



Ο εφιάλτης της ιλαράς επιστρέφει στην Ευρώπη

Τα κρούσματα στην ΕΕ και τι συμβαίνει στην Ελλάδα - Αθ. Τσακρής στην «Α»: «Οι γονείς αμελούν τις επαναληπτικές δόσεις»

ΡΕΠΟΡΤΑΖ
Βασίλης Βενιζέλος

Καμπανάκι κινδύνου για την πιθανότητα ευρύτερης διάδοσης της ιλαράς στη Γηραιά Ήπειρο, χτυπάει το Ευρωπαϊκό Κέντρο Ελέγχου και Πρόληψης των Νόσων (ECDC), την ώρα που και στην Ελλάδα η πλήρης εμβολιαστική κάλυψη των παιδιών απέναντι σε έναν από τους πλέον μεταδοτικούς ιούς, σημειώνει πτώση τα τελευταία χρόνια. Αυτός είναι και ο λόγος που δεν επιτρέπεται ο εφησυχασμός, παρά το γεγονός ότι η χώρα μας έχει καταγράψει μόνο ένα εξακριβωμένο κρούσμα από τον Ιούνιο του 2025 έως σήμερα, όταν χώρες της Ευρώπης, ακόμη και της ΕΕ, όπως η Ιταλία, η Βουλγαρία ή και η Ρουμανία, καταγράφουν ήδη εκατοντάδες

κρούσματα της νόσου. Η έκθεση του ECDC για την περίοδο από την 1η Σεπτεμβρίου 2025 έως την 31η Αυγούστου 2026 κατέγραψε συνολικά 2.335 κρούσματα σε 30 χώρες της ΕΕ/ΕΟΧ.

Οι χώρες με τα περισσότερα κρούσματα είναι: Ιταλία 653, Βουλγαρία 564, Ρουμανία 255, Ισπανία 230, Γαλλία 146. Οι ΗΠΑ έχουν ήδη καταγράψει πάνω από 4.400 κρούσματα, δηλαδή σχεδόν τα διπλάσια, σε σχέση με όσα είχαν καταγραφεί για ολόκληρο το 2025.

«ΚΑΝΕΝΑΣ ΕΦΗΣΥΧΑΣΜΟΣ»

Σύμφωνα με τα επιδημιολογικά στοιχεία, που παρουσιάζει στην «Α» ο καθηγητής Μικροβιολογίας της Ιατρικής Σχολής του ΕΚΠΑ και μέλος της Επιτροπής Εμπειρογνομόνων του υπουργείου Υγείας, Αθανάσιος Τσακρής, «στην Ελλάδα, το 2024 καταγράφηκαν 38 περιστατικά και κανένας θάνατος, ενώ το 2025 μόλις τέσσερα κρούσματα και κανένας θάνατος. Οι αριθμοί ίσως φαίνονται καθησυχαστικοί, στην πραγματικότητα όμως δεν πρέπει να οδηγήσουν σε εφησυχασμό. Σύμφωνα με στοιχεία από εκτιμήσεις του ΠΟΥ, της

UNICEF και του ECDC, η κάλυψη των παιδιών στη χώρα μας με την πρώτη δόση μειώθηκε από 97% για το 2019 σε 91% για το 2024, ενώ, με τη δεύτερη, από 76% σε 71%, αντίστοιχα. Φαίνεται ότι ολοένα και πιο συχνά οι Έλληνες γονείς αμελούν τις επαναληπτικές δόσεις ή υποτιμούν τη σημασία τους. Αν αυτή η πτωτική πορεία δεν ανακοπεί, οι αναζωπυρώσεις της νόσου, όπως αυτή του 2017-2018, κατά την οποία καταγράφηκαν περισσότερα από 3.000 περιστατικά, θα είναι όλο και πιο έντονες και απειλητικές».

Σύμφωνα με τον ίδιο, «η ιλαρά δεν αφορά μόνο τα παιδιά. Στην Ελλάδα, το 2024, η μεγαλύτερη ηλικιακή ομάδα μεταξύ των νοσούντων ήταν οι 45-64 ετών, ενώ ακολουθούσαν οι 25-44 ετών. Παράλληλα, το 30% των κρουσμάτων αφορούσε εργαζομένους σε μονάδες Υγείας οι οποίοι ήταν ανεμβολίαστοι ή ατελώς εμβολιασμένοι».

