Αθήνα, 30/07/2026
Α. Π.: 28427 ΕΞ 2026

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΕΠΙΤΕΛΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ
ΔΙΕΥΘΥΝΣΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΤΜΗΜΑ ΑΠΑΙΤΗΣΕΩΝ ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Ταχ. δ/νση : Χανδρή 1 & Θεσσαλονίκης
Τ.Κ. : 183 45 Μοσχάτο
Πληροφορίες : Α. Σταμούλης
Τηλέφωνο : 210 4802916
Email : a.stamoulis@cyber.gov.gr

ΠΡΟΣ:

Όπως Πίνακας Αποδεκτών

(Αποστολή με ηλεκτρονικό ταχυδρομείο)

ΘΕΜΑ: Διαχείριση ευπαθειών πληροφοριακών συστημάτων από τις βασικές οντότητες του ν. 5160/2024.

ΣΧΕΤ: α. Ο ν. 5160/2024 (Α’ 195)

β. Η ΚΥΑ 1689/2025 (Β΄ 2186)

1. Η εκμετάλλευση μη αποκατεστημένων ευπαθειών (unpatched vulnerabilities) σε μη ενημερωμένα συστήματα, αποτελεί μία από τις συχνότερες μεθόδους με τις οποίες οι επιτιθέμενοι αποκτούν μη εξουσιοδοτημένη πρόσβαση σε πληροφοριακά αγαθά οργανισμών, προκειμένου να επιτελέσουν τους κακόβουλους σκοπούς τους. Παράλληλα, τα εργαλεία τεχνητής νοημοσύνης έχουν εξελιχθεί σε τέτοιο βαθμό, ώστε ο χρόνος που μεσολαβεί από τη δημοσίευση μίας ενημέρωσης ασφάλειας (security patch) μέχρι την ανάπτυξη του κακόβουλου κώδικα εκμετάλλευσης της ευπάθειας (exploit) έχει μειωθεί εκθετικά, από διάστημα μηνών ακόμη και σε μερικές ώρες, περιορίζοντας σημαντικά το διαθέσιμο χρόνο αντίδρασης των αμυνόμενων και καθιστώντας τις ενέργειές τους απολύτως επείγουσες.

2. Η Εθνική Αρχή Κυβερνοασφάλειας, λαμβάνοντας υπόψη τις εξελίξεις αυτές, καθώς και τις υποχρεώσεις που απορρέουν από τα α’ και β’ σχετικά για τις βασικές οντότητες του ν. 5160/2024, παραθέτει πλαίσιο οδηγιών για την αποτελεσματική διαχείριση των τεχνικών ευπαθειών των πληροφοριακών τους συστημάτων:

Α. Διαχείριση των ενημερώσεων ασφάλειας

Αναπτύξτε διαδικασίες διαχείρισης των ενημερώσεων λογισμικού (software updates) και των ενημερώσεων ασφάλειας (security patches), με σκοπό την έγκαιρη υλοποίησή τους σε λειτουργικά συστήματα και εφαρμογές. Για το πλάνο προτεραιοποίησης των ενεργειών αποκατάστασης / επιδιόρθωσης της ευπάθειας, εφαρμόστε κριτήρια επικινδυνότητας ως εξής:

(1) *Είναι το ευπαθές πληροφοριακό αγαθό εκτεθειμένο στο διαδίκτυο;*

Οι οντότητες δύνανται να εφαρμόσουν διάφορες μεθόδους εύρεσης των αγαθών τους που είναι προσβάσιμα μέσω δημοσίων δικτύων, όπως ενδεικτικά

εξωτερικές σαρώσεις δικτύου (π.χ. Nmap), εξωτερικές σαρώσεις ευπαθειών, υπηρεσίες αναζήτησης εκτεθειμένων συστημάτων όπως το Shodan (shodan.io), λύσεις External Attack Surface Management (EASM), καθώς και, συμπληρωματικά, εργαλεία EDR (Endpoint Detection and Response), εργαλεία NAC (Network Access Control) και εργαλεία asset management.

