14PROC002328423 2014-10-08

ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΣΤΟ ΜΗΤΡΩΟ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΕΠΙΤΡΟΠΗ ΚΕΦΑΛΑΙΑΓΟΡΑΣ Ν.Π.Δ.Δ.

Διεύθυνση Οικονομικών Υπηρεσιών

Τμήμα Προμηθειών

ΠΛΗΡΟΦΟΡΙΕΣ: Α. Βλάχος
ΤΗΛ.: 2103377185
Fax 2103377173
e-mail a.vlachos@cmc.gov.gr

Πληροφορίες τεχνικού περιεχομένου: Ι. Καφέντζης, 210 3377138, i.kafetzis@cmc.gov.gr.

Αθήνα, 08/10/2014

Αρ. Πρ.: 3658

ΠΡΟΚΗΡΥΞΗ ΠΡΟΧΕΙΡΟΥ ΜΕΙΟΔΟΤΙΚΟΥ ΔΙΑΓΩΝΙΣΜΟΥ

Διενέργεια πρόχειρου μειοδοτικού διαγωνισμού σε ευρώ για το έργο: «Διενέργεια Δοκιμών Παρείσδυσης (vulnerability/penetration test) με στόχο την εκτίμηση του επιπέδου Ασφαλείας των υπό έλεγχο εφαρμογών της Επιτροπής Κεφαλαιαγοράς», σύμφωνα με τις διαδικασίες της περίπτωσης (δ) του άρθρου 4 της κανονιστικής απόφασης 1/491/14.11.2008 της Επιτροπής Κεφαλαιαγοράς Ν.Π.Δ.Δ. «Κανονισμός Προμηθειών της Επιτροπής Κεφαλαιαγοράς Ν.Π.Δ.Δ.» (ΦΕΚ Β΄/2425/1.12.2008).

Η Επιτροπή Κεφαλαιαγοράς, αφού έλαβε υπόψη :

1. Την Απόφαση 7/513/18-06-09 του Διοικητικού Συμβουλίου της Επιτροπής Κεφαλαιαγοράς «Μεταβίβαση αρμοδιοτήτων στην Εκτελεστική Επιτροπή, στους Α' και Β' Αντιπροέδρους, στο Γενικό Διευθυντή και στους Προϊσταμένους Διευθύνσεων, Τμημάτων, Γραφείων και λοιπών Υπηρεσιακών Μονάδων της Επιτροπής Κεφαλαιαγοράς.» (ΦΕΚ Β΄/1279/29.06.2009).
2. Την υπ' αριθ. 8496/Β΄ 3113/13.2.2009 Απόφαση του Υπουργού Οικονομίας και Οικονομικών «Κανονισμός Οικονομικής Διαχείρισης του Ν.Π.Δ.Δ. Επιτροπή Κεφαλαιαγοράς» (ΦΕΚ Β΄/320/23.2.2009) και ειδικότερα τις περιπτώσεις (ζ) και (η) του άρθρου 3 του ως άνω Κανονισμού.
3. Την περ. δ του άρθρου 4 της υπ. αριθμ. 1/491/14-11-08 Απόφασης του Δ.Σ. της Επιτροπής Κεφαλαιαγοράς Ν.Π.Δ.Δ. (ΦΕΚ Β΄ / 2425 / 1-12-08) αναφορικά με την προμήθεια υπηρεσιών και υλικών με συνοπτικές διαδικασίες – πρόχειρος διαγωνισμός όταν η προϋπολογιζόμενη δαπάνη υπολείπεται των ορίων κατώτερης αξίας των κοινοτικών διατάξεων αλλά υπερβαίνει το εκάστοτε όριο ποσού της διαδικασίας της διαπραγμάτευσης – απευθείας ανάθεσης.