Σημειώνεται ότι η ιλαρά αποτελεί την επόμενη νόσο-στόχο του Παγκοσμίου Οργανισμού Υγείας (ΠΟΥ) προς παγκόσμια εξάλειψη, μετά την πολιομυελίτιδα. ven.ygeia@gmail.com

Ο καθηγητής Μικροβιολογίας της Ιατρικής Σχολής του ΕΚΠΑ, Αθανάσιος Τσακρής



Οι χώρες της ΕΕ με τα περισσότερα κρούσματα

Ιταλία	653
Βουλγαρία	564
Ρουμανία	255
Ισπανία	230
Γαλλία	146

Μέσο: ΤΑ ΝΕΑ

Ημ. Έκδοσης: ...23/10/2026 Ημ. Αποδελτίωσης: ...23/10/2026

Σελίδα: 12



ΤΑ ΝΕΑ ΠΑΡΑΣΚΕΥΗ 23 ΟΚΤΩΒΡΙΟΥ 2026

Τεντωμένα νεύρα για τις συνεργασίες

Παρασκηνιακές εντολές από το Μαξίμου να αποφεύγονται δημόσιες συζητήσεις για πήχεις, κυβερνητικούς εταίρους και εκλογικούς γύρους

ΤΗΣ ΕΛΕΝΗΣ ΕΥΑΓΓΕΛΟΔΗΜΟΥ

Εκνευρισμό προκαλούν στο Μαξίμου οι κατά καιρούς λοξές γαλάζιες ματιές στα δεξιάτερα της ΝΔ, οι οποίες το αναγκάζουν ξανά να κλείνει τη δημόσια συζήτηση για πιθανές μετεκλογικές εξελίξεις – πήχεις, συνεργασίες, δεύτερους ή τρίτους εκλογικούς γύρους. Υπολογισμοί για το μετεκλογικό τοπίο προφανώς και γίνονται στα κομματικά επιτελεία, αλλά όλοι θέλουν να τους κρατούν πίσω από κλειστές πόρτες, αποφεύγοντας ερωτήσεις που τους φέρνουν σε αμηχανία.

Όσο η ΝΔ, το ΠΑΣΟΚ και η ΕΛΑΣ πασχίζουν για νέες δεξαμενές πέραν του σκληρού πυρήνα ψηφοφόρων τους, τόσο ξορκίζουν σιδηρώς απειλεί να υποσκάψει τον μείζονα εκλογικό στόχο, τον οποίο προβάλλουν: για τον Κυριάκο Μητσοτάκη είναι η αυτοδυναμία, για τον Νίκο Ανδρουλάκη η νίκη του ΠΑΣΟΚ ακόμα και με διαφορά μιας ψήφου, για τον Αλέξη Τσίπρα η νίκη της ΕΛΑΣ έναντι της «ποιο διεφθαρμένης κυβέρνησης». Με δεδομένες τις δεξιές πιέσεις και την ανησυχία για εκτεταμένη χαλαρή ψήφο, εφόσον στο μυαλό των εκλογέων προεξοφλείται δεύτερη κάλπη, όπως έδειξε η δημοσκοπήσι της Metron Analysis για το Mega και μάλιστα τηλεοπτικά στο φάσμα αριστέρων – κεντρώων – δεξιών (το 69% προβλέπει ότι θα χρειαστεί να ξαναγίνουν εκλογές), το Μαξίμου τρέχει να μαζέψει τη νεοδημοκρατι-

κή какоφωνία. Ο Μητσοτάκης προσπαθεί να ενισχύσει το αφήγημα της σταθερότητας, αντιπαράβλλοντας το διεθνές σκηνικό και ταυτόχρονα να καλλιεργεί προσδοκίες. «Μόνο αυτή η κυβέρνηση συνομιλεί με το αύριο, άλλες πολιτικές δυνάμεις παραμένουν εγκλωβισμένες στο χθες», έλεγε μέσα στην εβδομάδα από την Αγία Παρασκευή και αντίστοιχα σινάλα αναμένονται στη σημερινή περιοδεία του στα Βρυξέλλες. Παράλληλα, ο αντιπρόεδρος της κυβέρνησης Κωστής Χατζηδάκης περιμένει έως τις 15 Δεκεμβρίου προτάσεις από υπουργούς, βουλευτές και κομματικά μέλη για το προεκλογικό πρόγραμμα της ΝΔ.