(2) *Έχει επιβεβαιωθεί ότι η ευπάθεια αποτελεί αντικείμενο ενεργούς εκμετάλλευσης;*

Μία βασική πηγή πληροφόρησης για την εν λόγω παράμετρο αποτελεί ο κατάλογος KEV (Known Exploited Vulnerabilities Catalog) της Υπηρεσίας Κυβερνοασφάλειας και Ασφάλειας Υποδομών των ΗΠΑ (Cybersecurity and infrastructure Security Agency – CISA), ο οποίος περιλαμβάνει ευπάθειες για τις οποίες υπάρχουν επιβεβαιωμένα στοιχεία ενεργούς εκμετάλλευσης (actively exploited).

(3) *Είναι οι επιτιθέμενοι ικανοί να αυτοματοποιήσουν όλα τα απαραίτητα βήματα για την εκμετάλλευση της ευπάθειας;*

Τα εν λόγω βήματα είναι: (α) η συλλογή πληροφοριών για το στόχο (reconnaissance), όπως π.χ. emails προσωπικού, ανοικτές δικτυακές θύρες και πιθανές ευπάθειες, (β) η ανάπτυξη κακόβουλου κώδικα (weaponization), (γ) η αποστολή του κακόβουλου κώδικα στο στόχο (delivery), π.χ μέσω phishing emails ή μολυσμένων ιστότοπων και (δ) η εκμετάλλευση (exploitation), όπου ο κακόβουλος κώδικας εκτελείται στα συστήματα του στόχου. Πρόκειται για τα βήματα 1 – 4 του “Cyber Kill Chain”.

(4) Τεχνικός *αντίκτυπος (technical impact): μετά την εκμετάλλευση της ευπάθειας, οι επιτιθέμενοι αποκτούν μερικό ή πλήρη έλεγχο του ευπαθούς πληροφοριακού αγαθού;*

Παράδειγμα μερικού ελέγχου (partial control) αποτελεί μία επίθεση άρνησης υπηρεσίας (denial-of-service attack). Παραδείγματα πλήρους ελέγχου (total control) αποτελούν η δυνατότητα του επιτιθέμενου να εγκαταστήσει και να εκτελέσει αυθαίρετο κώδικα (arbitrary code), η πρόσβασή του σε διαχειριστικό λογαριασμό (administrator / root) του ευπαθούς αγαθού, το υψηλό (high) CVSS score της ευπάθειας για τις μετρικές “Confidentiality & Integrity Impact” κ.α.

Για τα σημεία 3 και 4 ανωτέρω, οι οντότητες δύνανται να λαμβάνουν ενημέρωση μέσω δημοφιλών ιστοτόπων, όπως το cve.org, που πλέον περιέχει, μεταξύ άλλων, πληροφόρηση και για τα πεδία Automatable: yes / no και Technical Impact: total / partial.

Στο συνημμένο παράρτημα παρατίθεται πίνακας με συνιστώμενα χρονοδιαγράμματα για τις ενέργειες αποκατάστασης των οργανισμών, ανάλογα με το συνδυασμό των απαντήσεων στα 4 παραπάνω κριτήρια. Επισημαίνεται ότι τα ως άνω κριτήρια επικινδυνότητας, καθώς και τα χρονοδιαγράμματα του πίνακα, αποτελούν, πλέον, εμπεδωμένη διεθνή πρακτική η οποία αποτυπώνεται και σε νομικά δεσμευτικές οδηγίες άλλων κρατών. Στο πλαίσιο αυτό, τονίζεται ότι με βάση το συνδυασμό των απαντήσεων στον πίνακα, υπάρχουν περιπτώσεις ευπαθειών που χρήζουν άμεσης αποκατάστασης **εντός τριών ημερών το αργότερο**.

Β. Δοκιμές των ενημερώσεων ασφάλειας

Διενεργήστε δοκιμές (testing) των ενημερώσεων ασφάλειας πριν την εγκατάστασή τους σε παραγωγικό περιβάλλον, σε όσα συστήματα αυτό απαιτείται βάσει

της κρισιμότητας του συστήματος και του δυνητικού επιχειρησιακού αντικτύπου. Το μέτρο εφαρμόζεται με σκοπό τον εντοπισμό τυχόν προβλημάτων που ενδέχεται να ανακύψουν, όπως διακοπές λειτουργίας συστημάτων, ασυμβατότητες λογισμικού ή μειωμένη απόδοση. Οι εν λόγω δοκιμές δύνανται να διενεργούνται χειρωνακτικά (manually) ή μέσω αυτοματοποιημένων μεθόδων.