14PROC002328423 2014-10-08

4. Το από 08.08.2014 πρωτογενές αίτημα - εισηγητικό σημείωμα του Τμήματος Πληροφορικής της Διεύθυνσης Διοικητικών Υπηρεσιών προς τη Διεύθυνση Οικονομικών Υπηρεσιών (ΑΔΑΜ: 14REQ002236677).
5. Την απόφαση 1/1286/26.09.2014 (ΑΔΑ: 6Ξ7ΑΟΡΡΠ-Δ4Ι) (ΑΔΑΜ: 14REQ002325960) της Εκτελεστικής Επιτροπής της Επιτροπής Κεφαλαιαγοράς Ν.Π.ΔΔ., περί έγκρισης διενέργειας πρόχειρου μειοδοτικού διαγωνισμού για το έργο: «Διενέργεια Δοκιμών Παρείσδυσης (vulnerability/penetration test) με στόχο την εκτίμηση του επιπέδου Ασφαλείας των υπό έλεγχο εφαρμογών της Επιτροπής Κεφαλαιαγοράς», σύμφωνα με τις διαδικασίες της περίπτωσης (δ) του άρθρου 4 της κανονιστικής απόφασης 1/491/14.11.2008 της Επιτροπής Κεφαλαιαγοράς Ν.Π.Δ.Δ. «Κανονισμός Προμηθειών της Επιτροπής Κεφαλαιαγοράς Ν.Π.Δ.Δ.» (ΦΕΚ Β΄/2425/1.12.2008).
6. Το γεγονός ότι η παρούσα δαπάνη θα βαρύνει τον Κωδικό Αριθμό ***Εξόδων 0426 «Αμοιβές ιδιωτικών γραφείων και ιδιωτών για την εκτέλεση μηχανογραφικών εργασιών»*** των προϋπολογισμών της Επιτροπής Κεφαλαιαγοράς των οικονομικών ετών 2014 και 2015 για τον οποίο έχει προβλεφθεί η σχετική πίστωση ως προς το οικονομικό έτος 2014, ενώ θα προβλεφθεί η σχετική πίστωση ως προς το οικονομικό έτη 2015 και θα εκτελεστεί εφόσον δεν υπερβαίνει το 50% των εγγεγραμμένων πιστώσεων στον αντίστοιχο Κωδικό Αριθμό Εξόδου των προϋπολογισμών του οικονομικού έτους 2014, και πάντως για διάστημα όχι πέραν του εξαμήνου, σύμφωνα με την παράγραφο 2 του άρθρου 4 του Ν.Δ. 496/1974 «Περί Λογιστικού των Νομικών Προσώπων Δημοσίου Δικαίου», όπως αυτή αντικαταστάθηκε με το άρθρο 1 του ν. 369/1976 (ΦΕΚ Α΄/164/29.6.1976)
7. Τον Ν. 2286/1995 «Προμήθειες του Δημοσίου Τομέα και ρυθμίσεις συναφών θεμάτων», (ΦΕΚ 19/Α΄/1995).
8. Τον Ν. 2362/1995 «Περί Δημοσίου Λογιστικού Ελέγχου των Δαπανών του Κράτους και άλλες διατάξεις», (ΦΕΚ247/Α΄/1995).
9. Το Π.Δ. 118/2007 (ΦΕΚ 150/Α΄/10-7-2007) «Κανονισμός Προμηθειών του Δημοσίου».

Διενεργεί:

ΠΡΟΧΕΙΡΟ ΔΙΑΓΩΝΙΣΜΟ

με σφραγισμένες προσφορές, συνολικής δαπάνης ύψους έως **€6.000,00 (έξι χιλιάδες ευρώ) μη συμπεριλαμβανομένου του Φ.Π.Α. 23%**, (€7.380,00 συμπεριλαμβανομένων του Φ.Π.Α. 23% και όλων των νόμιμων κρατήσεων), για το έργο: «Διενέργεια Δοκιμών Παρείσδυσης (vulnerability/penetration test) με στόχο την εκτίμηση του επιπέδου Ασφαλείας των υπό έλεγχο εφαρμογών της Επιτροπής Κεφαλαιαγοράς».

CPV: 72254100-1 «Υπηρεσίες δοκιμής συστημάτων πληροφορικής»

Η ανάδειξη της μειοδότριας εταιρίας θα γίνει με κριτήριο την **ΧΑΜΗΛΟΤΕΡΗ ΤΙΜΗ**. Επισημαίνεται ότι η εν λόγω δαπάνη υπόκειται στις εξής κρατήσεις:

i. Επί της καθαρής τιμολογιακής αξίας ποσοστό κρατήσεων 3,072% (υπέρ Μ.Τ.Π.Υ. μετά του αναλογούντος χαρτοσήμου και ΟΓΑ χαρτοσήμου)

ii. Επί της καθαρής τιμολογιακής αξίας και αφαιρουμένου του συνόλου των παραπάνω κρατήσεων γίνεται παρακράτηση φόρου εισοδήματος σε ποσοστό 8% για την παροχή υπηρεσιών, σύμφωνα με το άρθρο 24 του ν.2198/94 (ΦΕΚ 43 Α/ 22.3.94).

iii. Επί της καθαρής τιμολογιακής αξίας ποσοστό κρατήσεων 0,10% για τις λειτουργικές ανάγκες της Ενιαίας Ανεξάρτητης Αρχής Δημοσίων Συμβάσεων, σύμφωνα με τη παράγραφο 3 του άρθρου 4 του Ν. 4013/2011 (ΦΕΚ Α' / 204/15.09.2011)

Οι μεν παραπάνω κρατήσεις βαρύνουν το μειοδότη, ο δε Φ.Π.Α. βαρύνει την Επιτροπή Κεφαλαιαγοράς Ν.Π.Δ.Δ.

