

7 – 13 ΣΕΠΤΕΜΒΡΙΟΥ 2026

Define Resilience Brief

Η εβδομάδα αναδεικνύει τρεις άμεσες προτεραιότητες για τις ελληνικές επιχειρήσεις: υποχρεωτική αναφορά κυβερνοπεριστατικών βάσει του Cyber Resilience Act, διαχείριση του κινδύνου κακόβουλης χρήσης AI και ετοιμότητα για τη νέα φάση χρηματοδότησης μέσω Ταμείου Ανάκαμψης.

01

CYBERSECURITY • CRA • INCIDENT RESPONSE

Ο Cyber Resilience Act φέρνει άμεση υποχρέωση αναφοράς κυβερνοπεριστατικών

Από τις 11 Σεπτεμβρίου, κάθε κατασκευαστής προϊόντων με ψηφιακά στοιχεία στην ΕΕ οφείλει να αναφέρει σοβαρά περιστατικά εντός 24 ωρών - ανεξαρτήτως μεγέθους επιχείρησης.

ΓΕΓΟΝΟΣ:

Από τις 11 Σεπτεμβρίου 2026, όλοι οι κατασκευαστές προϊόντων με ψηφιακά στοιχεία που διατίθενται στην ΕΕ υποχρεούνται να αναφέρουν ενεργά εκμεταλλευόμενες ευπάθειες και σοβαρά περιστατικά μέσω της πλατφόρμας της ENISA, βάσει του Κανονισμού για την Κυβερνοανθεκτικότητα (Cyber Resilience Act). Η υποχρέωση ισχύει ανεξαρτήτως μεγέθους επιχείρησης.

ΣΗΜΑΣΙΑ:

Το χρονοδιάγραμμα αναφοράς είναι ιδιαίτερα αυστηρό: αρχική προειδοποίηση εντός 24 ωρών, αναλυτική κοινοποίηση εντός 72 ωρών και τελική αναφορά εντός 14 ημερών από τη διάθεση διορθωτικού μέτρου ή εντός ενός μήνα για σοβαρό περιστατικό. Οι περισσότερες ΜμΕ δεν διαθέτουν ακόμη σαφή διαδικασία vulnerability disclosure, 24ωρη κλιμάκωση, τεχνικά logs και προκαθορισμένη αρμοδιότητα υποβολής αναφοράς. Η πλήρης εφαρμογή του CRA και οι απαιτήσεις σήμανσης CE ακολουθούν στις 11 Δεκεμβρίου 2027.

ΠΟΙΟΙ ΕΠΗΡΕΑΖΟΝΤΑΙ

Εταιρείες λογισμικού, εφαρμογών, IoT και συνδεδεμένων συσκευών, hardware και cybersecurity products, καθώς και επιχειρήσεις που διαθέτουν προϊόν τρίτου με τη δική τους επωνυμία.

ΠΗΓΗ: [Εθνική Αρχή Κυβερνοασφάλειας, 11.09.2026](#) [↗](#)

ACTION - ΤΙ ΝΑ ΕΛΕΓΞΕΤΕ ΑΜΕΣΑ ΓΙΑ ΤΟ CRA:

- Υπάρχει σαφής διαδικασία vulnerability disclosure και ορισμένος υπεύθυνος υποβολής αναφορών προς την ENISA.
- Λειτουργεί μηχανισμός 24ωρου εντοπισμού και κλιμάκωσης ενεργά εκμεταλλευόμενων ευπαθειών.
- Τηρούνται τεχνικά logs που τεκμηριώνουν το χρονοδιάγραμμα 24 ωρών / 72 ωρών / 14 ημερών.
- Έχει ελεγχθεί αν προϊόντα τρίτων που διαθέτετε με δική σας επωνυμία εμπίπτουν στην υποχρέωση αναφοράς.
- Υπάρχει σχέδιο για τις απαιτήσεις σήμανσης CE και πλήρους εφαρμογής του CRA έως τον Δεκέμβριο 2027.

