

Τεχνικές Προδιαγραφές

Οι Τεχνικές Προδιαγραφές του αιτούμενου εξοπλισμού παρατίθενται κατωτέρω

Λογισμικό Antivirus, XDR, E-mail Protection, VA&PM,

A/A	Προδιαγραφή	Απαίτηση
1.2	Το λογισμικό προστασίας να υποστηρίζει τα εξής λειτουργικά συστήματα: MS Windows 10, 11 MS Windows Server 2012, 2012r2, 2016,2019,2022,2025 Linux (Ubuntu Desktop Ubuntu Desktop 20.04 LTS, Ubuntu Desktop 22.04 LTS, Ubuntu Desktop 24.04 LTS , Red Hat Enterprise Linux 8, 9, 10 with supported desktop environment installed, Linux Mint 21, 22) MacOS 11 and later MacOS Server 11 and later	NAI
1.3	Οι ελάχιστες απαιτήσεις συστήματος να είναι 0.3 GB ελεύθερη διαθέσιμη μνήμη (RAM) και 1 GB ελεύθερος χώρος στον σκληρό δίσκο.	NAI
1.4	Το σύστημα προστασίας θα πρέπει να έχει πιστοποίηση του ανεξάρτητου οργανισμού AV-Comparatives “Business Security Approved” και “Real World Protection Advanced” κατ’ ελάχιστον, για τα τελευταία 2 έτη τουλάχιστον.	NAI
1.5	Το σύστημα θα πρέπει να έχει πιστοποίηση του ανεξάρτητου ινστιτούτου AV-TEST GmbH, “Approved Corporate Endpoint Protection - TOP Product” κατ’ ελάχιστον τα τελευταία 2 έτη	NAI
1.6	Προϋπόθεση αξιολόγησης, επί ποινή αποκλεισμού, αποτελεί η συμπλήρωση του φύλλου συμμόρφωσης με παραπομπή σε φυλλάδια του κατασκευαστικού οίκου προς απόδειξη ζητούμενων στοιχείων και με σαφή αναφορά στην σελίδα και παράγραφο του φυλλαδίου, όπου εμπεριέχονται τα στοιχεία αυτά.	NAI
2	Αντική Προστασία	
2.1	Η κεντρική βάση ανίχνευσης κακόβουλου λογισμικού και οι σχετικοί μηχανισμοί ενημέρωσης, ανάλυσης και συσχέτισης απειλών θα πρέπει να παρέχονται μέσω ασφαλούς υποδομής cloud του κατασκευαστή.	NAI
2.2	Να υποστηρίζεται ανίχνευση και καθαρισμός όλων των τύπων απειλών malware: viruses, malware, trojans, dialers, spyware, jokes, hoaxes, ransomware.	NAI
2.3	Να υποστηρίζεται αυτόματη ανίχνευση και καθαρισμός των προαναφερθέντων απειλών σε πραγματικό χρόνο.	NAI
2.4	Να υποστηρίζεται ανίχνευση και καθαρισμός των προαναφερθέντων απειλών.	NAI
2.5	Να υποστηρίζεται IPS (intrusion prevention system).	NAI
2.6	Να υποστηρίζονται τεχνολογίες advanced heuristics (ενδεικτικά: DNA, smart signatures, Behavioral Analysis) για δυνατότητα ανίχνευσης άγνωστου malware.	NAI
2.7	Προστασία για SSL/TLS filtering στα πρωτόκολλα HTTPS, IMAPS, POP3S.	NAI
2.8	Δυνατότητα αποτροπής γνωστών exploits	NAI
2.9	Δυνατότητα μπλοκαρίσματος όλων των σελίδων του Internet σε ένα client καθώς και διαχείριση των σελίδων που μπορούν να είναι	NAI

	διαθέσιμες στο χρήστη ανά κατηγορία, π.χ. αποτροπή επίσκεψης σε σελίδες social media, streaming videos.	
2.10	Δυνατότητα προστασίας σε δικτυακό επίπεδο με client based Firewall, με δυνατότητα φιλτραρίσματος σε επίπεδο θυρών και εφαρμογών σε εισερχόμενες και εξερχόμενες συνδέσεις.	NAI
2.11	Δυνατότητα προστασίας από δικτυακές απειλές και botnets	NAI
2.12	Δυνατότητα ενιαίας καραντίνας αρχείων που ανιχνεύθηκαν για όλο το δίκτυο, με δυνατότητες προβολής clients ανά απειλή, εξαγωγή και εξαίρεση	NAI
2.13	Να παρέχεται από το πρόγραμμα ασφαλής περιηγητής (browser) για την προστασία ευαίσθητων δεδομένων κατά την περιήγηση στο διαδίκτυο.	NAI
2.14	Να παρέχεται η δυνατότητα ρύθμισης προκαθορισμένων site με σκοπό την αυτόματη ανακατεύθυνση τους στον προστατευμένο περιηγητή που παρέχεται από το πρόγραμμα.	NAI
2.15	Να παρέχεται η δυνατότητα του προγράμματος σε λειτουργικό windows server να ελέγχει τους φακέλους και τα αρχεία στο Microsoft OneDrive for Business για κακόβουλο λογισμικό.	NAI
2.16	Να παρέχεται η δυνατότητα του προγράμματος σε λειτουργικά windows server να λειτουργούν μεταξύ τους ως cluster με σκοπό τον συγχρονισμό των δεδομένων, των ρυθμίσεων και ειδοποιήσεων. (πχ. Ανταλλαγή των προαναφερόμενων δεδομένων και ρυθμίσεων του antivirus program σε windows failover cluster nodes, network load balancing nodes, όπου και είναι απαραίτητο το πρόγραμμα να έχει το ίδιο configuration σε όλα τα nodes).	NAI
2.17	Να παρέχεται η δυνατότητα του προγράμματος τοπικά σε λειτουργικά windows server όπου έχουν τον ρόλο του hypervisor, να πραγματοποιεί scan στους εικονικούς δίσκους (Basic) των hyper-v virtual machines σε on line state αλλά και σε offline state των εν λόγω VM.	NAI
2.18	Δυνατότητα προστασίας από Brute Force Attack	NAI
2.19	Ενσωματωμένη λειτουργία Sandbox καθών και πρόσθετη στο cloud.	NAI
2.20	Application control για android συσκευές.	NAI
2.21	Διαχείριση συσκευών (Device Control).	NAI
2.22	Να υποστηρίζεται η δυνατότητα επαναφοράς αρχείων από επιθέσεις ransomware.	
3	Κεντρική διαχείριση	
3.1	Να υποστηρίζεται η κεντρική διαχείριση όλων των λογισμικών προστασίας των σταθμών εργασίας / servers (antivirus client) μέσω κεντρικής cloud κονσόλας και με τη δυνατότητα εγκατάστασης τοπικά.	NAI
3.2	Να υποστηρίζεται η δημιουργία πολλαπλών ομάδων με δυνατότητα εφαρμογής διαφορετικών πολιτικών / ρυθμίσεων για κάθε ομάδα.	NAI
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 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	Να υπάρχει η δυνατότητα αυτόματων αναβαθμίσεων του προϊόντος.	NAI
3.13	Επισκόπηση σε πραγματικό χρόνο για όλα τα τερματικά: υπολογιστές, διακομιστές, εικονικές μηχανές, διαχειριζόμενες κινητές συσκευές	NAI
3.14	Επισκόπηση σε πραγματικό χρόνο για όλα τα τερματικά: υπολογιστές, διακομιστές, εικονικές μηχανές, διαχειριζόμενες κινητές συσκευές	NAI
3.15	Ασφάλεια πρόσβασης RBAC Να διαθέτει σύστημα διαχείρισης προσβάσεων Role-Based Access Control για λεπτομερή εκχώρηση δικαιωμάτων διαχειριστή και χρήση κονσόλας σε συγκεκριμένες ομάδες δικτύου, ομάδες αντικειμένων.	NAI
3.16	Πρόσβαση κονσόλας με έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA)	NAI
3.17	Διαχείριση κινητών συσκευών (MDM -Mobile Device Management) που να καλύπτει συσκευές Android και Apple.	NAI
3.18	Αποθετήριο Υλικού/Λογισμικού (Hardware/Software Inventory) Εντοπισμός και προβολή πληροφοριών για όλες τις εγκατεστημένες εφαρμογές λογισμικού στον οργανισμό, αλλά και για το εγκατεστημένο hardware.	NAI
3.19	Να υποστηρίζει τα εργαλεία SIEM και να μπορεί να εξαγάγει όλες τις πληροφορίες καταγραφής στην ευρέως αποδεκτή μορφή JSON ή LEEF/CEF, επιτρέποντας την ενσωμάτωση με τα Κέντρα Επιχειρήσεων Ασφαλείας.	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 παράκαμψη 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 υπάρχει η δυνατότητα αυτόματων αναβαθμίσεων του προϊόντος.	NAI
5	Πρόσθετη cloud ασφάλεια για νέες απειλές	