Κατόπιν της κατακύρωσης υπογράφεται σύμβαση έργου με τον μειοδότη. Η εκτέλεση κάθε κύκλου του έργου θα πρέπει να έχει ολοκληρωθεί σε δεκαπέντε (15) ημερολογιακές ημέρες από την έναρξη τους, πάντα κατόπιν γραπτής ειδοποίησης από το Τμήμα Πληροφορικής. Η έκδοση των τιμολογίων από τον ανάδοχο γίνεται κατόπιν της υπογραφής της σύμβασης έργου και της οριστικής παραλαβής των παραδοτέων κάθε κύκλου της προκήρυξης. Η πληρωμή του 50% της αξίας της έργου θα γίνεται μετά την οριστική παραλαβή των παραδοτέων κάθε κύκλου του έργου της προκήρυξης, από την αρμόδια Επιτροπή Παραλαβών της Επιτροπής Κεφαλαιαγοράς Ν.Π.Δ.Δ. στην έδρα της Επιτροπής Κεφαλαιαγοράς (Κολοκοτρώνη 1 & Σταδίου, 10562 Αθήνα), όπως ακριβώς ορίζονται στο Παράρτημα Α' (άρθρο 9).

I. Σε περίπτωση ενδιαφέροντος, η οικονομική προσφορά καθώς και η τεχνική πρόσφορα σύμφωνα με τα οριζόμενα στην παρούσα, θα πρέπει να υποβληθούν μέχρι την καταληκτική ημερομηνία του διαγωνισμού, ήτοι την **Πέμπτη 23/10/2014,** και ώρα **11.00 πμ,** υπόψη **κ. ΣΑΒΒΙΔΗ ΙΩΑΝΝΗ** στο Πρωτόκολλο της ΕΠΙΤΡΟΠΗΣ ΚΕΦΑΛΑΙΑΓΟΡΑΣ, **(1ος όροφος, Κολοκοτρώνη 1 & Σταδίου, 10562 Αθήνα)**, μέσα σε **ΕΝΑΝ ΕΝΙΑΙΟ ΚΛΕΙΣΤΟ ΚΑΙ ΣΦΡΑΓΙΣΜΕΝΟ** φάκελο στον οποίο θα αναγράφονται ευκρινώς τα ακόλουθα:

i. Η ένδειξη "**ΠΡΟΣΟΧΗ - ΝΑ ΜΗΝ ΑΝΟΙΧΘΕΙ Ο ΦΑΚΕΛΟΣ**" με κεφαλαία γράμματα
ii. Η λέξη "**ΟΙΚΟΝΟΜΙΚΗ ΠΡΟΣΦΟΡΑ**" με κεφαλαία γράμματα
iii. **Υπόψη κ. ΣΑΒΒΙΔΗ ΙΩΑΝΝΗ.**
iv. **ΤΑ ΣΤΟΙΧΕΙΑ ΤΟΥ ΑΠΟΣΤΟΛΕΑ**
v. Αφορά: **Διαγωνισμό για το έργο:** «**Διενέργεια Δοκιμών Παρείσδυσης (vulnerability/penetration test) με στόχο την εκτίμηση του επιπέδου Ασφαλείας των υπό έλεγχο εφαρμογών της Επιτροπής Κεφαλαιαγοράς»**

Επισημαίνεται ότι όλες οι προσφορές πρέπει να είναι υπογεγραμμένες και σφραγισμένες, η δε οικονομική προσφορά, πρέπει να βρίσκεται σε ξεχωριστό κλειστό και σφραγισμένο φάκελο, εντός του ως άνω ΕΝΙΑΙΟΥ ΚΛΕΙΣΤΟΥ ΚΑΙ ΣΦΡΑΓΙΣΜΕΝΟΥ ΦΑΚΕΛΟΥ. Προσφορές που κατατίθενται μετά την παραπάνω ημερομηνία και ώρα, θεωρούνται εκπρόθεσμες και επιστρέφονται.