ΕΡΩΤΗΣΗ ΓΙΑ ΤΗ ΔΙΟΙΚΗΣΗ:

- Αν εντοπιστεί σήμερα ενεργά εκμεταλλευόμενη ευπάθεια, γνωρίζουμε ποιος αναφέρει τι, σε ποιον και μέσα σε πόσες ώρες;

02

AI GOVERNANCE • THREAT INTELLIGENCE • CYBERSECURITY

Η κακόβουλη χρήση AI γίνεται μετρήσιμος επιχειρησιακός κίνδυνος

Η Anthropic εντόπισε και διέκοψε περιστατικά χρήσης μοντέλων AI σε κυβερνοεπιθέσεις, απάτες και παραβίαση εταιρικών δεδομένων. Η αγορά AI governance ωριμάζει ταχύτερα από τους ελέγχους των επιχειρήσεων.

ΓΕΓΟΝΟΣ:

Η Anthropic ανακοίνωσε ότι εντόπισε και διέκοψε περιστατικά χρήσης μοντέλων AI σε κυβερνοεπιχειρήσεις και ανάπτυξη κακόβουλου λογισμικού, απάτες και πλαστές ψηφιακές ταυτότητες, επιχειρήσεις επιρροής και παρακολούθησης, προμήθεια dual-use εξοπλισμού, ανάπτυξη λογισμικού για drones και οπλικά συστήματα, καθώς και μη εξουσιοδοτημένη εξαγωγή δυνατοτήτων μοντέλων μέσω τρίτων υπηρεσιών. Η εταιρεία ανέφερε επίσης περιπτώσεις όπου εταιρικά δεδομένα και διαπιστευτήρια χρηστών πέρασαν από μη ελεγχόμενες υπηρεσίες διαμεσολάβησης μοντέλων. Στις 12 Σεπτεμβρίου, ο CEO της Anthropic ζήτησε δημόσια επιβράδυνση της ανάπτυξης ισχυρότερων μοντέλων, ανεξάρτητους αξιολογητές και συντονισμό των μεγάλων εταιρειών AI.

ΣΗΜΑΣΙΑ:

Η αγορά AI governance ωριμάζει ταχύτερα: οι επιχειρήσεις θα χρειάζονται πλέον όχι μόνο AI policy, αλλά κατάλογο εγκεκριμένων εργαλείων, data classification και access controls, απαγόρευση μη ελεγμένων model routers, έλεγχο API keys και εταιρικών μυστικών, logging και ανθρώπινη έγκριση κρίσιμων ενεργειών, καθώς και διαδικασία AI-related incident response. Το εύρημα συνδέεται άμεσα με ISO/IEC 42001, ISO/IEC 27001, Secure SDLC, GDPR και κυβερνοασφάλεια: η AI δεν χρησιμοποιείται πλέον μόνο για σύνταξη παραπλανητικών emails ή κώδικα, αλλά μπορεί να οργανώνει ολόκληρη την ακολουθία μιας επίθεσης.

ΠΟΙΟΙ ΕΠΗΡΕΑΖΟΝΤΑΙ

Οργανισμοί που χρησιμοποιούν GenAI, πάροχοι SaaS και τεχνολογίας, χρηματοοικονομικές υπηρεσίες, υποδομές και δημόσιοι φορείς - κάθε επιχείρηση με πρόσβαση σε API keys, εταιρικά δεδομένα ή μοντέλα AI.

ΠΗΓΗ: [Anthropic — Threat Intelligence Report, 11.09.2026](#) ↗

ACTION - ΤΙ ΝΑ ΕΛΕΓΞΕΤΕ ΑΜΕΣΑ ΓΙΑ ΤΗΝ ΚΑΚΟΒΟΥΛΗ ΧΡΗΣΗ AI:

- Υπάρχει κατάλογος εγκεκριμένων AI εργαλείων και απαγόρευση μη ελεγμένων model routers.
- Εφαρμόζονται data classification και access controls για δεδομένα που εισάγονται σε GenAI εργαλεία.
- Τα API keys και τα εταιρικά μυστικά ελέγχονται, περιστρέφονται και παρακολουθούνται.
- Κρίσιμες ενέργειες μέσω AI agents περνούν από logging, ανθρώπινη έγκριση και ένα σαφές incident response σενάριο.