Τι δήλωσαν Δένδιας και Μπακογιάννη

Παρά τις κεντρικές προσπάθειες να μένουν εκτός δημόσιας σφαίρας οι απόψεις στελεχών για μετεκλογικά σενάρια, ΝΔ, ΠΑΣΟΚ και ΕΛΑΣ δύσκολα θα αποφεύγουν τέτοιες συζητήσεις όσο πλησιάζει ο εκλογικός ορίζοντας. Ερωτηθείς για την απάντηση Μητσοτάκη περί 25% και διαδικασιών διαδοχής στη ΝΔ, ο Νίκος Δένδιας απέφυγε αριθμητικές αναφορές, σημειώνοντας «με απόλυτη ικανοποίηση και ταύτιση την προσπάθεια για την αυτοδυναμία». Την πεποίθηση ότι ο Μητσοτάκης θα αναλάβει ευθύνες αν η ΝΔ πέσει κάτω από 25% εξέφρασε η Ντόρα Μπακογιάννη, εκτιμώντας ότι η αυτοδυναμία δεν είναι πολύ μακριά

– και κάνοντας λόγο (στο videocast του Γιάννου Παπαχρήστου στον ιστότοπο των «ΝΕΩΝ» - tanea.gr) για όνειρα θερινής νυκτός του Αντώνη Σαμαρά στην ερώτηση αν ο πρώην πρωθυπουργός θα στήριζε μια κυβέρνηση ΝΔ χωρίς τον Μητσοτάκη.

Τα ενδεχόμενα συγκυβέρνησης

Στο μεταξύ σιγόκαιγε η φωτιά που άναψε ο βουλευτής Β' Θεσσαλονίκης, Θεόδωρος Καραγιώργου, με το «δεν πρέπει να είμαστε δογματικοί» και, εφόσον χαθεί η αυτοδυναμία, «θα πρέπει να απευθυνθούμε στα δημοκρατικά κόμματα που είναι δεξιά μας» – από τον Σαμαρά έως τους Κυριάκο Βελόπουλο, Δημήτρη Νατσίου, Αφροδίτη Λατινιόπουλο ακόμα και τη Μαρία Καρυστιανού. Ο ίδιος φάνηκε γρήγορα να στρογγυλεύει τις διατυπώσεις, ενόσω συζητιόταν παρασκηνιακά ότι λόγω της απόφασής του να διεκδικήσει την Περιφέρεια Κεντρικής Μακεδονίας το 2028 επιθυμεί ανοίγματα σε δεξιάτερα ακροατήρια.

Σημειωτέον, η Β' Θεσσαλονίκης είναι από τις δυσκολότερες Περιφέρειες για τη ΝΔ, εξού και οι εισογήσεις να είναι μία από τις τρεις στις οποίες θα είναι υποψήφιος ο Μητσοτάκης το 2027. Πάντως, δεν ήταν η πρώτη φορά που άνοιξε θέμα κόντρα στην επίσημη γραμμή ότι ο Μητσοτάκης «αποκλείει κατηγορηματικά» ενδεχόμενο συγκυβέρνησης με κόμματα «της Ακροδεξιάς και της άλλης όψης του λαϊκισμού». Ακόμα και ο Αδωνης Γεωργιάδης προκαλούσε αναστάτωση προ μηνών λέγοντας «προφανώς θα μιλούσαμε και με τον Σαμαρά» αλλά όχι με όρο «άλλον πρωθυπουργό», ενώ παράθυρο σε κάθε ενδεχόμενο έχει ανοίξει ο βουλευτής Ανατολικής Αττικής Γιώργος Βλάχος. Και σε κάθε περίπτωση ΠΑΣΟΚ και ΕΛΑΣ θα αναδεικνύουν τέτοιες δηλώσεις γαλάζιων για να σπρώχνουν τη ΝΔ δεξιάτερα.