5.1	Να παρέχεται cloud reputation database για αμεσότερη προστασία από νέες απειλές.	NAI
5.2	Να υπάρχει δυνατότητα ώστε τα ύποπτα δείγματα που δεν έχουν ακόμη επιβεβαιωθεί ως κακόβουλα και ενδέχεται να μεταφέρουν κακόβουλο λογισμικό να υποβάλλονται αυτόματα η και χειροκίνητα σε απομονωμένο cloud περιβάλλον του κατασκευαστή ώστε να εκτελεστούν και να αξιολογηθούν σε περιβάλλον προστατευμένης εκτέλεσης από τους Προηγμένους μηχανισμούς ανίχνευσης κακόβουλου λογισμικού του κατασκευαστή.	NAI
5.3	Να ενημερώνεται αυτόματα η κονσόλα διαχειρίσεις για τα αποτελέσματα των υποβληθέντων αρχείων στο cloud.	NAI
5.4	Η λύση του κατασκευαστή για τα υποβληθέντα αρχεία στο cloud να μπορεί να χρησιμοποιήσει διακομιστή μεσολάβησης για την προώθηση της σύνδεσης με τους διακομιστές του και για προσωρινή αποθήκευση των μεταφερόμενων δεδομένων.	NAI
5.5	Να υπάρχει δυνατότητα εξαίρεσης ενός αρχείου που έχει ανιχνευθεί και υποβληθεί στο cloud του κατασκευαστή σε όλους τους υπολογιστές του δικτύου η και σε μερικούς εξ αυτών.	NAI
5.6	Να επιτρέπεται η ρύθμιση μέσω της κεντρικής κονσόλας διαχείρισης μέσω της οποίας θα ορίζονται οι προϋποθέσεις για τα αρχεία που θα υποβάλλονται στο cloud (π.χ. ενέργειες που θα πραγματοποιηθούν μετά την ανάλυση του αρχείου, υποβολή συγκεκριμένων file types, εξαίρεση υποβολής αρχείων με συγκεκριμένο extension, μέγιστο μέγεθος ενός υποβληθέντος αρχείου (MB)).	NAI
6	Ασφάλεια αρχείων	
6.1	Δυνατότητα διαχείρισης της πλήρους κρυπτογράφησης δίσκου των διαχειριζόμενων σταθμών εργασίας Windows με πρόσθετο επίπεδο ασφάλειας πριν την εκκίνηση του υπολογιστή (pre-boot login), μέσω της κεντρικής κονσόλας.	NAI
6.2	Να παρέχεται η επιλογή κρυπτογράφησης όλων των δίσκων η μόνο του δίσκου εκκίνησης του υπολογιστή η των υπολογιστών στο δικτυο μέσω της κεντρικής διαχείρισης.	NAI
6.3	Να υπάρχει η δυνατότητα επιλογής χρησιμοποίησης υποστήριξης λειτουργικής μονάδας αξιόπιστης πλατφόρμας (TPM) ή Υποστήριξη μονάδας δίσκου αυτόματης κρυπτογράφησης Opal (OPAL) για την κρυπτογράφησή, με βάση το υλικό που είναι διαθέσιμο στους διαχειριζόμενους σταθμούς εργασίας.	NAI
6.4	Να υπάρχει δυνατότητα να παραχθεί ένα μοναδικό αρχείου για κάθε υπολογιστή του δικτύου με σκοπό την αποκρυπτογράφηση του δίσκου μέσω αφαιρούμενου μέσου (usb,cd) και το οποίο θα δημιουργείται από την κεντρική κονσόλα διαχειρίσεις.	NAI
6.5	Να υπάρχει δυνατότητα αποκρυπτογράφησης του δίσκου η των δίσκων του υπολογιστή η των υπολογιστών του δικτύου απευθείας μέσω πολιτικής από την κονσόλα κεντρικής διαχείρισης.	NAI
6.6	Να υπάρχει η δυνατότητα επαναφοράς κωδικού χρήστη όσον αφορά την πιστοποίηση του πριν την εκκίνηση των windows σε κρυπτογραφημένους δίσκους (pre-boot login) από την κεντρική κονσόλα διαχείρισης.	NAI
6.7	Να παρέχεται η δυνατότητα απενεργοποίησης της πιστοποίησης του χρήστη (pre-boot login) πριν την εκκίνηση του λειτουργικού συστήματος, σε κρυπτογραφημένο δίσκο συστήματος για καθορισμένο αριθμό επανεκκινήσεων του υπολογιστή.	NAI
7	On boot scan	
7.1	Να υποστηρίζεται σάρωση και καθαρισμός κατά την εκκίνηση του σταθμού εργασίας / server (on-boot scan) χωρίς να χρειάζεται να ξεκινήσει το λειτουργικό σύστημα.	NAI

8	Ειδικές απαιτήσεις	
8.1	Να υποστηρίζεται η εξαγωγή των ρυθμίσεων ενός antivirus client σε αρχείο και εισαγωγής των ρυθμίσεων σε άλλον από το ίδιο αρχείο.	NAI
8.2	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
8.3	Το μενού της κονσόλας διαχείρισης και των antivirus clients για τους σταθμούς εργασίας να διατίθεται και στην ελληνική γλώσσα.	NAI
9	Extended Detection and Response XDR-EDR	
9.1	Να παρέχεται η δυνατότητα εισαγωγής κανόνων για τον εντοπισμό εφαρμογών κατά την εκτέλεση από προσωρινούς φακέλους, εντοπισμό αρχείων του Office με ενσωματωμένα scripts ή εκτελέσιμα.	NAI
9.2	Να υπάρχει άμεση ειδοποίηση κατά την εμφάνιση γνωστού ransomware extension σε μια συσκευή και προβολή του συνολου των ενημερώσεων ransomware shield στην ίδια κονσόλα.	NAI
9.3	Να υπάρχει δυνατότητα εντοπισμού αδύναμων στοιχείων με ταξινόμηση των υπολογιστών κατά αριθμό μοναδικών συναγερμών, προβληματικών συσκευών/χρηστών και δυνατότητα ανάλυσης root cause για γρήγορο εντοπισμό της πηγής μόλυνσης.	NAI
9.4	Τα υπάρχει η δυνατότητα ταξινόμησης με βάση τη δημοτικότητα ή τη φήμη του αρχείου, την ψηφιακή υπογραφή, τη συμπεριφορά και τις πληροφορίες metadata και παραπομπή των στοιχείων με την πλατφόρμα MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™).	NAI
9.5	Να παρέχεται η δυνατότητα αναζήτησης σε όλους τους υπολογιστές για την ύπαρξη της νέας απειλής και για ενδείξεις παραβίασης ότι η απειλή υπήρχε απο πριν και δυνατότητα αποκλεισμού περαιτέρω διεύθυνσης στο δίκτυο.	NAI
9.6	Να υποστηρίζεται προσαρμογή κανόνων ανίχνευσης που περιγράφουν τεχνικές επίθεσης στο συγκεκριμένο περιβάλλον του οργανισμού.	NAI
9.7	Να υπάρχει δυνατότητα προβολής, φιλτραρίσματος, αποκλεισμού, καθαρισμού και ειδοποίησης των χρηστών για όλες τις εγκατεστημένες εφαρμογές και αρχεία αυτοματοποίησης(scripts).	NAI
9.8	Να υποστηρίζει διερεύνηση και αποκατάσταση με κατανόηση περιέχομένου (Context aware) όπως και να υπάρχει δυνατότητα προσδιορισμού και ταξινόμησης των υπολογιστών αυτόματα ή χειροκίνητα ή με χρήση Active Directory.	NAI
9.9	Να υποστηρίζει έλεγχο (Allow or Block) εφαρμογών ή αρχείων αυτοματοποίησης(scripts) βάση ομαδοποίησης υπολογιστών ή χρήστη και δυνατότητα ειδοποίησης μόνο για συγκεκριμένες ομάδες.	NAI
9.10	Να διαθέτει πάνω από 800 προρυθμισμένους κανόνες με δυνατότητα επεξεργασίας με γλώσσα XML για εύκολη ρύθμιση ή δημιουργία νέων.	NAI
9.11	Να υποστηρίζει λειτουργία εύκολης όπως και άμεσης απόκλισης	NAI
9.12	Να επιτρέπει τον αποκλεισμό αρχείων βάση hash, να έχει την ικανότητα τερματισμού διαδικασιών, εισαγωγής σε καραντίνα και απομόνωσης ή απενεργοποίησης μηχανημάτων εξ αποστάσεως με ένα κλικ καθώς και να παρέχει πρότασεις για αποκατάσταση.	NAI
9.13	Λεπτομερής ανάλυση Root Cause με αποτύπωση της αλυσίδας γεγονότων.	NAI

