



22PROC010497273 2022-05-05

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΕΡΙΦΕΡΕΙΑ ΑΝΑΤ. ΜΑΚΕΔΟΝΙΑΣ-ΘΡΑΚΗΣ
ΓΕΝ. Δ/ΝΣΗ ΕΣΩΤΕΡΙΚΗΣ ΛΕΙΤΟΥΡΓΙΑΣ
Δ/ΝΣΗ ΔΙΑΦΑΝΕΙΑΣ & ΗΛΕΚΤΡΟΝ.
ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΠΕ ΚΑΒΑΛΑΣ
ΤΚ : 651 10 ΚΑΒΑΛΑ
Πληροφορίες : Ευριπίδης Ζαϊμίδης
Τηλέφωνο : 2513 503332-3
Fax : 2513 503344
e - mail : plirkav@pamth.gov.gr
eyrisz@pamth.gov.gr
ο δ ό ς : Εθνικής Αντίστασης 20

ΠΡΟΣ : 1. Όλους τους ενδιαφερομένους.

ΠΡΟΣΚΛΗΣΗ ΕΚΔΗΛΩΣΗΣ ΕΝΔΙΑΦΕΡΟΝΤΟΣ

ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ

ΠΑΜΘ / ΠΕ ΚΑΒΑΛΑΣ / ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΚΡΙΤΗΡΙΟ ΚΑΤΑΚΥΡΩΣΗΣ

ΧΑΜΗΛΟΤΕΡΗ ΤΙΜΗ

48760000-3

CPV

Πακέτα λογισμικού προστασίας από ιούς

ΑΔΑ ΑΠΟΦΑΣΗΣ ΑΝΑΛΗΨΗΣ ΥΠΟΧΡΕΩΣΗΣ

6ΘΧΔ7ΛΒ-Λ7Υ

ΑΔΑΜ ΕΓΚΕΚΡΙΜΕΝΟΥ ΑΙΤΗΜΑΤΟΣ

ΑΔΑΜ_ 22REQ010459154 2022-04-27

ΚΩΔ. ΠΡΟΥΠΟΛΟΓΙΣΜΟΥ

3072.1723.0001

ΣΥΝΟΛΙΚΗ ΠΡΟΫΠΟΛΟΓΙΘΕΙΣΑ ΔΑΠΑΝΗ

ΣΥΝΟΛΟ: 4.216,00 ΜΕ Φ.Π.Α.

ΚΑΤΑΛΗΚΤΙΚΟΣ ΧΡΟΝΟΣ ΥΠΟΒΟΛΗΣ
ΠΡΟΣΦΟΡΩΝ

ΗΜΕΡΟΜΗΝΙΑ: 12/05/2022 ΚΑΙ ΩΡΑ: 10:00

Ανακοινώνεται ότι, η Περιφέρεια Ανατολικής Μακεδονίας Θράκης (Τμήμα Πληροφορικής ΠΕ Καβάλας) στα πλαίσια της εύρυθμης και απρόσκοπτης λειτουργία όλων των Υπηρεσιών που στεγάζονται στο Διοικητήριο της Π.Ε. Καβάλας, θα δεχτεί οικονομικές προσφορές με κριτήριο κατακύρωσης τη χαμηλότερη τιμή για την προμήθεια **ανανέωσης ESET ENDPOINTPROTECTION NEW 2 YEARS 200 αδειών χρήσης Λογισμικού προστασίας (Antivirus)** για το σύνολο των **Η/Υ της Περιφερειακής Ενότητας Καβάλας** με τις παρακάτω προδιαγραφές όπως αυτές περιγράφεται παρακάτω :