Με δεδομένες τις δεξιές πιέσεις και την ανησυχία για εκτεταμένη χαλαρή ψήφο, το κυβερνητικό επιτελείο τρέχει να μαζέψει τη νεοδημοκρατική какоφωνία, ενώ ο Μητσοτάκης προσπαθεί να ενισχύσει το αφήγημα της σταθερότητας και ταυτόχρονα να καλλιεργεί προσδοκίες

Παρά τις κεντρικές προσπάθειες να μένουν εκτός δημόσιας σφαίρας οι απόψεις στελεχών για μετεκλογικά σενάρια, ΝΔ, ΠΑΣΟΚ και ΕΛΑΣ δύσκολα θα αποφεύγουν τέτοιες συζητήσεις όσο πλησιάζει ο εκλογικός ορίζοντας



FOCUS - 1

Από την Τετάρτη, χιλιάδες ιστούποιοι σε όλο τον πλανήτη αντιμετωπίζουν σοβαρά προβλήματα. Ορισμένοι, ανάμεσά τους και 32 κυβερνητικές πλατφόρμες του Ηνωμένου Βασιλείου, τέθηκαν εκτός λειτουργίας, κυρίως για προληπτικούς λόγους. Κι αυτό διότι λίγο νωρίτερα, το προηγμένο μοντέλο τεχνητής νοημοσύνης (TN) της Anthropic είχε ανακαλύψει τυφλά σημεία (ευαλωτότητες) στη γλώσσα προγραμματισμού PHP, που χρησιμοποιείται περίπου από 7 στις 10 ιστοσελίδες παγκοσμίως.

Τα κενά στον κώδικα φέρονται να διέρρευσαν σε μέσα κοινωνικής δικτύωσης και διαδικτυακά φόρα, προκαλώντας ένα κύμα κυβερνοεπιθέσεων. Παρ' ότι οι διαχειριστές του έσπευσαν να προσφέρουν μια νεότερη και ενημερωμένη έκδοση, υπάρχουν εκατοντάδες χιλιάδες συστήματα παγκοσμίως στα οποία δεν είναι δυνατή η αναβάθμιση, αλλά απαιτείται αντικατάσταση – κάτι που, προφανώς, συνεπάγεται περισσότερο χρόνο και κινδύνους.

Ταυτόχρονα, νέα έρευνα της αμερικανικής εταιρείας κυβερνοασφάλειας Treno έδειξε ότι τα ανεπτυγμένα μοντέλα TN (frontier AI) έχουν τη δυνατότητα να πραγματοποιούν επιτυχημένες κυβερνοεπιθέσεις στο 90% των μηχανημάτων βιομηχανικού ελέγχου (Operating Technology ή OT) που υπάρχουν σε κρίσιμες υποδομές, όπως τα δίκτυα ηλεκτρισμού και υδροδότησης. Μάλιστα, το πρωί της περασμένης Δευτέρας, οι εργαζόμενοι σε περισσότερα από 500 σουπερμάρκετ της Γαλλίας αντίκρισαν μια εικόνα καταστροφής όταν έφτασαν στα καταστήματα. Οι συνθήκες στους διαδρόμους θυμίζουν καύσωνα, χιλιάδες τρόφιμα είχαν χαλάσει και ορισμένα ψυγεία είχαν τυλιχθεί στις φλόγες. Όπως διαπιστώθηκε, το προηγούμενο βράδυ είχε πραγματοποιηθεί μια μεγάλη κλιμακωτή κυβερνοεπίθεση στα κεντρικά συστήματα εξ αποστάσεως ελέγχου που χρησιμοποιούν τα περισσότερα σουπερμάρκετ της χώρας. Πρόκειται για μηχανήματα OT της δανικής Danfoss, στα οποία ήταν ήδη γνωστό ότι υπήρχαν κενά ασφαλείας. Οι επιτιθέμενοι – που δεν έχουν ακόμη ταυτοποιηθεί – χάκαραν το σύστημα και ανέβασαν τη θερμοκρασία των ψυγείων στους 50 βαθμούς Κελσίου, με καταστροφικές συνέπειες και σημαντικές οικονομικές ζημιές.