Γ. Λήψη αυτοματοποιημένων ενημερώσεων

Διασφαλίστε τη λήψη αυτοματοποιημένων ενημερώσεων και ενημερώσεων ασφάλειας για τα λειτουργικά συστήματα Windows και για τα προγράμματα περιήγησης στο διαδίκτυο (web browsers) στους σταθμούς εργασίας χρηστών. Όπου απαιτείται προηγούμενος έλεγχος συμβατότητας ή λειτουργικότητας, εφαρμόστε μηχανισμούς σταδιακής ανάπτυξης, ώστε οι ενημερώσεις να εγκαθίστανται αρχικά σε περιορισμένο αριθμό συστημάτων και στη συνέχεια στο σύνολο των σταθμών εργασίας.

Δ. Σαρώσεις ευπαθειών

Διενεργήστε τακτικές σαρώσεις ευπαθειών (vulnerability scans) στα πληροφοριακά σας συστήματα με χρήση αυτοματοποιημένων εργαλείων. Τα εν λόγω εργαλεία εμφανίζουν αποτελέσματα για: (i) μη ενημερωμένα (unpatched) συστήματα, (ii) λειτουργίες, θύρες, πρωτόκολλα ή υπηρεσίες που δεν θα έπρεπε να είναι προσβάσιμα σε χρήστες ή συσκευές και (iii) λανθασμένες παραμετροποιήσεις (misconfigurations). Η συχνότητα των σαρώσεων είναι ανάλογη με την κρισιμότητα των συστημάτων και του επιπέδου κινδύνου. Γενικά, η συχνότητα συνίσταται να είναι σε μηνιαία βάση ή και νωρίτερα, ανάλογα με τις δυνατότητες της οντότητας. *Δώστε απόλυτη προτεραιότητα στους διακομιστές και στις δικτυακές συσκευές που είναι προσβάσιμες από το διαδίκτυο*.

Ε. Πλάνο αντιμετώπισης ευπαθειών

Αναπτύξτε πλάνο αντιμετώπισης των ευπαθειών που ανακαλύπτονται κατά τη διαδικασία των σαρώσεων, ορίζοντας σαφείς ρόλους, αρμοδιότητες και ευθύνες και λαμβάνοντας υπόψη παραμέτρους όπως είναι η κρισιμότητα των ευπαθών συστημάτων και το γενικότερο περιβάλλον κινδύνου. Ενέργειες αντιμετώπισης της ευπάθειας δύνανται να είναι:

(1) η πλήρης αποκατάσταση / επιδιόρθωσή της (remediation), όπως ενδεικτικά η εφαρμογή ενημέρωσης ασφάλειας (software patch) με βάση τις οδηγίες του κατασκευαστή ή η αφαίρεση / απόσυρση του ευπαθούς συστήματος.

(2) ο μετριασμός των επιπτώσεών της (impact mitigation) στις περιπτώσεις όπου η αποκατάσταση δεν είναι εφικτή ή άμεση, με ενέργειες όπως ενδεικτικά την αφαίρεση προεπιλεγμένων συνθηματικών (default credentials), τη διαμερισματοποίηση του δικτύου, την αλλαγή των κανόνων του firewall, την υλοποίηση ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA), την καταγραφή και παρακολούθηση συμβάντων κ.α.

Στις περιπτώσεις κατά τις οποίες η αποκατάσταση μιας ευπάθειας δεν είναι άμεσα εφικτή ή αποφασίζεται η μη εφαρμογή διαθέσιμης ενημέρωσης ασφάλειας, η σχετική απόφαση θα πρέπει να τεκμηριώνεται επαρκώς, να εφαρμόζονται κατάλληλα αντισταθμιστικά μέτρα ασφάλειας και να παρακολουθείται ο υπολειπόμενος κίνδυνος έως την οριστική αντιμετώπιση της ευπάθειας.

Στ. Εντοπισμός πηγών πληροφόρησης

Εντοπίστε αξιόπιστες και αναγνωρισμένες πηγές πληροφόρησης σχετικές με ευπάθειες τεχνολογιών πληροφορικής και επικοινωνιών, όπως είναι κατασκευαστές και προμηθευτές λογισμικού, ομάδες απόκρισης για περιστατικά κυβερνοασφάλειας (CSIRTs) ή αρμόδιες κρατικές Αρχές.