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ ΤΕΚΜΗΡΙΩΣΗΣ
1	Γενικά			
1.1	Να αναφερθεί ο κατασκευαστής και το όνομα/έκδοση του λογισμικού προστασίας από ιούς.	ΝΑΙ		
1.2	Το λογισμικό προστασίας να υποστηρίζει τα εξής λειτουργικά συστήματα: MS Windows 8, 10 MS Windows Server 2008, 2012, 2016 Linux (kernel 2.6.x και νεότερο), MAC OS X	ΝΑΙ		
1.3	Οι ελάχιστες απαιτήσεις συστήματος να είναι 0.3 GB ελεύθερη διαθέσιμη μνήμη (RAM) και 1 GB ελεύθερος χώρος στον σκληρό δίσκο.	ΝΑΙ		
2	Αντιική Προστασία			
2.1	Η εγκατάσταση της κεντρικής βάσης malware θα γίνει σε server στο εσωτερικό δίκτυο του φορέα και όχι σε εξωτερικό δίκτυο (πχ στο cloud ή σε server που είναι εγκατεστημένος σε server εκτός εγκαταστάσεων του φορέα). Να προσφερθούν όλα τα απαραίτητα για τον εν λόγω server (φυσικό ή εικονικό).	ΝΑΙ		
2.2	Να υπάρχει η δυνατότητα ο κεντρικός Server να παρασχεθεί σε μορφή εικονικής μηχανής (VM Appliance).	ΝΑΙ		
2.3	Να υποστηρίζεται ανίχνευση και καθαρισμός όλων των τύπων απειλών malware: viruses, malware, trojans, dialers, spyware, jokes, hoaxes, ransomware.	ΝΑΙ		
2.4	Να υποστηρίζεται αυτόματη ανίχνευση και καθαρισμός των προαναφερθέντων απειλών σε πραγματικό χρόνο.	ΝΑΙ		
2.5	Να υποστηρίζεται on-demand ανίχνευση και καθαρισμός των προαναφερθέντων απειλών.	ΝΑΙ		
2.6	Να υποστηρίζεται IPS (intrusion prevention system).	ΝΑΙ		
2.7	Να υποστηρίζονται τεχνολογίες advanced heuristics (ενδεικτικά: DNA, smart signatures, Behavioral Analysis) για δυνατότητα ανίχνευσης άγνωστου malware.	ΝΑΙ		
2.8	Προστασία για SSL/TLS filtering στα πρωτόκολλα HTTPS, IMAPS, POP3S.	ΝΑΙ		
2.9	Δυνατότητα αποτροπής γνωστών exploits	ΝΑΙ		
2.10	Δυνατότητα μπλοκαρίσματος όλων των σελίδων του Internet σε ένα client καθώς και διαχείριση των σελίδων που μπορούν να είναι διαθέσιμες στο χρήστη ανά κατηγορία, π.χ. αποτροπή επίσκεψης σε σελίδες social media, streaming videos.	ΝΑΙ		
2.11	Δυνατότητα προστασίας σε δικτυακό επίπεδο με client based Firewall, με δυνατότητα φιλτραρίσματος σε επίπεδο θυρών και εφαρμογών σε εισερχόμενες και εξερχόμενες συνδέσεις.	ΝΑΙ		
2.12	Δυνατότητα προστασίας από δικτυακές απειλές και botnets	ΝΑΙ		
2.13	Δυνατότητα ενιαίας καραντίνας αρχείων που ανιχνεύθηκαν για όλο το δίκτυο, με δυνατότητες προβολής clients ανά απειλή, εξαγωγή και εξαίρεση	ΝΑΙ		
2.14	Δυνατότητα προστασίας απο Brute Force Attack	ΝΑΙ		
3	Κεντρική διαχείριση			
3.1	Να υποστηρίζεται η κεντρική διαχείριση όλων των λογισμικών προστασίας των σταθμών εργασίας / servers (antivirus client) μέσω κεντρικής κονσόλας.	ΝΑΙ		
3.2	Να υποστηρίζεται η δημιουργία πολλαπλών ομάδων με δυνατότητα εφαρμογής διαφορετικών πολιτικών / ρυθμίσεων για κάθε ομάδα.	ΝΑΙ		