II. Η διενέργεια του διαγωνισμού θα πραγματοποιηθεί από την αρμόδια Επιτροπή Αξιολόγησης Διαγωνισμών (Ε.Α.Δ.) της Επιτροπής Κεφαλαιαγοράς Ν.Π.Δ.Δ.. Η αποσφράγιση των προσφορών γίνεται δημόσια από την αρμόδια επιτροπή την

καταληκτική ημερομηνία και ώρα κατάθεσης των προσφορών στα γραφεία της Επιτροπής Κεφαλαιαγοράς**,** Κολοκοτρώνη 1 και Σταδίου, Αθήνα, ΤΚ 10562, παρουσία όσων εκ τους προσφέροντες ή των νομίμως εξουσιοδοτημένων εκπροσώπων τους, το επιθυμούν. Η εξέταση των περιεχομένων των προσφορών από τους συμμετέχοντες θα γίνει κατά την διαδικασία αποσφράγισης των προσφορών, χωρίς την απομάκρυνσή τους από το χώρο της Επιτροπής Κεφαλαιαγοράς και χωρίς να επιτρέπεται η φωτοαντιγραφή. Ο έλεγχος και η αξιολόγηση των προσφορών γίνεται από την αρμόδια Επιτροπή σε κλειστές συνεδριάσεις. Η Επιτροπή Αξιολόγησης Διαγωνισμών μετά την υποβολή των προσφορών στα πλαίσια πρόχειρων διαγωνισμών ελέγχει την συμβατότητα των τεχνικών προσφορών με τις ζητούμενες τεχνικές προδιαγραφές και αποκλείει τυχόν αποκλίνουσες προσφορές. Οι προσφορές που γίνονται τεχνικοοικονομικά αποδεκτές καταχωρούνται σε σχετικό πίνακα κατά σειρά μειοδοσίας. **Η κατακύρωση γίνεται στην προσφορά με την χαμηλότερη τιμή.** Τυχόν ζητούμενες διευκρινίσεις από τους προσφέροντες ζητούνται και παρέχονται εγγράφως. Σε περίπτωση ισότιμων προσφορών η Επιτροπή Αξιολόγησης έχει την διακριτική ευχέρεια είτε να κατανείμει μεταξύ των περισσοτέρων το έργο, είτε, εφόσον το έργο δεν είναι διαιρετό, να επιλέξει το μειοδότη κατόπιν διαπραγμάτευσης αφού κληθούν όλοι οι προσφέροντες που είχαν ισότιμες προσφορές.

III. Οι προσφέροντες υποχρεούνται με την προσφορά τους να καταθέσουν Υπεύθυνη Δήλωση της παρ. 4 του άρθρου 8 του ν. 1599/1986 υπογεγραμμένη και νομίμως επικυρωμένη ως προς το γνήσιο της υπογραφής, στην οποία θα δηλώνονται τα εξής:

i. Έλαβα γνώση των όρων του διαγωνισμού τους οποίους και αποδέχομαι.
ii. Δεν υπάρχουν νομικοί περιορισμοί στη λειτουργία της Επιχείρησης.
iii. Δεν έχω αποκλεισθεί, από την συμμετοχή σε διαγωνισμούς του Δημοσίου.
iv. Δεν έχω κάνει ψευδείς ή ανακριβείς δηλώσεις κατά την παροχή πληροφοριών που ζητούνται από την Υπηρεσία
v. Δεν έχω υποπέσει σε σοβαρά παραπτώματα κατά την άσκηση της επαγγελματικής μου δραστηριότητας.
vi. Θα είμαστε συνεπείς στην εκπλήρωση των συμβατικών μας υποχρεώσεων που ζητούνται από την Υπηρεσία.

Η μη προσκόμιση των παραπάνω δικαιολογητικών, αλλά και η διαπίστωση κατά τον έλεγχο σοβαρής ανειλικρίνειας των στοιχείων συνεπάγεται τον αποκλεισμό από τον διαγωνισμό. Προς διευκόλυνση των ενδιαφερομένων το κείμενο της προκήρυξης διατίθεται σε ηλεκτρονική μορφή από την ιστοσελίδα της Επιτροπής Κεφαλαιαγοράς, **www.hcmc.gr.** Τόσο η προκήρυξη, όσο και η σχετική για την διενέργεια του διαγωνισμού απόφαση της Εκτελεστικής Επιτροπής της Επιτροπής Κεφαλαιαγοράς Ν.Π.Δ.Δ. έχουν αναρτηθεί στον ιστότοπο των προγραμμάτων: ΔΙΑΥΓΕΙΑ (αρθ. 2 ν.3861/2010, ΦΕΚ Α΄/112/13.07.2010) και Κ.Η.Μ.ΔΗ.Σ. (αρθ.11 ν.4013/2011, ΦΕΚ Α΄/204/15.09.2011 και αρθ. 3 Π1/2380/18.12.2012, ΦΕΚ Β'/3400/20.12.2012). **Για κάθε διευκρίνιση επί του αντικειμένου του έργου, οι ενδιαφερόμενοι μπορούν να επικοινωνούν με τον κ. Καφέντζη Ιωάννη 210 – 3377138 (i.kafetzis@cmc.gov.gr)**

