02/04/2012
EPR02/2012
www.enisa.europa.eu

Ασφαλείς προμήθειες: Ο νέος οδηγός της ENISA για την παρακολούθηση των συμβάσεων Υπολογιστικού Νέφους (Cloud Computing)

Οι προμήθειες των υπηρεσιών cloud computing είναι ένα όλο και περισσότερο σημαντικό έργο για τις κυβερνήσεις και επιχειρήσεις ανά την Ευρώπη - και η ασφάλεια των πληροφοριών αποτελεί κεντρικό προβληματικό σημείο. Για να βοηθήσει στην επίλυση αυτού του προβλήματος, η υπηρεσία ηλεκτρονικής ασφάλειας της ΕΕ, ENISA, εγκαινίασε σήμερα ένα νέο, πρακτικό οδηγό για τις ομάδες ηλεκτρονικών προμηθειών, που εστιάζει στη διαρκή παρακολούθηση της ασφάλειας καθόλη τη διάρκεια του κύκλου ζωής μιας σύμβασης.

Η έκδοση βασίζεται στα θεμέλια που έθεσε η ENISA το 2009, όταν ο οργανισμός δημιούργησε ένα πλαίσιο ασφαλείας και εργαλείο για τους υπεύθυνους ανάπτυξης δικτύων προκειμένου να εκτιμήσει την ασφάλεια των παροχέων πριν πάρουν την απόφαση να κινηθούν προς το Υπολογιστικό Νέφος (ΥΝ) ή αλλιώς Cloud Computing (CC). Η ENISA τώρα πάει ένα βήμα παραπέρα, συντάσσοντας έναν λεπτομερή οδηγό στο πώς να παρακολουθεί την ασφάλεια των υπηρεσιών cloud computing καθόλη τη διάρκεια του έργου. Ο νέος οδηγός αφορά στις προμήθειες του Δημοσίου, οι οποίες αντιστοιχούν σχεδόν στο 20% του ΑΕΠ της ΕΕ, περίπου 2,2 τρις. (στοιχεία της Eurostat από το 2009).

Ο καθηγητής Udo Helmbrecht, Εκτελεστικός Διευθυντής του ENISA, σχολιάζει: *«Οι Ευρωπαίοι πολίτες εμπιστεύονται στους δημόσιους και ιδιωτικούς φορείς την προστασία των δεδομένων μας. Με όλο και περισσότερους οργανισμούς να κινούνται προς το* Υπολογιστικό Νέφος *(cloud computing), οι νέες οδηγίες της ENISA έρχονται πάνω στην ώρα για να δώσουν κατευθυντήριες γραμμές σε κάτι που, για τους περισσότερους αγοραστές, είναι ένας πρωτόγνωρος τομέας.»*

Μια πρόσφατη έρευνα της ENISA για τις Υπηρεσίες SLA έδειξε ότι οι περισσότεροι υπεύθυνοι δικτύων στον δημόσιο τομέα σπανίως λαμβάνουν ενημέρωση σε σημαντικούς τομείς ασφαλείας, όπως η διαθεσιμότητα των υπηρεσιών ή οι ευπάθειες του λογισμικού. Ο Οδηγός Ασφαλών Προμηθειών βοηθάει τους καταναλωτές να είναι ικανοί να παρακολουθούν την ασφάλεια σε μόνιμη βάση. *«Ο Οδηγός του ENISA τονίζει τη σημασία της διαρκούς παρακολούθησης της ασφάλειας, σε συνδυασμό με την πιστοποίηση και την διαπίστευση των διαδικασιών»,* λέει ο δόκτωρ Giles Hobgen, συντάκτης της έκθεσης.

Ο οδηγός του ENISA περιλαμβάνει μια λίστα ελέγχου για τις ομάδες προμηθειών, καθώς και μία σε βάθος περιγραφή της κάθε παραμέτρου ασφαλείας: τί πρέπει να μετρηθεί και πώς. Οι παράμετροι ασφαλείας που καλύπτει είναι οι εξής: αντιμετώπιση έκτακτων περιστατικών, ελαστικότητα υπηρεσιών και ανοχή φορτίου, διαχείριση του κύκλου ζωής των δεδομένων, τεχνική συμμόρφωση και διαχείριση ευπάθειας, διοίκηση αλλαγών, απομόνωση δεδομένων και διαχείριση καταγραφής και έρευνας.

02/04/2012

EPR02/2012

www.enisa.europa.eu

Αυτός ο οδηγός συμπληρώνει μια σειρά από έγγραφα που δημοσίευσε η ENISA για το cloud security, που περιλαμβάνει την ευρέως χρησιμοποιούμενη έκθεση του 2009, Το Υπολογιστικό Νέφος (Cloud Computing); Πλεονεκτήματα, Κίνδυνοι και Συστάσεις για την Ασφάλεια των Πληροφοριών.

Πλήρης έκθεση: Αυτή η έκθεση θα παρουσιαστεί αναλυτικά κατά τη διάρκεια του SecureCloud 2012, – τη μοναδική Ευρωπαϊκή διάσκεψη για την ασφάλεια του Υπολογιστικού Νέφους (Cloud Computing).

Για συνεντεύξη: Graeme Cooper, Επικεφαλής Public Affairs, ENISA, press@enisa.europa.eu. Κινητό: + 30 6951 782 268 ή Giles Hogben ή Marnix Dekker, Εμπειρογνώμονας, ENISA, resilience@enisa.europa.eu

Μετάφραση. Η έκδοση στην αγγλική γλώσσα είναι η μόνη έγκυρη.
http://www.enisa.europa.eu/media/enisa-in-greek/
www.enisa.europa.eu