Οι κίνδυνοι στην Ελλάδα

Σε αυτό το φόντο, είναι λογικό να τίθεται το ερώτημα πόσο προστατευμένοι είναι οι ελληνικές επιχειρήσεις και υποδομές απέναντι σε ενδεχόμενη κυβερνοεπίθεση. «Ο τραπεζικός τομέας, οι τηλεπικοινωνίες και η ενέργεια εμφανίζουν παραδοσιακά υψηλότερη ωριμότητα στην κυβερνοασφάλεια, κυρίως λόγω της αυστηρότερης εποπτείας και των σημαντικών επενδύσεων που έχουν πραγματοποιήσει. Αντίθετα, μεγαλύτερες προκλήσεις εντοπίζονται στην υγεία, στη δημόσια διοίκηση, στις μεταφορές και σε επιχειρήσεις που χρησιμοποιούν παλαιά βιομηχανικά συστήματα», υπογραμμίζει στα «ΝΕΑ» ο καθηγητής Ψηφιακών



Πόσο και γιατί μας απειλούν οι κυβερνοεπιθέσεις;

Ορισμένοι τομείς θεωρείται πως έχουν επαρκή θωράκιση, ιδιαίτερα ευάλωτα παραμένουν όμως πολλά συστήματα ■ Τι προβλέπει και σε ποιον βαθμό έχει εφαρμοστεί η ευρωπαϊκή Οδηγία ■ Μιλούν στα «ΝΕΑ» ειδικοί και ο υποδιοικητής της Εθνικής Αρχής Κυβερνοασφάλειας

Συστημάτων στο Πανεπιστήμιο Πειραιώς (ΠΑΠΕΠ) Χρήστος Ξενάκης. «Αυτή η εικόνα επιβεβαιώνεται σε ευρωπαϊκό επίπεδο και από τις αξιολογήσεις του ENISA (η Υπηρεσία Κυβερνοασφάλειας της ΕΕ). Στην Ελλάδα, ιδιαίτερα προσοχή απαιτείται επίσης στις μικρομεσαίες επιχειρήσεις, όπου συχνά οι διαθέσιμοι πόροι και η τεχνολογία είναι περιορισμένοι», προσθέτει ο ίδιος. «Οι κυριότερες αδυναμίες είναι η χρήση παλαιού λογισμικού, η καθυστέρηση στην εγκατάσταση ενημερώσεων ασφαλείας, οι ανεπαρκείς έλεγχοι πρόσβασης, η ελλιπής εκπαίδευση του προσωπικού και η απουσία δοκιμασμένων σχεδίων αντιμετώπι-

ZOOM ΣΤΑ «ΝΕΑ»

ΣΥΝΤΟΝΙΣΜΟΣ
ΠΑΡΩΣ ΠΑΛΟΠΟΥΛΟΣ

ΓΡΑΦΕΙ
ΠΕΤΡΟΣ ΚΩΝΣΤΑΝΤΙΝΙΔΗΣ

σης περιστατικών» υπερθεματίζει ο Διομίδης Σπινέλλης, καθηγητής στο Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας του Οικονομικού Πανεπιστημίου Αθηνών (ΟΠΑ). Όπως λέει από την πλευρά του στα «ΝΕΑ» ο γενικός διευθυντής της εταιρείας κυβερνοασφάλειας Odyssey Cybersecurity, Απόστολος Πανδρούλας, τα ελληνικά σουπερμάρκετ είναι εκτεθειμένα σε αντίστοιχους κινδύνους, καθώς χρησιμοποιούν παρόμοιες τεχνολογίες με τα γαλλικά για τα ψυγεία τους. «Οι περισσότεροι δεν έχουν κάνει τις απαραίτητες επενδύσεις. Δεν αντιλαμβάνονται τον κίνδυνο από κυβερνοεπιθέσεις και δεν θέτουν

την ασφάλεια ως προτεραιότητα», επισημαίνει. Επιπλέον, αναφέρει ότι βιομηχανίες πρώτων υλών και φαρμακοβιομηχανίες βρίσκονται επίσης αρκετά πίσω σε αυτό το ζήτημα.