Ζ. Αντικατάσταση πεπαλαιωμένων συστημάτων

Υλοποιήστε, κατά προτεραιότητα, πλάνο άμεσης αντικατάστασης των λειτουργικών συστημάτων και του εξοπλισμού πληροφορικής που δεν λαμβάνουν, πλέον, από τον κατασκευαστή ενημερώσεις ασφάλειας και τεχνική υποστήριξη.

3. Με βάση τα παραπάνω, οι βασικές οντότητες του ν. 5160/2024 πρέπει να επικαιροποιούν τις πολιτικές και διαδικασίες διαχείρισης ευπαθειών, συμπεριλαμβανομένων των ρόλων και αντίστοιχων ευθυνών, ώστε να προσαρμόζονται στα νέα δεδομένα. Η διαχείριση ευπαθειών πρέπει να αποτελεί μία συνεχή δραστηριότητα για τους οργανισμούς και απαιτεί οργάνωση, χρόνο, δέουσα προσοχή και πόρους.

Για κάθε ζήτημα σχετικά με την εφαρμογή της παρούσας μπορείτε να επικοινωνείτε με την αρμόδια Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας της Γενικής Διεύθυνσης Επιτελικού Σχεδιασμού (email : **dir.strategy@cyber.gov.gr**). Η Εθνική Αρχή Κυβερνοασφάλειας, στο πλαίσιο του ρόλου και της αποστολής της, παραμένει στη διάθεση των φορέων για κάθε τυχόν αναγκαία διευκρίνιση και περαιτέρω καθοδήγηση για την υλοποίηση των μέτρων της παρούσας.

Ο ΔΙΟΙΚΗΤΗΣ ΤΗΣ ΕΘΝΙΚΗΣ ΑΡΧΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Μ. ΜΠΛΕΤΣΑΣ

ΠΑΡΑΡΤΗΜΑ

Συνιστώμενο χρονοδιάγραμμα αποκατάστασης ευπαθειών

	Η ευπάθεια είναι εκτεθειμένη στο διαδίκτυο;	Η ευπάθεια αποτελεί αντικείμενο ενεργούς εκμετάλλευσης;	Τα βήματα εκμετάλλευσης της ευπάθειας μπορούν να αυτοματοποιηθούν από τον επιτιθέμενο;	Ποιος είναι ο τεχνικός αντίκτυπος της ευπάθειας;	Συνιστώμενο μέγιστο χρονοδιάγραμμα για ενέργειες αποκατάστασης
1	Ναι	Ναι	Ναι	Πλήρης έλεγχος	3 ημέρες
2	Ναι	Ναι	Ναι	Μερικός έλεγχος	3 ημέρες
3	Ναι	Ναι	Όχι	Πλήρης έλεγχος	3 ημέρες
4	Ναι	Ναι	Όχι	Μερικός έλεγχος	14 ημέρες
5	Ναι	Όχι	Ναι	Πλήρης έλεγχος	3 ημέρες
6	Ναι	Όχι	Ναι	Μερικός έλεγχος	14 ημέρες
7	Ναι	Όχι	Όχι	Πλήρης έλεγχος	14 ημέρες
8	Ναι	Όχι	Όχι	Μερικός έλεγχος	60 ημέρες
9	Όχι	Ναι	Ναι	Πλήρης έλεγχος	3 ημέρες
10	Όχι	Ναι	Ναι	Μερικός έλεγχος	14 ημέρες
11	Όχι	Ναι	Όχι	Πλήρης έλεγχος	14 ημέρες
12	Όχι	Ναι	Όχι	Μερικός έλεγχος	14 ημέρες
13	Όχι	Όχι	Ναι	Πλήρης έλεγχος	60 ημέρες
14	Όχι	Όχι	Ναι	Μερικός έλεγχος	60 ημέρες
15	Όχι	Όχι	Όχι	Πλήρης έλεγχος	Αποκατάσταση κατά την επόμενη αναβάθμιση του συστήματος
16	Όχι	Όχι	Όχι	Μερικός έλεγχος	Αποκατάσταση κατά την επόμενη αναβάθμιση του συστήματος