Ώρες επικοινωνίας: 10.00 πμ – 14.00 μμ

IV. Ειδικότερα, επισημαίνονται τα ακόλουθα:

i. Η συμμετοχή στο διαγωνισμό προϋποθέτει και αποτελεί τεκμήριο ότι κάθε διαγωνιζόμενος έχει λάβει πλήρη γνώση και έχει αποδεχθεί ανεπιφύλακτα το

σύνολο των όρων που περιλαμβάνονται στην Προκήρυξη και στα Παραρτήματα Α΄ και Β΄ αυτής.

ii. Οι συμμετέχουσες εταιρείες έχουν υποχρέωση - επί ποινή αποκλεισμού - να καταθέσουν μία ενιαία προσφορά για το σύνολο των υπό προμήθεια υπηρεσιών, καθότι θα υπάρξει ένας και μόνο μειοδότης.

iii. Η ανάδειξη του μειοδότη θα γίνει με κριτήριο τη χαμηλότερη τιμή, η οποία θα εκφράζεται σε Ευρώ και θα είναι **μία και ενιαία για το σύνολο του έργου** μη συμπεριλαμβανομένου του ΦΠΑ. **Ο ΦΠΑ θα δίδεται σε ξεχωριστή στήλη.**

iv. Προσφορές που το τίμημά τους υπερβαίνει την προϋπολογισθείσα δαπάνη θα απορρίπτονται.

v. Ο χρόνος ισχύος των προσφορών είναι εκατόν είκοσι (120) ημερολογιακές ημέρες, προσμετρούμενες από την επόμενη της ημέρας διενέργειας του διαγωνισμού.

V. Ενστάσεις – Προσφυγές υποβάλλονται για τους λόγους και με τη διαδικασία που προβλέπεται από το άρθρο 15 του Π.Δ. 118/2007 (ΦΕΚ 150/Α΄/10-7-2007) «Κανονισμός Προμηθειών του Δημοσίου», στην αρμόδια Επιτροπή Αξιολόγησης Ενστάσεων (Ε.Α.Ε.) της Επιτροπής Κεφαλαιαγοράς Ν.Π.Δ.Δ.

Ο Προϊστάμενος της Διεύθυνσης
Οικονομικών Υπηρεσιών

Γ Ε Ω Ρ Γ Ι Ο Σ Κ Ο Κ Κ Ο Β Α Σ

14PROC002328423 2014-10-08

ΠΑΡΑΡΤΗΜΑ Α΄
ΟΡΟΙ ΚΑΙ ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

1. Σκοπός Τεχνικών Προδιαγραφών Έργου:

Σκοπός των τεχνικών προδιαγραφών είναι να περιγράψουν τις απαιτήσεις της Επιτροπής Κεφαλαιαγοράς (ΕΚ) με στόχο την πρόσκληση για κατάθεση τεχνικής και οικονομικής προσφοράς, σχετικά με την διενέργεια Δοκιμών Παρείσδυσης (vulnerability/penetration test) με στόχο την εκτίμηση του επιπέδου Ασφάλειας των υπό έλεγχο εφαρμογών.

2. Στόχος Έργου:

Η ΕΚ στο πλαίσιο αναβάθμισης των υπηρεσιών που προσφέρει, στοχεύει τόσο στη βελτίωση αυτών, όσο και στη δυνατότητα συνολικής διαχείρισης των κινδύνων που αυτές τυχόν περικλείουν, λόγω της φύσης των δραστηριοτήτων και των τεχνολογικών υποδομών του οργανισμού.

Η ΕΚ επιθυμεί την περιγραφή και ανάλυση των ευπαθειών και κινδύνων των δικτυακών εφαρμογών (Web Applications) καθώς και να περιγράψει τις επιπτώσεις τους, ώστε να μπορέσει να καλύψει τις σημερινές ανάγκες, επισημαίνοντας τα τυχόν προβλήματα και ευπάθειες των δικτυακών εφαρμογών και προτείνοντας τρόπους αντιμετώπισης τους.

Για το σκοπό αυτό η ΕΚ, προκηρύσσει διαγωνισμό για την επιλογή μελετητή, ο οποίος θα αναλάβει την εκπόνηση της παραπάνω μελέτης.

3. Αντικείμενο Έργου

Κατά το παρόν έργο ο ανάδοχος θα πρέπει να διεξάγει δοκιμές παρείσδυσης στις δικτυακές εφαρμογές της ΕΚ (Penetration Testing) και να παραδώσει αναφορά για τις δοκιμές αυτές που θα περιλαμβάνουν τα πιθανά ευρήματα ασφάλειας, τις επιπτώσεις αυτών καθώς και προτεινόμενες ενέργειες αντιμετώπισής τους. Οι εφαρμογές που θα ελεγχθούν αναφέρονται σε δύο (2) δικτυακούς τόπους.