3.3	Λειτουργία προσωρινής απενεργοποίησης πολιτικής ανά client	NAI		
3.4	Να υποστηρίζεται η διαχείριση των ιστοσελίδων (επιτρεπόμενες, μη επιτρεπόμενες) σε ένα σταθμό εργασίας / server όπου είναι εγκατεστημένος ο antivirus client.	NAI		
3.5	Να υποστηρίζεται η αυτόματη ανίχνευση των σταθμών εργασίας που βρίσκονται στο τοπικό δίκτυο δεδομένων ακόμα κι αν αυτά δεν ανήκουν σε υπηρεσία ενεργού καταλόγου.	NAI		
3.6	Να υποστηρίζεται η εγκατάσταση και απεγκατάσταση του λογισμικού προστασίας (antivirus client) μέσω της κεντρικής κονσόλας.	NAI		
3.7	Να υποστηρίζεται ενεργοποίηση άδειας antivirus client σε σταθμό εργασίας ή server μέσω δικτύου χωρίς σύνδεση στο διαδίκτυο internet (offline activation).	NAI		
3.8	Να υπάρχει η δυνατότητα εξαγωγής πακέτου με το πρόγραμμα προστασίας, διαχείρισης, τις αντίστοιχες πολιτικές - ρυθμίσεις τους και την άδεια ενεργοποίησης για τοπικές εγκαταστάσεις.	NAI		
3.9	Να μπορεί να γίνει εισαγωγή λίστας των υπολογιστών του δικτύου με τη χρήση ενδεικτικά CSV αρχείου ή text file ή Active Directory Scan ή Active Directory import ή Network Pool ή IP range κτλ.	NAI		
3.10	Να υποστηρίζεται έλεγχος και ειδοποίηση στην κεντρική κονσόλα για το αν υπάρχουν ενημερώσεις για λειτουργικά συστήματα Windows των σταθμών εργασίας / server όπου είναι εγκατεστημένος ο antivirus client.	NAI		
3.11	Να υποστηρίζεται η παρακολούθηση όλων των antivirus client και η παραγωγή αναφορών και στατιστικών σε μορφές (ενδεικτικά) PDF, PS, CSV, Charts καθώς και η αποστολή αυτοματοποιημένων emails των προαναφερόμενων αναφορών/στατιστικών.	NAI		
3.12	Η επικοινωνία του κεντρικού server και των antivirus clients θα διασφαλίζεται μέσω certificate.	NAI		
3.13	Να υπάρχει η δυνατότητα αυτόματων αναβαθμίσεων του προϊόντος.	NAI		
4	Ενημερώσεις			
4.1	Οι ενημερώσεις από το διαδίκτυο για της κεντρικής βάσης malware θα γίνονται αυτόματα σε κεντρικό σημείο (server διαχείρισης) από το οποίο στην συνέχεια θα ενημερώνονται όλοι οι σταθμοί εργασίας και οι servers. Σε περίπτωση που δεν είναι διαθέσιμος ο server διαχείρισης, να υποστηρίζεται αυτόματη παράκαμψή του.	NAI		
4.2	Οι προαναφερόμενες ενημερώσεις θα προσφέρονται έως τη λήξη της περιόδου εγγυημένης λειτουργίας προμήθειας.	NAI		
4.3	Rollback σε προηγούμενη έκδοση του Signature File με ταυτόχρονη παύση των ενημερώσεων, επιλέγοντας το κεντρικά ή απευθείας από τον client.	NAI		
4.4	Να παρέχεται cloud reputation database για αμεσότερη προστασία από νέες απειλές.	NAI		
5	On boot scan			
5.1	Να υποστηρίζεται σάρωση και καθαρισμός κατά την εκκίνηση του σταθμού εργασίας / server (on-boot scan) χωρίς να χρειάζεται να ξεκινήσει το λειτουργικό σύστημα.	NAI		
6	Ειδικές απαιτήσεις			
6.1	Να υποστηρίζεται η εξαγωγή των ρυθμίσεων ενός antivirus client σε αρχείο και εισαγωγής των ρυθμίσεων σε άλλον από το ίδιο αρχείο.	NAI		
6.2	Να υποστηρίζεται η προστασία εικονικών μηχανών σε περιβάλλον VMWare χωρίς εγκατάσταση λογισμικού προστασίας (agent / antivirus client) στο λειτουργικό σύστημα της κάθε εικονικής μηχανής είτε με την εγκατάσταση ενός light agent.	NAI		
6.3	Να περιέχεται εφαρμογή που να καταγράφει την κατάσταση των agents / antivirus clients (εφαρμογές, processes, services κ.α) σε μία χρονική στιγμή (snapshot) και προαιρετικά να μπορεί να γίνει σύγκριση με προηγούμενη κατάσταση.	NAI		
6.4	Επικοινωνία του software μόνο με IP δηλαδή να δουλέψει σε περιπτώσεις όπου δεν υπάρχουν υπηρεσίες ονοματοδοσίας (DNS server).	NAI		
6.5	Το μενού της κονσόλας διαχείρισης και των antivirus clients για τους σταθμούς εργασίας να διατίθεται και στην ελληνική γλώσσα.	NAI		