ΠΙΝΑΚΑΣ ΑΠΟΔΕΚΤΩΝ

ΠΡΟΣ ΕΝΕΡΓΕΙΑ:

1. Υπεύθυνοι Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.) των βασικών οντοτήτων

2. Γραφεία Υπουργών, Υφυπουργών, Αναπληρωτών Υπουργών:

- Υπουργείο Εθνικής Οικονομίας και Οικονομικών
- Υπουργείο Εξωτερικών
- Υπουργείο Εθνικής Άμυνας
- Υπουργείο Εσωτερικών
- Υπουργείο Παιδείας, Θρησκευμάτων και Αθλητισμού
- Υπουργείο Υγείας
- Υπουργείο Προστασίας του Πολίτη
- Υπουργείο Υποδομών και Μεταφορών
- Υπουργείο Περιβάλλοντος και Ενέργειας
- Υπουργείο Ανάπτυξης
- Υπουργείο Εργασίας και Κοινωνικής Ασφάλισης
- Υπουργείο Δικαιοσύνης
- Υπουργείο Πολιτισμού
- Υπουργείο Μετανάστευσης και Ασύλου
- Υπουργείο Κοινωνικής Συνοχής και Οικογένειας
- Υπουργείο Ναυτιλίας και Νησιωτικής Πολιτικής
- Υπουργείο Αγροτικής Ανάπτυξης και Τροφίμων
- Υπουργείο Τουρισμού
- Υπουργείο Ψηφιακής Διακυβέρνησης
- Υπουργείο Κλιματικής Κρίσης και Πολιτικής Προστασίας

3. Γραφεία Γραμματέων Αποκεντρωμένων Διοικήσεων:

- Αποκεντρωμένη Διοίκηση Αττικής
- Αποκεντρωμένη Διοίκηση Μακεδονίας – Θράκης
- Αποκεντρωμένη Διοίκηση Ηπείρου – Δυτικής Μακεδονίας
- Αποκεντρωμένη Διοίκηση Θεσσαλίας – Στερεάς Ελλάδας
- Αποκεντρωμένη Διοίκηση Πελοποννήσου – Δυτικής Ελλάδας και Ιονίου
- Αποκεντρωμένη Διοίκηση Αιγαίου
- Αποκεντρωμένη Διοίκηση Κρήτης

4. Γραφεία Προέδρων:

- Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)
- Ανώτατο Συμβούλιο Επιλογής Προσωπικού (ΑΣΕΠ)
- Εθνικό Συμβούλιο Ραδιοτηλεόρασης (ΕΣΡ)
- Συνήγορος του Πολίτη
- Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Ανεξάρτητη Αρχή Δημοσίων Εσόδων (ΑΑΔΕ)

- Ελληνική Στατιστική Αρχή (ΕΛΣΤΑΤ)
- Ρυθμιστική Αρχή Ενέργειας (ΡΑΕ)
- Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)
- Επιτροπή Ανταγωνισμού
- Επιτροπή Κεφαλαιαγοράς
- Εθνική Αρχή Διαφάνειας (ΕΑΔ)
- Συνήγορος του Καταναλωτή

5. Γραφεία Διοικητών:

- Τράπεζα της Ελλάδος (ΤτΕ)
- Αρχή Πολιτικής Αεροπορίας (ΑΠΑ)
- Υπηρεσία Πολιτικής Αεροπορίας (ΥΠΑ)

ΚΟΙΝΟΠΟΙΗΣΗ:

1. Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ) / Ε5
2. Εθνική Υπηρεσία Πληροφοριών (Ε.Υ.Π.) / Διεύθυνση Κυβερνοχώρου

ΕΣΩΤΕΡΙΚΗ ΔΙΑΝΟΜΗ:

1. Διοικητής Εθνικής Αρχής Κυβερνοασφάλειας
2. Υποδιοικητής Α’ Εθνικής Αρχής Κυβερνοασφάλειας
3. Υποδιοικητής Β’ Εθνικής Αρχής Κυβερνοασφάλειας
4. Γενική Διεύθυνση Επιχειρησιακού Σχεδιασμού
5. Γενική Διεύθυνση Επιτελικού Σχεδιασμού
6. Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας
7. Τμήμα Απαιτήσεων και Αρχιτεκτονικής Ασφάλειας