Ο Ανάδοχος θα πρέπει να προβεί σε εκτέλεση δοκιμών παρείσδυσης στις προαναφερόμενες WEB εφαρμογές οι οποίες βρίσκονται σε λειτουργία σε δύο ιστοτόπους. Οι δοκιμές αυτές σκοπό έχουν να εξασφαλίσουν στην ΕΚ καλύτερη κατανόηση των αδυναμιών των εφαρμογών με στόχο την προστασία αυτών από ενδεχόμενες επιθέσεις που μπορεί να εκτελεσθούν από το διαδίκτυο.

Ειδικότερα, ο ανάδοχος θα πρέπει να εκτελέσει δοκιμές στις δικτυακές εφαρμογές ως εξής:

a) Δοκιμές Παρείσδυσης (Penetration Test) Χωρίς Γνώση (Black Box) σε επίπεδο εφαρμογής. Σε αυτή την φάση ο ανάδοχος θα εκτελέσει τις δοκιμές παρείσδυσης

γνωρίζοντας μόνο τη δικτυακή διεύθυνση της εφαρμογής.

b) Δοκιμές Παρείσδυσης (Penetration Test) Με Γνώση (White Box) σε επίπεδο εφαρμογής. Στην παρούσα φάση υλοποίησης του έργου οι τεχνικοί έλεγχοι θα πραγματοποιηθούν με συγκεκριμένα δικαιώματα χρήστη και με χρήση διαβαθμισμένων ρόλων, όπως αυτοί θα ορισθούν από την ΕΚ. Συγκεκριμένα θα δημιουργηθούν δοκιμαστικοί λογαριασμοί (test accounts) που θα αντιπροσωπεύουν έναν απλό χρήστη των εφαρμογών καθώς και ένα χρήστη με δικαιώματα διαχειριστή.

Ο Ανάδοχος αφού παραδώσει τα ευρήματα των δοκιμών, θα πραγματοποιήσει και δεύτερο κύκλο ελέγχων, ώστε να διαπιστωθεί αν διορθώθηκαν τα ευρήματα της πρώτης φάσης ελέγχων (retesting activities).

4. Προδιαγραφές Ελέγχων

Τα ειδικά εργαλεία που θα χρησιμοποιηθούν για την εκτέλεση του έργου θα πρέπει να περιγραφούν αναλυτικά στην προσφορά. Ο ανάδοχος θα πρέπει να υποβάλλει ενδεικτικές και αντιπροσωπευτικές οθόνες, εκτυπώσεις από τα εν λόγω εργαλεία ενώ παράλληλα θα πρέπει να παραδώσει δειγματοληπτικές αναφορές από άλλα παρόμοια έργα.

Επιπρόσθετα οι εκτελούμενες δοκιμές και έλεγχοι παρείσδυσης δε θα βασίζονται μόνο σε διαθέσιμους στο εμπόριο ανιχνευτές ασφάλειας και σε αυτοματοποιημένα εργαλεία αλλά και σε προσαρμοσμένα μοντέλα επίθεσης για της ανάγκες της συγκεκριμένης εφαρμογής.

Επιπρόσθετα, ο υποψήφιος ανάδοχος θα πρέπει να εκτελέσει μεταξύ άλλων τους παρακάτω ελέγχους:

- OWASP Top10 Vulnerabilities
- Συλλογή πληροφοριών
- Επίθεση στους διακομιστές ιστού
- Επιθέσεις στους μηχανισμούς πιστοποίησης αυθεντικότητας
- Επιθέσεις στο σχήμα εξουσιοδότησης
- Επιθέσεις στο κανάλι σύνδεσης δεδομένων
- Επιθέσεις στους χρήστες του portal
- Επιθέσεις άρνησης πρόσβασης (DoS)
- Επιθέσεις Cross Site Request Forgery
- Έλεγχος ευπαθειών που σχετίζονται με την επιχειρησιακή λογική της εφαρμογής (business logic).

