διεύθυνση cloud.security@enisa.europa.eu