9.14	Διαχείριση εφαρμογών με δυνατότητα αποκλεισμού με HASH.	NAI
10	Λογισμικό Mail Security	
10.1	Προστασία emails από malware, spam και phishing web pages	NAI
10.2	Δυνατότητα αποστολής αναφορών σε επιλεγμένους χρήστες και διαχειριστές για τα emails που βρίσκονται στην καραντίνα. Όπως και δυνατότητα διαγραφής ή απελευθέρωσης ενός email άμεσα.	NAI
10.3	Δυνατότητα τοπικής καραντίνας με λειτουργία απελευθέρωσης email όπως και εξαίρεση συγκεκριμένων διεργασιών ή εφαρμογών από την Anti-malware σάρωση.	NAI
10.4	Δυνατότητα αποθήκευσης και διαχείρισης μηνυμάτων καραντίνας από ένα σημείο μέσω του Quarantine mailbox ή MS Exchange quarantine.	NAI
10.5	Δυνατότητα διαχείρισης της καραντίνας μέσω web browser με πρόσβαση είτε από το διαχειριστή συνολικά, είτε από κάθε χρήστη προσωποποιημένα.	NAI
10.6	Δυνατότητα ελέγχου ύποπτων δειγμάτων που δεν έχουν ακόμη επιβεβαιωθεί ως κακόβουλα και ενδέχεται να μεταφέρουν κακόβουλο λογισμικό να υποβάλλονται αυτόματα η και χειροκίνητα σε απομονωμένο cloud περιβάλλον του κατασκευαστή ώστε να εκτελεστούν και να αξιολογηθούν από προηγμένους μηχανισμούς ανίχνευσης κακόβουλου λογισμικού.	NAI
10.7	Δυνατότητα cluster σε λειτουργικά συστήματα windows server (συγχρονισμός των δεδομένων , των ρυθμίσεων και ειδοποιήσεων).	NAI
10.8	Δυνατότητα καταγραφής σημαντικών συμβάντων του προγράμματος, καθώς και πλήρης καταγραφή αποτελεσμάτων σαρώσεων, ανιχνεύσεων/απειλών (logs).	NAI
10.9	Υποστήριξη Remote monitoring and management (RMM).	NAI
10.10	Πραγματοποίηση ελέγχων SPF, DKIM, DMARC.	NAI
10.11	Λειτουργία σάρωσης βάσης on-demand.	NAI
10.12	Υποστήριξη κανόνων φιλτραρίσματος με βάση τις ιδιότητες των emails (π.χ. τύπος επισυναπτόμενου) και αντιστοίχιση ενεργειών.	NAI
10.13	Υποστήριξη λιστών εγκεκριμένων/μη αποδεκτών IPs, domains, αποστολέων.	NAI
10.14	Υποστήριξη επιτλέων υπηρεσιών RBL/DNSBL.	NAI
10.15	Δυνατότητα λειτουργίας Greylisting.	NAI
10.16	Δυνατότητα σάρωσης Office 365 mailbox scan για περιβάλλοντα Exchange Hybrid.	NAI
10.17	Δυνατότητα Backscatter protection.	NAI
10.18	Δυνατότητα διαχείρισης και μέσω περιβάλλοντος γραμμής εντολών.	NAI
10.19	Δυνατότητα διαχείρισης του προϊόντος από κεντρική κονσόλα διαχείρισης.	NAI
11	Λογισμικό Cloud Office security για Microsoft 365 και Google Workspace	
11.1	Δυνατότητα προστασίας των cloud Microsoft 365, Exchange Online όπως και Microsoft OneDrive(να συμπεριλαμβάνονται τα Microsoft 365 plans: enterprise, business, education.)	NAI
11.2	Δυνατότητα προστασίας Google Workspace, Gmail και Google Drive.	

11.3	Δυνατότητα προστασίας Microsoft Teams και Sites.	NAI
11.4	Να υπάρχει δυνατότητα multi-tenant προστασίας.	NAI
11.5	Να υποστηρίζεται προστασία: Antispam, Anti-Phishing, Anti-Malware.	NAI
11.6	Να υπάρχει δυνατότητα διαχείριση καραντίνας με εναλλαγές ανάμεσα σε καρτέλες Exchange Online, OneDrive, Team groups και SharePoint sites.	NAI
11.7	Να υποστηρίζετε δημιουργία και κατανομή πολιτικών ανά γκρούπ ή ανά χρήστη.	NAI
11.8	Να υπάρχει η δυνατότητα προστασίας ανά γραμματοκιβώτιο όπως και κοινών γραμματοκιβωτίων(Shared Mailboxes).	NAI
11.9	Να υπάρχει η δυνατότητα δημιουργίας αναφορών με επιλεγμένα κριτήρια καθώς και προγραμματισμό παραγωγής αναφορών(Scheduled reports).	NAI
11.10	Να υπάρχει η δυνατότητα αποστολής αναφορών σε πολλαπλούς αποδέκτες.	NAI
11.11	Να υπάρχει δυνατότητα αυτόματου καθαρισμού παλαιότερων αρχείων αναφοράς(Log files rotation).	NAI
11.13	Δυνατότητα ανίχνευσης potentially unwanted, suspicious, unsafe applications.	NAI
11.13	Δυνατότητα προστασίας σε πραγματικό χρόνο (Real-time).	NAI
11.14	Δυνατότητα προστασίας με υποβοήθηση μάθησης μηχανής (Machine learning).	NAI
11.15	Δυνατότητα αλλαγής προφίλ ανίχνευσης(Aggressive, Balanced, Cautious, Off).	NAI
11.16	Δυνατότητα αναφοράς ψευδώς θετικών(False positive) και ψευδώς αρνητικών(False negative) δειγμάτων	NAI
11.17	Προβολή στατιστικών σε μια σελίδα με ανανέωση ανά 10 λεπτά(Dashboard).	NAI
11.18	Να ενσωματώνεται σαν υπηρεσία (SaaS)	NAI
12	Ενημερώσεις ασφαλείας και ευπαθειών για λειτουργικά συστήματα και εφαρμογές Windows	
12.1	Διαχείριση ενημερώσεων ασφαλείας και ευπαθειών για λειτουργικά συστήματα και εφαρμογές Windows και Linux (Patch Management/Vulnerability).	NAI
12.2	Αυτοματοποιημένη σάρωση εφαρμογών (Automated scanning).	NAI
12.3	Καθορισμός προτεραιότητας με βάση τη σοβαρότητα (Severity-based prioritization), πλήρης ορατότητα διαθέσιμων αναβαθμίσεων απο κεντρικό σημείο.	NAI
12.4	Αυτοματοποιημένη ή κατ' απαίτηση αναβάθμιση εφαρμογών μέσω πολιτικής (Automatic and manual patching)	NAI
13	Επαλήθευση ταυτότητας πολλαπλών παραγόντων (Multi-factor authentication)	
13.1	Αποτροπή παραβιάσεων σε κρίσιμες υποδομές.	NAI