ΕΡΩΤΗΣΗ ΓΙΑ ΤΗ ΔΙΟΙΚΗΣΗ:

- Αν κάποιος χρησιμοποιούσε σήμερα τα δικά μας AI εργαλεία ή διαπιστευτήρια κακόβουλα, θα το αντιλαμβανόμασταν έγκαιρα;

Νέα κεφάλαια €5 δισ. για τις ΜμΕ ανοίγουν χρηματοδοτικό ορίζοντα

Η μεταφορά κεφαλαίων του Ταμείου Ανάκαμψης στην Ελληνική Αναπτυξιακή Τράπεζα ανοίγει πρόσβαση σε χρηματοδότηση για τις ΜμΕ — αλλά η αξία της θα κριθεί από την ωριμότητα της επένδυσης.

ΓΕΓΟΝΟΣ:

Με κυβερνητική εξαγγελία στις 6 Σεπτεμβρίου, που επιβεβαιώθηκε σε συνέντευξη Τύπου στις 7 Σεπτεμβρίου, ανακοινώθηκε η μεταφορά €1,5 δισ. από το Ταμείο Ανάκαμψης στην Ελληνική Αναπτυξιακή Τράπεζα, με δανειοδοτικό σκέλος €1,1 δισ. και εγγυοδοτικό πυλώνα €400 εκατ. Με την τραπεζική συμμετοχή, η συνολική χρηματοδότηση εκτιμάται ότι μπορεί να φτάσει τα €5 δισ. Πρόκειται ακόμη για εξαγγελία πολιτικής — αναμένονται οι όροι, τα κριτήρια και το χρονοδιάγραμμα των χρηματοδοτικών εργαλείων.

ΣΗΜΑΣΙΑ:

Δημιουργείται πρόσβαση σε κεφάλαια για ΜμΕ που δυσκολεύονται να χρηματοδοτηθούν -ιδίως στη μεταποίηση, τον τουρισμό, τα logistics και την τεχνολογία- ενώ η επιτάχυνση των αποσβέσεων εξοπλισμού από δέκα σε έξι χρόνια ενισχύει τα επενδυτικά κίνητρα. Χωρίς τεκμηριωμένο business case, ρεαλιστικές προβλέψεις και αξιολόγηση λειτουργικών, cyber και supply-chain κινδύνων, αυξάνεται ο κίνδυνος αδυναμίας τραπεζικής τεκμηρίωσης και μη επιλέξιμων δαπανών.

ΠΟΙΟΙ ΕΠΗΡΕΑΖΟΝΤΑΙ

Μεταποίηση, τουρισμός, logistics, τεχνολογία και επιχειρήσεις που σχεδιάζουν παραγωγικό, ψηφιακό ή ενεργειακό εκσυγχρονισμό.

ΠΗΓΗ: [Πρωθυπουργός, 06–07.09.2026](#) ↗

ACTION - ΤΙ ΝΑ ΕΛΕΓΞΕΤΕ ΠΡΙΝ ΑΠΟ ΚΑΘΕ ΧΡΗΜΑΤΟΔΟΤΗΣΗ:

- Υπάρχει τεκμηριωμένο business case που συνδέει το πρόγραμμα με στρατηγικούς στόχους και ρεαλιστικές προβλέψεις.
- Έχει αξιολογηθεί η ετοιμότητα τραπεζικής τεκμηρίωσης πριν από την υποβολή αιτήματος.
- Το risk register καλύπτει λειτουργικούς, cyber και supply-chain κινδύνους της επένδυσης.
- Έχουν οριστεί ρόλοι, ορόσημα, KPIs και ενιαίος φάκελος τεκμηρίωσης εξαρχής.

ΕΡΩΤΗΣΗ ΓΙΑ ΤΗ ΔΙΟΙΚΗΣΗ:

- Είναι το business case μας αρκετά ώριμο ώστε να αντέξει σε τραπεζικό ή ελεγκτικό έλεγχο πριν διεκδικήσουμε τη χρηματοδότηση;

Βοηθάμε οργανισμούς να διαχειρίζονται
κανονιστικούς, ψηφιακούς και λειτουργικούς κινδύνους
με εποπτεία.



Managing risk. Enabling growth.