SOS για τις ενεργειακές υποδομές

Ο υποδιοικητής της Εθνικής Αρχής Κυβερνοασφάλειας (ΕΑΚ), Δημήτρης Ζαμπακόλας, υπογραμμίζει: «Ο κίνδυνος δεν περιορίζεται στα σουπερμάρκετ, αφού αντίστοιχες συσκευές ελέγχου φυσικών διεργασιών (OT) χρησιμοποιούνται στην παραγωγή, την ενέργεια, την ύδρευση και πολλές άλλες κρίσιμες υποδομές. Οι συσκευές αυτές έχουν μια ιδιαιτερότητα: το λογισμικό τους συνήθως δεν ενημερώνεται τακτικά, όπως ενός υπολογιστή ή κινητού, καθώς έχουν σχεδιαστεί για να λειτουργούν αδιάλειπτα επί σειρά ετών».

Πρόσφατη έρευνα της ολλανδικής Αρχής Κυβερνοασφάλειας και της εταιρείας Modat διαπίστωσε ότι χιλιάδες συστήματα αναεώσιμων πηγών ενέργειας (ΑΠΕ) ανά την Ευρώπη αντιμετωπίζουν υψηλό κίνδυνο κακορρύθμισης. Σύμφωνα με την έρευνα, υπάρχουν περισσότερα από 8.500 εκτεθειμένα συστήματα σε 35 χώρες, με την Ελλάδα να βρίσκεται στη δεύτερη θέση στα φωτοβολταϊκά, με 1.860 ελεγχτές ηλιακών πάρκων να είναι απευθείας συνδεδεμένοι στο Διαδίκτυο και επομένως να αντιμετωπίζουν μεγαλύτερο κίνδυνο. Στην πρώτη θέση βρίσκεται η Ισπανία, ενώ τα περισσότερα εκτεθειμένα αιολικά διαθέτει η Γερμανία.

«Ο διαχωρισμός των δικτύων αποκτά ιδιαίτερη σημασία. Κρίσιμα συστήματα και υποδομές θα πρέπει να λειτουργούν σε περιβάλλον



απομονωμένο από το Διαδίκτυο, καθώς ο απομακρυσμένος έλεγχος μέσω Διαδικτύου καθιστά τα συστήματα αυτά ιδιαίτερος ευάλωτα. Όταν η απομακρυσμένη σύνδεση είναι πραγματικά απαραίτητη, θα πρέπει να πραγματοποιείται μόνο μέσω ασφαλών καναλιών, όπως ένα ειδικό ιδιωτικό δίκτυο (VPN), με ισχυρή ταυτοποίηση των χρηστών, πρόσβαση αυστηρά περιορισμένη σε όσους τη χρειάζονται και καταγραφή κάθε ενέργειας», επισημαίνει ο υποδιοικητής της ΕΑΚ.

«Εξίσου σημαντική είναι η συντήρηση του εξοπλισμού: όχι μόνο η τακτική εγκατάσταση των ενημερώσεων ασφαλείας, αλλά και η έγκαιρη ανανέωσή του, ώστε να μην παραμένουν σε λειτουργία συσκευές που έχουν φτάσει στο τέλος του κύκλου ζωής τους (End of Life) και δεν υποστηρίζονται πλέον από τον κατασκευαστή», συνεχίζει.

Εκθετιμένοι και ο δημόσιος τομέας

Τα συστήματα του Δημοσίου είναι επίσης αρκετά εκτεθειμένα σε κυβερνοεπιθέσεις. Ιδιαίτερα μέρηνα απαιτείται για τα νοσοκομεία, στα συστήματα των οποίων διατηρούνται ιατρικοί φάκελοι ασθενών, ενώ μια ενδεχόμενη βλάβη στα δίκτυά τους θα μπορούσε να οδηγήσει σε μια πραγματικά ανθρωπιστική καταστροφή. «Δεν έχει ληφθεί μέριμνα για τα λειτουργικά μηχανήματα στην Ελλάδα ακόμα και στα νοσοκομεία», αναφέρει ο επικεφαλής της Odyssey Cybersecurity.