13.2	Πολλαπλοί τρόποι για αυθεντικοποίηση.	NAI
13.3	Να υπάρχει η δυνατότητα χρήσης MFA σε υποδομές, εικονικών ιδιωτικών δικτύων (VPN), remote desktop (RDP), διαδικτυακής πρόσβασης στο Outlook (OWA), VMware Horizon View και υπηρεσιών RADIUS-based.	NAI
13.4	Δυνατότητα αποστολής κωδικού (OTP) ή single tap το οποίο να λειτουργεί σε συσκευές Android και IOS.	NAI
13.5	Δυνατότητα integration τόσο σε cloud όσο και σε on-premise εφαρμογές.	NAI
13.6	Δυνατότητα integration με Active Directory περιβάλλοντα.	NAI
13.7	Να μπορεί να πραγματοποιηθεί απομακρυσμένη διαχείριση από κονσόλα Cloud ή on-premise.	NAI
13.8	Να υπάρχει η δυνατότητα extension του MFA σε προσαρμοσμένες εφαρμογές με API και SDK integration.	NAI
13.9	Η λύση θα πρέπει είναι συμβατή με OATH tokens και με Active Directory, Entra ID, Okta, LDAP	NAI
13.10	Η λύση πρέπει να διαθέτει IP address whitelisting, ώστε ο διαχειριστής να μπορεί να ορίζει εγκεκριμένες IP διευθύνσεις ή εύρη IP από τα οποία δεν θα ζητείται 2FA/OTP, όπου αυτό υποστηρίζεται από το εκάστοτε προστατευόμενο σενάριο πρόσβασης.	NAI
13.11	Η λύση πρέπει να υποστηρίζει χρήση third-party TOTP authenticator applications , όπως Google Authenticator, Microsoft Authenticator και λοιπές εφαρμογές που υποστηρίζουν OATH/TOTP, χωρίς υποχρεωτικό κλείδωμα του φορέα σε αποκλειστική εφαρμογή του κατασκευαστή.	NAI

Πρότυπα διασφάλισης ποιότητας και πρότυπα περιβαλλοντικής διαχείρισης

Ο ανάδοχος να διαθέτει τα παρακάτω πιστοποιητικά, τα οποία θα πρέπει να προσκομίσει μαζί με την προσφορά:

- **ISO 9001: 2015** ή ισοδύναμο ή μεταγενέστερης έκδοσής του στα πεδία εφαρμογής του σχεδιασμού, ανάπτυξης, εγκατάστασης υποστήριξης και συντήρησης πληροφοριακών συστημάτων
- **ISO 27001: 2013** ή ισοδύναμο ή μεταγενέστερης έκδοσής του στο πεδίο εφαρμογής της Ασφάλειας Πληροφοριών
- **ISO 14001: 2015** ή ισοδύναμο ή μεταγενέστερης έκδοσής του στο πεδίο εφαρμογής διαχείριση του περιβάλλοντος που καλύπτει τον εντοπισμό περιβαλλοντικών επιπτώσεων (ρύποι, απόβλητα, κατανάλωση ενέργειας κ.λπ.)

Η αναθέτουσα αρχή αναγνωρίζει ισοδύναμα πιστοποιητικά που έχουν εκδοθεί από φορείς διαπιστευμένους από ισοδύναμους Οργανισμούς διαπίστευσης, εδρεύοντες και σε άλλα κράτη - μέλη. Επίσης, κάνει δεκτά άλλα αποδεικτικά στοιχεία για ισοδύναμα μέτρα διασφάλισης ποιότητας, εφόσον ο ενδιαφερόμενος οικονομικός φορέας δεν είχε τη δυνατότητα να αποκτήσει τα εν λόγω πιστοποιητικά εντός των σχετικών προθεσμιών για λόγους για τους οποίους δεν ευθύνεται ο ίδιος,

υπό την προϋπόθεση ότι ο οικονομικός φορέας αποδεικνύει ότι τα προτεινόμενα μέτρα διασφάλισης ποιότητας πληρούν τα απαιτούμενα πρότυπα διασφάλισης ποιότητας.

ΠΑΡΑΡΤΗΜΑ II – ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ ΠΙΝΑΚΑΣ 1 : Τεχνικές Προδιαγραφές				
A/A	Προδιαγραφή	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΤΗΡΗΣΕΙΣ
1.	Γενικές απαιτήσεις			
1.1.	Ο ανάδοχος να διαθέτει τα παρακάτω πιστοποιητικά, τα οποία θα πρέπει να προσκομίσει μαζί με την προσφορά: ISO 9001: 2015 ή ισοδύναμο ή μεταγενέστερης έκδοσής του στα πεδία εφαρμογής του σχεδιασμού, ανάπτυξης, εγκατάστασης υποστήριξης και συντήρησης πληροφοριακών συστημάτων ISO 27001: 2013 ή ισοδύναμο ή μεταγενέστερης έκδοσής του στο πεδίο εφαρμογής της Ασφάλειας Πληροφοριών ISO 14001: 2015 ή ισοδύναμο ή μεταγενέστερης έκδοσής του στο πεδίο εφαρμογής διαχείριση του περιβάλλοντος που καλύπτει τον εντοπισμό περιβαλλοντικών επιπτώσεων (ρύποι, απόβλητα, κατανάλωση ενέργειας κ.λπ.)	NAI		

Επίσης, Ο υποψήφιος Ανάδοχος θα πρέπει να διαθέτει τουλάχιστον έναν (1), τουλάχιστον, εξειδικευμένο-πιστοποιημένο τεχνικό, για την υλοποίηση του έργου.

Υποβάλλεται το παρόν πρακτικό με τις Τεχνικές Προδιαγραφές, που τέθηκαν σε διαβούλευση με **ΑΔΑΜ 2026DIAB33485**, και υποβλήθηκε σχόλιο από Οικονομικό Φορέα, και παρατίθενται οι απαντήσεις στα σχόλια. Οι Τεχνικές Προδιαγραφές δε μεταβάλλονται.

1^ο Σχόλιο

Σχόλια - Προτάσεις στη Δημόσια Διαβούλευση για την «Προμήθεια συστήματος Κακόβουλου Λογισμικού ON SITE SUPPORT & Υπηρεσιών Παραμετροποίησης ασφάλειας και Νέων Αδειών EDR-XDR για την 1η ΥΠΕ Αττικής και τις αποκεντρωμένες μονάδες»

Αξιότιμοι κύριοι,

Με αφορμή τη δημόσια διαβούλευση για την προμήθεια νέου ολοκληρωμένου συστήματος ασφάλειας (EDR / XDR) και υπηρεσιών παραμετροποίησης για τις ανάγκες της 1ης ΥΠΕ Αττικής και των αποκεντρωμένων μονάδων της, θα θέλαμε να καταθέσουμε τις τεχνικές και οικονομικές μας παρατηρήσεις.