Παραδοτέα

Δοκιμές Παρείσδυσης Χωρίς Γνώση/Με Γνώση

Αναφορά δοκιμών η οποία θα πρέπει να περιλαμβάνει κατ' ελάχιστο τα εξής:

- Γενική Αποτίμηση της Ασφάλειας της εφαρμογής
- Σύντομη περιγραφή της εφαρμοσθείσας μεθοδολογίας.
- Λίστα με τα πιο κρίσιμα ευρήματα και τις επιπτώσεις τους σε επιχειρησιακό και τεχνικό επίπεδο.
- Συνοπτικό πλάνο ενεργειών που θα περιλαμβάνει τις ενέργειες για την επίλυση και την διαχείριση των προσδιορισμένων ρίσκων ασφάλειας.
- Για κάθε εύρημα:
  - Ευπάθεια
  - Κατάταξη κατά κρισιμότητα
  - Ευκολία ανακάλυψης
  - Τρόπος ανακάλυψης
  - Δυνατότητα εκμετάλλευσης
  - Επιχειρησιακές και τεχνικές επιπτώσεις
  - Προτεινόμενες επιδιορθωτικές κινήσεις
  - Πλήρη λίστα των εργαλείων που χρησιμοποιήθηκαν.

5. Φάκελος Τεχνική Προσφορά

Στο φάκελο Τεχνικής Προσφοράς θα πρέπει να περιλαμβάνονται:

- Τα γενικά χαρακτηριστικά της προτεινόμενης μεθοδολογίας και των προϊόντων που την υποστηρίζουν
- Λεπτομερή και κατανοητή περιγραφή της μελέτης (της μεθοδολογίας και του λογισμικού και της συμβολής καθενός από αυτά στη λύση).
- Τα παραδοτέα της μελέτης
- Χρονοδιάγραμμα υλοποίησης
- Ομάδα υλοποίησης
- Αναφορά εκτελεσθέντων παρόμοιων έργων στην Ελλάδα
- Πιστοποίηση κατά ISO27001
- Πιστοποίηση κατά ISO9001
- Υπεύθυνη Δήλωση υπογεγραμμένη και νομίμως επικυρωμένη από νόμιμο εκπρόσωπο της εταιρείας, ως προς το γνήσιο της υπογραφής, στην οποία θα δηλώνεται ότι ο υποψήφιος ανάδοχος έχει πέντε (5) χρόνια τουλάχιστον εμπειρία σε παρόμοια έργα

- Τουλάχιστον τρείς (3) Βεβαιώσεις εταιρειών – οργανισμών (πελατών της), στις οποίες να αναφέρεται σαφώς η επιτυχής εκτέλεση και οριστική παραλαβή, παρόμοιων έργων, κατά την διάρκεια των τριών (3) τελευταίων ετών.

6. Φάκελος Οικονομικής Προσφοράς

Στο φάκελο της Οικονομικής Προσφοράς θα πρέπει να περιέχονται:

- Συνολική Τιμή (πλέον Φ.Π.Α. 23%) και για τους (2) δύο κύκλους ελέγχων (Αρχικό και επαναληπτικό)
- Φ.Π.Α. 23% σε ξεχωριστή στήλη

7. Κριτήρια Αξιολόγησης Προσφορών

Οι προσφορές θα αξιολογηθούν **επί ποινή αποκλεισμού**, με βάση τα παρακάτω κριτήρια:

- Πληρότητα φακέλου Τεχνικής Προσφοράς (Άρθρο 6 Παραρτήματος Α')
- Πίνακα Συμμόρφωσης (Παράρτημα Β')

8. Έναρξη, διάρκεια και πληρωμή έργου

Η έναρξη του έργου (1ος κύκλος) θα γίνει, αφού υπογραφτεί η σχετική σύμβαση, κατόπιν σχετικής γραπτής ειδοποίησης από το Τμήμα Πληροφορικής της Ε.Κ.

Η αποστολή της ειδοποίησης θα γίνει διαμέσου ηλεκτρονικού ταχυδρομείου (email) ή μηχανήματος τηλεομοιοτυπίας (fax).

Στη συνέχεια, αφού παραδώσει τα παραδοτέα (ευρήματα) του 1ου κύκλου, με νέα σχετική γραπτή ειδοποίηση, θα προχωρήσει στον 2ο κύκλο του έργου, για να διαπιστωθεί εάν έχουν διορθωθεί τα ευρήματα του 1ου κύκλου.

Η διάρκεια κάθε κύκλου δεν θα πρέπει να υπερβαίνει τις 15 ημερολογιακές ημέρες.

Διάρκεια του κύκλου νοείται το χρονικό διάστημα από την λήψη της γραπτής ειδοποίησης έως και την παράδοση των παραδοτέων του άρθρου 5 του παρόντος Παραρτήματος.

Η πληρωμή του ποσού έργου θα γίνει σε δύο (2) δόσεις, με την έκδοση σχετικών τιμολογίων ως εξής:

- Το 50% με την παράδοση των παραδοτέων του 1ου κύκλου και την παραλαβή τους από την Επιτροπή Παραλαβής Προμηθειών (Ε.Π.Π.) της Ε.Κ.
- Το υπόλοιπο 50% με την παράδοση των παραδοτέων του 2ου κύκλου και την παραλαβή τους από την Ε.Π.Π. της Ε.Κ.