- Σημειώνεται ότι οι προσφορές δεν είναι δεσμευτικές για την Αναθέτουσα αρχή και ούτε αυτή υποχρεούται να προχωρήσει άμεσα στην εν λόγω προμήθεια.
- Η επιλογή του Αναδόχου μπορεί να γίνει και ανά κωδικό CPV προς όφελος του δημοσίου συμφέροντος.
- Η υπηρεσία δεν αναγνωρίζει καμία δαπάνη πέραν της προσφοράς που δίνεται.
- Όλες οι προβλεπόμενες κρατήσεις θα βαρύνουν τον μειοδότη.
- Μετά το πέρας της αξιολόγησης των προσφορών οι συμμετέχοντες θα ενημερωθούν (με email ή fax) για τα αποτελέσματα της αξιολόγησης και την κατάταξή τους.
- Η παρούσα πρόσκληση θα αναρτηθεί και στις ιστοσελίδες της ΠΑΜΘ www.pamth.gov.gr.

Ο φάκελος της προσφοράς θα υποβληθεί στο γραφείο του Τμήματος Πληροφορικής της ΠΕ Καβάλας ή ταχυδρομικώς (3ος Όροφος Γραφείο 332, Εθνικής Αντίστασης 20, Τ.Κ.65403) μέχρι την ανωτέρω καταληκτική ημερομηνία.

Οι ενδιαφερόμενοι οικονομικοί φορείς καταθέτουν με την προσφορά τους υπεύθυνη δήλωση όπου θα δηλώνεται:

Α)Αποδέχομαι τους όρους και τις τεχνικές προδιαγραφές που θέτει η Υπηρεσία στην παρούσα πρόσκληση.

Β)Εφόσον επιλεγώ ανάδοχος, δεσμεύομαι να προσκομίσω τα ακόλουθα δικαιολογητικά, προς απόδειξη της μη συνδρομής των λόγων αποκλεισμού από διαδικασίες σύναψης δημοσίων συμβάσεων των παρ.1 και 2 του άρθρου 73 και του άρθρου 74 του Ν.4412/2016, εντός δεκαπέντε (15) ημερών:

1. Απόσπασμά ποινικού μητρώου. Εφόσον πρόκειται για εταιρείες περιορισμένης ευθύνης (Ε.Π.Ε.) και προσωπικές (Ο.Ε. και Ε.Ε.), η υποχρέωση αφορά στους διαχειριστές της εταιρείας και εφόσον πρόκειται για ανώνυμες εταιρείες (Α.Ε.), η υποχρέωση αφορά στον Διευθύνοντα Σύμβουλο και όλα τα μέλη του Διοικητικού Συμβουλίου της εταιρείας.

2. Φορολογική ενημερότητα

3. Ασφαλιστική ενημερότητα για κύρια και επικουρική ασφάλεια (άρθρο 80 παρ.2 του Ν.4412/2016)

4. Εφόσον πρόκειται για νομικό πρόσωπο, αποδεικτικά έγγραφα νομιμοποίησης και εκπροσώπησης του νομικού προσώπου (άρθρο 93 του Ν.4412/2016).

Σε περίπτωση αδυναμίας προσκόμισης των ανωτέρω πιστοποιητικών εντός της ορισθείσας προθεσμίας ο υποψήφιος ανάδοχος αποκλείεται από τη διαδικασία και καλείται ο αμέσως επόμενος στην κατάταξη συμμετέχων.

ΜΕΠ
Ο Αναπληρωτής Προϊστάμενος
Τμήματος Πληροφορικής

Ευριπίδης Ζαϊμίδης