Στόχος της παρέμβασής μας είναι η διασφάλιση των θεμελιωδών αρχών της διαφάνειας, του ελεύθερου και ανόθευτου ανταγωνισμού, καθώς και της προστασίας του δημοσίου συμφέροντος μέσω της βέλτιστης αξιοποίησης των υφιστάμενων επενδύσεων και της διασφάλισης της επιχειρησιακής συνέχειας του Οργανισμού.

Α. Περιορισμός του Ανταγωνισμού και Αποκλεισμός Διεθνώς Αναγνωρισμένων Λύσεων

Από τη μελέτη του σχεδίου των τεχνικών προδιαγραφών προκύπτει ότι συγκεκριμένες απαιτήσεις εισάγουν τεχνικούς περιορισμούς που δεν συνάδουν με τις βέλτιστες πρακτικές της παγκόσμιας αγοράς κυβερνοασφάλειας.

Οι όροι αυτοί, λειτουργώντας προνομιακά υπέρ συγκεκριμένων αρχιτεκτονικών, αποκλείουν πληθώρα κορυφαίων και διεθνώς πιστοποιημένων λύσεων της αγοράς (π.χ. αναγνωρισμένων κατά Gartner / MITRE Engenuity). Οι εν λόγω αποκλειόμενες λύσεις προσφέρουν αποδεδειγμένα πολυεπίπεδη προληπτική προστασία, συνδυάζοντας προηγμένη ανάλυση συμπεριφοράς (behavioral analysis), μηχανική μάθηση (machine learning), αποτροπή δικτυακών απειλών (network-level attack prevention) και ενσωματωμένο έλεγχο ροής (firewall) – τεχνολογίες οι οποίες θωρακίζουν ήδη με απόλυτη επιτυχία κρίσιμες υποδομές του Δημοσίου.

B. Τεχνικές Προδιαγραφές που Περιορίζουν τον Ανταγωνισμό

Προς επίρρωση των ανωτέρω, επισημαίνουμε συγκεκριμένους όρους που αποκλείουν κορυφαίους κατασκευαστές (Tier-1 Enterprise Vendors) της διεθνούς αγοράς, χωρίς να προσφέρουν ουσιαστικό πλεονέκτημα ασφαλείας:

- Προδιαγραφές 2.13 & 2.14 (Ασφαλής Περιηγητής / Secure Browser): Η απαίτηση για αποκλειστικό browser αποτελεί χαρακτηριστικό κυρίως consumer προϊόντων. Οι enterprise λύσεις προστατεύουν το σύνολο της κίνησης (Web/Traffic Filtering, SSL/TLS Inspection) πάνω στους υπάρχοντες browsers του οργανισμού (π.χ. Edge, Chrome), διασφαλίζοντας τη συμβατότητα των εφαρμογών χωρίς να αλλοιώνουν την εμπειρία χρήσης.

ο Πρόταση: Να τροποποιηθεί ώστε να ζητείται: «Να παρέχεται προστασία και φιλτράρισμα της διαδικτυακής κίνησης στους υφιστάμενους περιηγητές του οργανισμού για την ασφάλεια ευαίσθητων δεδομένων».

- Προδιαγραφή 2.16 (Λειτουργία Cluster μεταξύ Windows Server Agents): Η απαίτηση οι agents να επικοινωνούν peer-to-peer για cluster synchronization περιορίζει αναίτια τον ανταγωνισμό. Στις σύγχρονες αρχιτεκτονικές, η ομοιομορφία του configuration σε Failover Clusters/NLB διασφαλίζεται απόλυτα και κεντρικά μέσω της Κονσόλας Διαχείρισης.

ο Πρόταση: Να τροποποιηθεί ως εξής: «Να υποστηρίζεται η εγκατάσταση σε περιβάλλοντα Windows Failover Cluster και NLB, διασφαλίζοντας την εφαρμογή ταυτόσημων πολιτικών ασφαλείας σε όλα τα nodes μέσω της κεντρικής κονσόλας».

- Προδιαγραφή 2.17 (Scan Εικονικών Δίσκων Hyper-V σε Online/Offline State): Η απαίτηση για τοπική σάρωση (scan) των εικονικών δίσκων (.vhd/.vhdx) των εικονικών μηχανών (VMs) σε online και offline κατάσταση απευθείας από τον Hyper-V Host, περιγράφει μια ξεπερασμένη αρχιτεκτονική που προκαλεί "AV Storms" και γονατίζει τις επιδόσεις των servers. Οι enterprise λύσεις χρησιμοποιούν dedicated Security Appliances (offloading architecture) που προστατεύουν το virtualization layer χωρίς να επιβαρύνουν τους πόρους του Hypervisor.

ο Πρόταση: Να τροποποιηθεί ώστε να επιτρέπεται εναλλακτική αρχιτεκτονική: «...είτε τοπικά είτε μέσω κεντρικού μηχανισμού σάρωσης (Security Appliance / Offloading Architecture) για την αποφυγή επιβάρυνσης των πόρων του Hypervisor».

- Προδιαγραφή 9.10 (Κανόνες XDR/EDR με επεξεργασία αποκλειστικά σε XML): Ο περιορισμός της δημιουργίας custom κανόνων αποκλειστικά μέσω γλώσσας XML είναι φωτογραφικός. Οι περισσότεροι κατασκευαστές προσφέρουν πλέον αυτή τη δυνατότητα μέσω σύγχρονων, visual graphical interfaces (GUI) που μειώνουν την πολυπλοκότητα.

ο Πρόταση: Να απαλειφθεί η αναφορά σε συγκεκριμένη γλώσσα (XML) και να ζητείται γενικά η δυνατότητα παραμετροποίησης και δημιουργίας custom κανόνων ανίχνευσης.

Γ. Επιχειρησιακό Ρίσκο και Άσκοπη Επιβάρυνση του Δημοσίου (Total Cost of Ownership)

Η εισαγωγή υπερβολικά εξειδικευμένων ή «φωτογραφικών» προδιαγραφών, οι οποίες υποχρεώνουν τον Οργανισμό σε μια βίαιη και καθολική αντικατάσταση του υφιστάμενου λογισμικού ασφαλείας (rip-and-replace), έρχεται σε αντίθεση με την αρχή της χρηστής δημοσιονομικής διαχείρισης. Μια τέτοια προσέγγιση συνεπάγεται:

- Υψηλό Λειτουργικό Ρίσκο: Η μαζική απεγκατάσταση και επανεγκατάσταση κεντρικά διαχειριζόμενων agents σε μια εκτεταμένη και γεωγραφικά διεσπαρμένη υποδομή (όπως αυτή των αποκεντρωμένων μονάδων της 1ης ΥΠΕ) δημιουργεί αναπόφευκτα ένα κρίσιμο «παράθυρο μετάβασης» (migration window) με σοβαρά κενά ασφαλείας.

- Απώλεια Ανθρώπων & Τεχνογνωσίας: Απαιτείται η εκ νέου παραμετροποίηση πολιτικών ασφαλείας, κανόνων και εξαιρέσεων από μηδενική βάση, καθώς και η δαπανηρή επανεκπαίδευση του

τεχνικού προσωπικού σε ένα εντελώς νέο περιβάλλον διαχείρισης, ακυρώνοντας την τεχνογνωσία που έχει αποκτηθεί επί σειρά ετών.

- **Κρυφά Κόστη Υλοποίησης:** Όταν η αγορά επιτρέπει την ομαλή, αρθρωτή και ελεγχόμενη αναβάθμιση (upgrade) μιας υφιστάμενης υποδομής, η επιλογή της ολικής αντικατάστασης επιβαρύνει άσκοπα τον προϋπολογισμό του έργου με κόστη υπηρεσιών εγκατάστασης που θα μπορούσαν να αποφευχθούν.