14PROC002328423 2014-10-08

ΠΑΡΑΡΤΗΜΑ Β΄ - ΠΙΝΑΚΑΣ ΣΥΜΟΡΦΩΣΗΣ

α/α	Προδιαγραφή	Επιθυμητή /Απαιτητή	Απάντηση Ναι/Όχι	Παραπομπή
1	Δοκιμές Παρείσδυσης (Penetration Test) Χωρίς Γνώση (Black Box) σε επίπεδο εφαρμογής. Σε αυτή την φάση ο ανάδοχος θα εκτελέσει τις δοκιμές παρείσδυσης γνωρίζοντας μόνο τη δικτυακή διεύθυνση της εφαρμογής.	Απαιτητή		
2	Δοκιμές Παρείσδυσης (Penetration Test) Με Γνώση (White Box) σε επίπεδο εφαρμογής. Στην παρούσα φάση υλοποίησης του έργου οι τεχνικοί έλεγχοι θα πραγματοποιηθούν με συγκεκριμένα δικαιώματα χρήστη και με χρήση διαβαθμισμένων ρόλων, όπως αυτοί θα ορισθούν από την ΕΚ. Συγκεκριμένα θα δημιουργηθούν δοκιμαστικοί λογαριασμοί (test accounts) που θα αντιπροσωπεύουν έναν απλό χρήστη των εφαρμογών καθώς και ένα χρήστη με δικαιώματα διαχειριστή.	Απαιτητή		
3	Αριθμός κύκλων ελέγχου: Δύο (2). (Πριν και μετά τις τυχόν διορθώσεις και στους δύο (2) διαδικτυακούς τόπους)	Απαιτητή		
4	Να περιγραφούν τα ειδικά εργαλεία που θα χρησιμοποιηθούν για την εκτέλεση του έργου.	Απαιτητή		
5	Οι εκτελούμενες δοκιμές και έλεγχοι παρείσδυσης θα βασίζονται τόσο σε διαθέσιμους στο εμπόριο ανιχνευτές ασφάλειας και σε αυτοματοποιημένα εργαλεία όσο και σε προσαρμοσμένα μοντέλα επίθεσης για της ανάγκες της συγκεκριμένης εφαρμογής.	Απαιτητή		

-	**Ο υποψήφιος ανάδοχος θα πρέπει να εκτελέσει κατ' ελάχιστον τους παρακάτω ελέγχους:**	-	-	-
6	OWASP Top10 Vulnerabilities	Απαιτητή		
7	Συλλογή πληροφοριών	Απαιτητή		
8	Επίθεση στους διακομιστές ιστού	Απαιτητή		
9	Επιθέσεις στους μηχανισμούς πιστοποίησης αυθεντικότητας	Απαιτητή		
10	Επιθέσεις στο σχήμα εξουσιοδότησης	Απαιτητή		
11	Επιθέσεις στο κανάλι σύνδεσης δεδομένων	Απαιτητή		
12	Επιθέσεις στους χρήστες του portal	Απαιτητή		
13	Επιθέσεις άρνησης πρόσβασης (DoS)	Απαιτητή		
14	Επιθέσεις Cross Site Request Forgery	Απαιτητή		
15	Έλεγχος ευπαθειών που σχετίζονται με την επιχειρησιακή λογική της εφαρμογής (business logic).	Απαιτητή		
16	Παράδοση αναφοράς δοκιμών η οποία θα πρέπει να περιλαμβάνει κατ' ελάχιστο τα εξής: Γενική Αποτίμηση της Ασφάλειας της εφαρμογής Σύντομη περιγραφή της εφαρμοσθείσας μεθοδολογίας. Λίστα με τα πιο κρίσιμα ευρήματα και τις επιπτώσεις τους σε επιχειρησιακό και τεχνικό επίπεδο. Συνοπτικό πλάνο ενεργειών που θα περιλαμβάνει τις ενέργειες για την επίλυση και την διαχείριση των προσδιορισμένων ρίσκων ασφάλειας. Για κάθε εύρημα: Ευπάθεια Κατάταξη κατά κρισιμότητα Ευκολία ανακάλυψης Τρόπος ανακάλυψης Δυνατότητα εκμετάλλευσης Επιχειρησιακές και τεχνικές επιπτώσεις Προτεινόμενες επιδιορθωτικές κινήσεις Πλήρη λίστα των εργαλείων που χρησιμοποιήθηκαν	Απαιτητή		