Από την ΕΑΚ κρούουν τον κώδωνα του κινδύνου και για τους οργανισμούς τοπικής αυτοδιοίκησης (ΟΤΑ), που από τα τέλη Νοεμβρίου

θα υπάγονται στο εθνικό πλαίσιο εποπτείας της NIS2 (η Ευρωπαϊκή Οδηγία για την Κυβερνοασφάλεια). «Η πρόκληση είναι ιδιαίτερα σημαντική για τους δήμους, καθώς μια κυβερνοεπιθεση μπορεί να διακόψει υπηρεσίες που επηρεάζουν άμεσα την καθημερινότητα των πολιτών», προειδοποιεί ο Δ. Ζαμπάκας. «Πρόκειται για ουσιαστικές απαιτήσεις διαχείρισης κινδύνων, προστασίας συστημάτων και αναστολής σημαντικών περιστατικών, όχι απλώς για μια γραφειοκρατική - τυπική διαδικασία. Τον Μάρτιο του 2026 προκηρύχθηκε από την ΕΔΥΤΕ ειδικό έργο ενίσχυσης της κυβερνοασφάλειας των ΟΤΑ που προβλέπει εξοπλισμό, αξιολογήσεις κινδύνων, τεχνικούς ελέγχους ασφαλείας, υπηρεσίες παρακολούθησης και εκπαίδευση».

«Οι οργανισμοί δεν πρέπει να διατάσσονται να δηλώνουν ένα περιστατικό στην ΕΑΚ από φόβο για τις πιθανές συνέπειες. Η δήλωση δεν είναι ομολογία αποτυχίας, είναι πράξη υπευθυνότητας και συλλογικής άμυνας. Όσο περισσότερα περιστατικά δηλώνονται τόσο πληρέστερη είναι η εικόνα που έχει η Αρχή για το πραγματικό επίπεδο κυβερνοασφάλειας της χώρας και τόσο πιο πιθανό είναι να εντοπιστούν έγκαιρα οργανωμένες επιθέσεις και εκστρατείες που στοχεύουν ταυτόχρονα πολλούς οργανισμούς», σημειώνει επίσης.

Δεν υπάρχει 100% ασφάλεια

«Η αποτελεσματικότητα της εποπτείας θα εξαρτηθεί από τη διαθεσιμότητα εξειδικευμένου προσωπικού, την τεχνική υποδομή και την ικανότητα διενέργειας ουσιαστικών ελέγχων.

Απαιτείται συνεχής ενίσχυση των επιχειρησιακών της δυνατοτήτων και συνεργασία με την επιστημονική κοινότητα και την αγορά. Η επιτυχία δεν θα κριθεί μόνο από τον αριθμό των επιχειρήσεων που θα εγγραφούν στο σχετικό μητρώο, αλλά κυρίως από το επίπεδο ασφάλειας που θα επιτευχθεί στην πράξη», επισημαίνει ο Χρ. Ξενάκης.

«Εκτός ότι οι μεγαλύτεροι και πιο οργανωμένοι φορείς μπορούν να επιτύχουν ικανοποιητικό επίπεδο συμμόρφωσης μέσα στα επόμενα ένα έως δύο χρόνια. Για μικρότερους ή λιγότερο ώριμους οργανισμούς, η διαδικασία ενδέχεται να απαιτήσει περισσότερο χρόνο. Ο ρεαλιστικός στόχος είναι μέσα στην επόμενη τριετία να έχει διαμορφωθεί ένα ουσιαστικά υψηλότερο επίπεδο κυβερνοανθεκτικότητας στη χώρα», προσθέτει ο καθηγητής του ΠΑΠΕΙ.

Ωστόσο, όλοι τονίζουν ότι η κυβερνοασφάλεια δεν είναι μια διαδικασία με οριστικό τέλος. «Δεν είναι ένας στόχος που επιτυγχάνεται οριστικά, αλλά μια συνεχής διαδικασία προσαρμογής σε νέες τεχνολογίες και νέες απειλές» υπογραμμίζει ο Δ. Σπινέλλης. «Όσα μέτρα και αν ληφεί ένας οργανισμός, ποτέ δεν μπορεί να θεωρείται 100% ασφαλής. Ο στόχος δεν είναι να εξασφαλίσουμε μηδενικό κίνδυνο, αλλά να περιορίζουμε την πιθανότητα μιας επίθεσης και, κυρίως, τις συνέπειές της όταν αυτή συμβεί», λέει και ο Δ. Ζαμπάκας.