Πέρα από επιμέρους τεχνικούς όρους που εισάγουν αδικαιολόγητους περιορισμούς, η παρούσα διατύπωση των προδιαγραφών οδηγεί *de facto* σε βίαιη αλλαγή της υφιστάμενης αρχιτεκτονικής ασφαλείας του Οργανισμού. Μια τέτοια εξέλιξη συνεπάγεται σοβαρούς κινδύνους για την επιχειρησιακή συνέχεια και υπέρογκα κρυφά κόστη, τα οποία έρχονται σε ευθεία αντίθεση με τις αρχές της χρηστής δημοσιονομικής διαχείρισης

Κατόπιν των ανωτέρω, ζητούμε την τροποποίηση των προαναφερθέντων όρων, ώστε να επιτραπεί η συμμετοχή όλων των αναγνωρισμένων κατασκευαστών λογισμικού ασφαλείας. Με τον τρόπο αυτό, ο Φορέας θα διασφαλίσει τη μέγιστη δυνατή οικονομική και τεχνική προσφορά, αποφεύγοντας παράλληλα ένα κοστοβόρο και υψηλού ρίσκου *migration* που θέτει σε κίνδυνο την καθημερινή του λειτουργία.

Απαντήσεις στο 1^ο Σχόλιο

1. Προδιαγραφές 2.13 & 2.14 — Ασφαλής Περιηγητής / Secure Browser

Η απαίτηση για secure browser ή ασφαλές περιβάλλον περιήγησης είναι τεχνικά εύλογη και δεν αποτελεί χαρακτηριστικό μόνο consumer προϊόντων.

Οι browsers αποτελούν βασικό σημείο εισόδου επιθέσεων. Το CIS Control 9 αναφέρεται ειδικά σε “Email and Web Browser Protections”, αναγνωρίζοντας ότι οι browsers είναι συχνό σημείο εισόδου για επιθέσεις σε enterprise περιβάλλοντα.

Το Secure Browser προσθέτει protections που δεν είναι ισοδύναμα με ένα απλό web filter:

- προστασία της browser memory από inspection άλλων processes,
- προστασία browser data από άλλες εφαρμογές,
- protection έναντι screen capture/screen recording,
- keyboard protection έναντι keyloggers,
- clipboard protection,
- έλεγχο browser extensions,
- scanning των JavaScript scripts που εκτελούνται στον browser.

Αυτό έχει πραγματική security αξία. Το MITRE ATT&CK αναγνωρίζει ξεχωριστά το Credentials from Web Browsers – T1555.003, συμπεριλαμβανομένης της προσπάθειας ανάγνωσης browser credential stores ή browser process memory, καθώς και το Input Capture / Keylogging – T1056.001.

Web/Traffic Filtering, SSL/TLS Inspection δεν είναι τεχνικά ισοδύναμη με την αρχική απαίτηση.

Web filtering/HTTPS inspection προστατεύει κυρίως την κίνηση. Secure Browser προστατεύει επιπλέον το execution context, memory, keyboard, clipboard και screen του browser.

2. Προδιαγραφή 2.16 — Cluster μεταξύ Windows Server Agents

Η απαίτηση είναι τεχνικά δικαιολογημένη και πρέπει να παραμείνει.

Δεν αφορά απλή εφαρμογή πολιτικών από κεντρική κονσόλα. Αφορά την ασφαλή και σωστή λειτουργία του antivirus/endpoint agent μέσα σε Windows Failover Cluster ή NLB περιβάλλον.

Η Microsoft αναφέρει ότι antivirus software που δεν είναι cluster-aware μπορεί να δημιουργήσει προβλήματα σε Cluster Services, όπως resource failures ή προβλήματα κατά τη μετακίνηση ενός group σε άλλο node. Αναφέρει επίσης ότι οι antivirus filter drivers μπορεί να μην κατανοούν σωστά το shared disk model και να επηρεάσουν το failover.

Είναι σημαντικό διότι τα clustered workloads έχουν ειδική λειτουργική συμπεριφορά. Η ίδια η Microsoft προειδοποιεί ότι antivirus software που δεν είναι cluster-aware μπορεί να δημιουργήσει προβλήματα στα Cluster Services, όπως failures σε resources και προβλήματα κατά τη μετακίνηση workloads από node σε

node. Μάλιστα συστήνει ρητά χρήση cluster-aware antivirus και συνεννόηση με τον security vendor για interoperability.

[Antivirus software that isn't cluster-aware may cause problems with Cluster Services](#)

3. Προδιαγραφή 2.17 — Scan εικονικών δίσκων Hyper-V online/offline

Καταρχάς, η ίδια η Microsoft εξακολουθεί να αντιμετωπίζει ενεργά τα .vhd και .vhdx ως Hyper-V security objects και δίνει συγκεκριμένες οδηγίες antivirus configuration για Hyper-V hosts. Δεν θεωρεί επομένως τη host-level interaction με virtual disks κάποια παρωχημένη έννοια.

[Recommended antivirus exclusions for Hyper-V hosts](#)

Η απαίτηση για δυνατότητα σάρωσης VHD/VHDX είναι τεχνικά εύλογη, εφόσον εφαρμόζεται ελεγχόμενα και με σωστή παραμετροποίηση.

Η Microsoft αναγνωρίζει ρητά ότι σε Hyper-V hosts υπάρχουν ειδικά αρχεία που χρειάζονται προσοχή από antivirus software, όπως VHD, VHDX, AVHD και AVHDX. Επίσης αναφέρει ότι σε enterprise Windows Server περιβάλλοντα η σάρωση συγκεκριμένων αρχείων μπορεί να προκαλέσει θέματα απόδοσης ή αξιοπιστίας λόγω file locking, γι' αυτό χρειάζεται σωστή πολιτική exclusions και scanning.

Αυτό δεν σημαίνει ότι η δυνατότητα σάρωσης είναι παρωχημένη. Σημαίνει ότι πρέπει να υπάρχει η δυνατότητα, αλλά να χρησιμοποιείται με σωστό scheduling, exclusions και πολιτικές ώστε να μην επηρεάζεται ο Hypervisor.

Επομένως, η προδιαγραφή μπορεί να παραμείνει, γιατί ζητά κρίσιμη δυνατότητα ελέγχου εικονικών δίσκων και όχι ανεξέλεγκτο real-time scanning.

Για παράδειγμα, ένα offline VM μπορεί να είναι:

- shutdown,
- template,
- dormant VM,
- παλαιό workload,
- forensic image,
- VM που δεν μπορεί να bootάρει,
- VM χωρίς ενεργό security agent.

Σε αυτές τις περιπτώσεις ο in-guest EDR/EPP agent προφανώς δεν λειτουργεί.

Το host-side/offline scanning συνεπώς παρέχει ανεξάρτητο inspection capability.

Παράλληλα, η Microsoft προειδοποιεί να μην γίνεται αυθαίρετο mount άγνωστων VHDs επειδή μπορεί να εκθέσει τον host σε filesystem-level attacks. Αυτό ακριβώς ενισχύει την αξία ενός security mechanism που έχει σχεδιαστεί ειδικά για virtual-disk inspection αντί για ad-hoc mounting.

[Plan for Hyper-V security in Windows Server](#)

Η δυνατότητα σάρωσης των virtual disks (.VHD/.VHDX) σε online και offline κατάσταση αποτελεί σημαντικό πρόσθετο επίπεδο ασφάλειας, καθώς επιτρέπει την ανίχνευση κακόβουλου λογισμικού ακόμη και όταν η εικονική μηχανή δεν βρίσκεται σε λειτουργία ή ο μηχανισμός προστασίας εντός του guest OS δεν είναι ενεργός. Με αυτόν τον τρόπο παρέχεται ανεξάρτητος έλεγχος του περιεχομένου των VMs και ενισχύεται η συνολική κάλυψη του περιβάλλοντος Hyper-V στο πλαίσιο μιας προσέγγισης Defense in Depth.

Το «θα προκαλεί AV storm και θα γονατίζει τον hypervisor» δεν είναι τεχνικά αποδεκτό ως γενική θέση.

4. Προδιαγραφή 9.10 — Custom EDR/XDR Rules σε XML

Ένα GUI δεν είναι ισοδύναμο με machine-readable rule representation.

Ένα structured definition επιτρέπει:

- deterministic definition του rule,
- export/import,
- version control,
- backup,
- audit,
- automated deployment,

- **programmatic manipulation,**
- **rule portability μεταξύ instances του ίδιου προϊόντος,**
- **review/change control,**
- **integration με APIs και automation.**

Αυτό έχει ιδιαίτερη αξία σε SOC/EDR περιβάλλον.

Η απαίτηση XML διασφαλίζει ότι ο Φορέας έχει πλήρη πρόσβαση στη λογική των detection rules σε structured format για auditing, backup, reuse, automation και change management, αντί η παραμετροποίηση να παραμένει αποκλειστικά κλειδωμένη σε vendor GUI.

Αυτό δεν αποτελεί τεχνική απόδειξη ότι πρέπει να αλλάξουν οι specifications.

Ο ισχυρισμός ότι οι προδιαγραφές δημιουργούν υποχρεωτικό “rip-and-replace” δεν τεκμηριώνεται τεχνικά από μόνος του. Δε σημαίνει ότι η Αναθέτουσα Αρχή πρέπει να μειώσει τις τεχνικές απαιτήσεις για να αποφύγει πιθανή μετάβαση. Σημαίνει ότι η μετάβαση, εφόσον απαιτηθεί, πρέπει να γίνει οργανωμένα, με σχέδιο υλοποίησης, σταδιακή εγκατάσταση και ελεγχόμενο migration window.

Το σωστό είναι να αξιολογηθεί συνολικό TCO:

License + deployment + migration + training + operational cost + security capability + support lifecycle.

Όχι:

κόστος migration = λόγος αφαίρεσης τεχνικών απαιτήσεων.

- pilot,
- staged rollout,
- migration groups,
- tested uninstall/install procedures,
- monitoring,
- rollback,
- change management,
- maintenance windows.

Δεν είναι μείωση των security requirements.

2° Σχόλιο

Αξιότιμοι κύριοι / Αξιότιμες κυρίες,

Στο πλαίσιο της δημόσιας διαβούλευσης και με γνώμονα τη διασφάλιση των θεμελιωδών αρχών της ίσης μεταχείρισης, της διαφάνειας και της ευρείας συμμετοχής, υποβάλλουμε με το παρόν τις τεχνικά και νομικά τεκμηριωμένες παρατηρήσεις μας επί του σχεδίου των Τεχνικών Προδιαγραφών για τον υπόψη διαγωνισμό. Στόχος μας είναι η βελτιστοποίηση του τεύχους ώστε να επιτρέπει την υγιή ανάπτυξη του ανταγωνισμού, προς όφελος του Δημοσίου.

Όπως ρητά ορίζεται στο Άρθρο 54 του Ν. 4412/2016, οι τεχνικές προδιαγραφές πρέπει να επιτρέπουν την ισότιμη πρόσβαση των οικονομικών φορέων στη διαδικασία ανάθεσης και να μην εισάγουν αδικαιολόγητα εμπόδια στο άνοιγμα των δημόσιων συμβάσεων στον ανταγωνισμό. Κατά την ολική αξιολόγηση του υπό διαβούλευση τεύχους, εντοπίζονται δομικοί όροι που εισάγουν υπέρμετρους περιορισμούς, φωτογραφίζοντας συγκεκριμένες αρχιτεκτονικές και ορολογίες, με αποτέλεσμα τον αδικαιολόγητο αποκλεισμό κορυφαίων, διεθνώς αναγνωρισμένων και πιστοποιημένων λύσεων της αγοράς.

Στην ενότητα «Αντικλή Προστασία» (Προδιαγραφή 2.6) γίνεται αναφορά σε ενδεικτικές τεχνολογίες *advanced heuristics* χρησιμοποιώντας ονομασίες όπως «DNA, smart signatures».

Οι συγκεκριμένες εκφράσεις αποτελούν εμπορικές ορολογίες και τεχνολογίες συγκεκριμένου κατασκευαστικού οίκου. Η χρήση τους, ακόμη και ενδεικτικά, δημιουργεί ασάφεια και στρεβλώνει την αντικειμενικότητα της αξιολόγησης. Βάσει της παραγράφου 4 του Άρθρου 54 του Ν. 4412/2016, οι τεχνικές

προδιαγραφές δεν επιτρέπεται να παραπέμπουν σε συγκεκριμένη προέλευση, εμπορικά σήματα ή διπλώματα ευρεσιτεχνίας.

- **Πρόταση Τροποποίησης:** Να απαλειφθούν οι συγκεκριμένες ονομασίες και ο όρος να διαμορφωθεί με τεχνολογικά ουδέτερο τρόπο: «Να υποστηρίζονται προηγμένες τεχνολογίες ευρετικής ανάλυσης (Advanced Heuristics), ανάλυσης συμπεριφοράς (Behavioral Analysis) και Μηχανικής Μάθησης (Machine Learning) για τη δυνατότητα ανίχνευσης άγνωστου κακόβουλου λογισμικού (malware)».

2. Περιορισμός Αρχιτεκτονικής Υλοποίησης σε Επίπεδο Endpoint

Στην Προδιαγραφή 2.16 ζητείται η δυνατότητα του προγράμματος σε Windows Server να λειτουργεί ως cluster με σκοπό τον συγχρονισμό δεδομένων και ρυθμίσεων (π.χ. Windows failover cluster nodes, network load balancing nodes).

Η απαίτηση αυτή επιβάλλει μια πολύ συγκεκριμένη αρχιτεκτονική προσέγγιση σε επίπεδο τοπικού λειτουργικού συστήματος. Οι πλέον σύγχρονες, enterprise λύσεις ασφάλειας (Cloud-native ή με κεντρικά Virtual Appliances) πραγματοποιούν τον απόλυτο συγχρονισμό πολιτικών, configurations και ειδοποιήσεων απευθείας μέσω της κεντρικής κονσόλας διαχείρισης. Με τον τρόπο αυτό καλύπτεται πλήρως και με ασφαλέστερο τρόπο η λειτουργική ανάγκη της Αναθέτουσας Αρχής, χωρίς να επιβαρύνονται τα endpoint nodes με τοπικά clusters. Ο υφιστάμενος όρος αποκλείει αδικαιολόγητα ηγετικούς κατασκευαστές.

- **Πρόταση Τροποποίησης:** Να τροποποιηθεί η προδιαγραφή ώστε να εστιάζει στο λειτουργικό αποτέλεσμα της κεντρικής διαχείρισης: «Να διασφαλίζεται ο αυτόματος συγχρονισμός δεδομένων, πολιτικών και ρυθμίσεων σε όλα τα nodes (συμπεριλαμβανομένων περιβαλλόντων windows failover cluster, network load balancing κ.λπ.) είτε τοπικά, είτε μέσω της κεντρικής κονσόλας διαχείρισης, ώστε να εξασφαλίζεται ταυτόσημη παραμετροποίηση».

3. Ονομαστικές Πιστοποιήσεις Τρίτων Οργανισμών

Στις Προδιαγραφές 1.4 και 1.5 ζητούνται σωρευτικά συγκεκριμένοι ονομαστικοί τίτλοι πιστοποιήσεων από τους οργανισμούς AV-Comparatives («Business Security Approved» και «Real World Protection Advanced») και AV-TEST GmbH («Approved Corporate Endpoint Protection - TOP Product») για τα τελευταία 2 έτη τουλάχιστον.

Η προσήλωση σε πολύ συγκεκριμένους ονομαστικούς τίτλους βραβείων (οι οποίοι συχνά αλλάζουν ονομασία ανά έτος) ενδέχεται να οδηγήσει σε τυπικό αποκλεισμό κορυφαίων λογισμικών που κατέχουν εξίσου ανώτατες βαθμολογίες και εγκεκριμένες πιστοποιήσεις ασφάλειας (Approved) στους ίδιους οργανισμούς. Για την πιστή τήρηση της αρχής της ισοδυναμίας (παρ. 4, Άρθρο 54, Ν. 4412/2016), κάθε απαίτηση για πιστοποιητικό πρέπει να επιτρέπει το ισοδύναμο.

- **Πρόταση Τροποποίησης:** Προτείνεται να προστεθεί ρητά η φράση «ή ισοδύναμη πιστοποίηση/διάκριση» και οι όροι να διαμορφωθούν ως εξής: «Το σύστημα προστασίας να διαθέτει επίσημη πιστοποίηση/έγκριση ως αναγνωρισμένο επιχειρηματικό προϊόν ασφάλειας (Approved Business/Corporate Security Product) από ανεξάρτητους οργανισμούς δοκιμών (ενδεικτικά AV-Comparatives, AV-TEST ή ισοδύναμους) για τα τελευταία 2 έτη».

4. Ανάγκη Οριζόντιας Ρήτρας Ισοδυναμίας στις Τεχνικές Απαιτήσεις

Ενώ στο Παράρτημα II η Αναθέτουσα Αρχή αναγνωρίζει ορθώς την αρχή της ισοδυναμίας για τα πιστοποιητικά διασφάλισης ποιότητας ISO, δεν υπάρχει αντίστοιχη ρητή, οριζόντια πρόβλεψη για τις τεχνικές προδιαγραφές του ίδιου του λογισμικού.

- **Πρόταση / Παρέμβαση:** Ζητείται η προσθήκη γενικού όρου στο σώμα της διακήρυξης: «Όπου στις τεχνικές προδιαγραφές αναφέρονται συγκεκριμένα πρότυπα, ελάχιστες απαιτήσεις συστήματος, χωρητικότητες ή

μεθοδολογίες, γίνονται δεκτές και προσφορές που αποδεικνύουν με ισοδύναμο τρόπο ότι ικανοποιούν πλήρως τις λειτουργικές απαιτήσεις και τις ανάγκες ασφάλειας της Αναθέτουσας Αρχής».

Με τις ανωτέρω απαραίτητες τροποποιήσεις, η Αναθέτουσα Αρχή θωρακίζει νομικά τη διαγωνιστική διαδικασία, εναρμονίζεται πλήρως με την εθνική και ευρωπαϊκή νομολογία περί δημοσίων συμβάσεων και διασφαλίζει ότι θα λάβει τις πλέον σύγχρονες, τεχνολογικά προηγμένες και οικονομικά συμφέρουσες προσφορές που προσφέρει η παγκόσμια αγορά κυβερνοασφάλειας.

Απαντήσεις στο 2° Σχόλιο

Για την αναφορά σε DNA / Smart Signatures

Δεν κρίνεται απαραίτητη η απαλοιφή των αναφορών, εφόσον αυτές χρησιμοποιούνται ενδεικτικά για να περιγράψουν το επιθυμητό τεχνικό επίπεδο ανίχνευσης και όχι ως υποχρέωση συγκεκριμένου κατασκευαστή.

Η απαίτηση αφορά προηγμένη προστασία από κακόβουλο λογισμικό με χρήση υπογραφών, ευρετικής ανάλυσης και μη υπογραφικών τεχνικών ανίχνευσης. Αυτό είναι σύμφωνο με τη διεθνή πρακτική. Το NIST αναφέρει ότι οι μηχανισμοί προστασίας από κακόβουλο κώδικα περιλαμβάνουν τόσο signature-based όσο και non-signature-based τεχνολογίες, όπως τεχνικές τεχνητής νοημοσύνης και heuristics για ανίχνευση συμπεριφοράς κακόβουλου κώδικα όταν οι υπογραφές δεν επαρκούν.

Επομένως, η απαίτηση είναι τεχνικά βάσιμη. Δεν ζητά εμπορικό προϊόν, αλλά συγκεκριμένο επίπεδο ανίχνευσης. Αν χρειάζεται διευκρίνιση, μπορεί να αναφερθεί ότι γίνονται αποδεκτές ισοδύναμες τεχνολογίες, χωρίς να αλλάξει η ουσία της προδιαγραφής.

Για τη λειτουργία σε Windows Server Cluster

Η απαίτηση πρέπει να παραμείνει, γιατί δεν αφορά απλή κεντρική διαχείριση πολιτικών. Αφορά την ορθή λειτουργία του endpoint security agent σε περιβάλλοντα υψηλής διαθεσιμότητας, όπως Windows Failover Cluster και Network Load Balancing.

Η Microsoft αναφέρει ξεκάθαρα ότι antivirus software που δεν είναι cluster-aware μπορεί να δημιουργήσει απρόβλεπτα προβλήματα σε Cluster Services, όπως resource failures ή προβλήματα κατά τη μετακίνηση ενός group σε άλλο node. Επίσης αναφέρει ότι οι antivirus filter drivers μπορεί να μην κατανοούν σωστά το shared disk model και να επηρεάσουν το failover.

Antivirus software that isn't cluster-aware may cause problems with Cluster Services

Άρα η απαίτηση για σωστή λειτουργία σε clustered περιβάλλον δεν είναι περιορισμός αρχιτεκτονικής. Είναι τεχνική απαίτηση διαθεσιμότητας, σταθερότητας και ασφαλούς λειτουργίας κρίσιμων servers.

Για τις πιστοποιήσεις AV-Comparatives και AV-TEST

Η απαίτηση για συγκεκριμένες ανεξάρτητες πιστοποιήσεις είναι τεχνικά αιτιολογημένη, γιατί παρέχει αντικειμενικό και επαληθεύσιμο τρόπο αξιολόγησης της ποιότητας της λύσης.

Το AV-Comparatives αναφέρει ότι για να λάβει ένα προϊόν την πιστοποίηση “Approved Business Product”, πρέπει να επιτύχει συγκεκριμένα ελάχιστα ποσοστά σε Malware Protection και Real-World Protection, με αυστηρά όρια στα false positives και στις επιδόσεις.

Αντίστοιχα, το AV-TEST αξιολογεί τα προϊόντα σε Protection, Performance και Usability, με μέγιστη βαθμολογία 18 μονάδες, ενώ το “TOP PRODUCT” αποδίδεται σε προϊόντα με βαθμολογία από 17,5 και άνω.

Συνεπώς, οι πιστοποιήσεις αυτές δεν φωτογραφίζουν κατασκευαστή. Θέτουν ελάχιστο επίπεδο ποιότητας, με βάση ανεξάρτητες και δημοσιευμένες δοκιμές. Η απαίτηση για κάλυψη των τελευταίων δύο ετών είναι εύλογη, γιατί δείχνει σταθερή απόδοση και όχι τυχαία ή περιστασιακή επιτυχία.

Για τη γενική ρήτρα ισοδυναμίας

Δεν απαιτείται πρόσθετη γενική ρήτρα που να αποδυναμώνει όλες τις τεχνικές απαιτήσεις. Το Άρθρο 54 του Ν. 4412/2016 ήδη προβλέπει ότι οι τεχνικές προδιαγραφές μπορούν να διατυπώνονται ως επιδόσεις ή λειτουργικές απαιτήσεις, αρκεί να είναι σαφείς και επαρκώς προσδιορισμένες.

Το ίδιο άρθρο προβλέπει επίσης την αποδοχή ισοδύναμων λύσεων, όταν ο προσφέρων αποδεικνύει με κατάλληλα μέσα ότι η λύση του καλύπτει τις απαιτήσεις.

Επομένως, η ισοδυναμία υπάρχει ήδη στο θεσμικό πλαίσιο. Η προσθήκη μιας υπερβολικά γενικής ρήτρας μπορεί να δημιουργήσει ασάφεια στην αξιολόγηση και να επιτρέψει προσφορές που δεν καλύπτουν πλήρως το ζητούμενο τεχνικό επίπεδο.