Agentic AI

Πράγματι, καθώς νέες τεχνολογίες μπαίνουν στην ζωή μας, το επίπεδο των κυβερνοεπιθέσεων γίνεται ολοένα και υψηλότερο. «Η ΤΝ επιτρέπει στους επιτιθέμενους να αυτοματοποιούν εργασίες και να δημιουργούν πιο πειστικές απόπειρες εξαπάτησης. Σε πολλές περιπτώσεις, μάλιστα, χρησιμοποιούνται πλέον αυτόνομοι πράκτορες (Agentic AI), εξελίξη που έχει μειώσει δραματικά τον χρόνο προετοιμασίας: 6,1 παλαιότερα απαιτούσε μήνες σχεδιασμού, σήμερα μπορεί να οργανωθεί μέσα σε λίγες ώρες», υπογραμμίζει ο υποδιοικητής της ΕΑΚ. «Η ίδια τεχνολογία, βεβαίως, μπορεί να ενισχύσει και την άμυνα, βοηθώντας στην ταχύτερη ανίχνευση και ανάλυση απειλών, για αυτό και είναι επιτακτική η όσο το δυνατόν ταχύτερη ενσωμάτωσή της».

Ο Απόστολος Πανδρόυλας διαπιστώνει ότι το τελευταίο διάστημα παρατηρείται αύξηση ειδικά στα συστήματα Internet of Things (IoT), δηλαδή σε συσκευές που είναι συνδεδεμένες στο Διαδίκτυο, αλλά και στα συστήματα βιομηχανικών λειτουργιών (OT). Ο Γιάννης Ιωαννίδης, καθηγητής στο τμήμα Πληροφορικής και Τηλεπικοινωνιών του ΕΚΠΑ, υπογραμμίζει ότι σήμερα, οι επιθέσεις γίνονται συχνά με υβριδικό τρόπο, δηλαδή τόσο στον ψηφιακό όσο και στον φυσικό κόσμο. Σημειώνει, δε, ότι καταγράφεται αύξηση στις κυβερνοεπιθέσεις με γεωπολιτικό κίνητρο. «Υπάρχουν χώρες που έχουν στρατίες ολόκληρες για την πραγματοποίηση κυβερνοεπιθέσεων» λέει και επισημαίνει ότι έχουν καταγραφεί και στην Ελλάδα αρκετά περιστατικά επιθέσεων από μη φιλικά διακείμενα γειτονικά κράτη.

Η κρίσιμη διετία

Η NIS2 είναι η Οδηγία της ΕΕ που θέτει το πλαίσιο για την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων στην Ευρώπη. Εχει ψηφιστεί από το 2022 και απαιτεί από τα κράτη-μέλη να ενισχύσουν τις ικανότητές τους στον τομέα της κυβερνοασφάλειας, εισάγοντας παράλληλα μέτρα διαχείρισης κινδύνων και απαιτήσεις υποβολής εκθέσεων για περιστατικά, ενώ παράλληλα θεσπίζει κανόνες για τη συνεργασία, την ανταλλαγή πληροφοριών, την ανταλλαγή πληροφοριών, την εποπτεία και την επιβολή των μέτρων. Η Ελλάδα ήταν η έβδομη χώρα στην ΕΕ που ενσωμάτωσε την Οδηγία στην εθνική νομοθεσία, με τον ν. 5160/2024.

Τομές υψηλής κρισιμότητας

Η NIS2 ορίζει 11 τομείς της οικονομίας που χαρακτηρίζονται υψηλής κρισιμότητας και ακόμα 7 που επίσης θεωρούνται κρίσιμοι, αλλά σε μικρότερο βαθμό. Στην κατηγορία των τομών υψηλής κρισιμότητας συμπεριλαμβάνονται οι εξής: ενέργεια, μεταφορές, τράπεζες, χρηματοπιστωτικές αγορές, υγεία, δίκτυο πόσιμου νερού, λύματα, ψηφιακές υποδομές (data centers κ.λπ.), υπηρεσίες πληροφορικής και κυβερνοασφάλειας, δημόσια διοίκηση και ο τομέας του Διαστήματος. Στη δεύτερη κατηγορία κρισιμότητας βρίσκουμε τις ταχυδρομικές υπηρεσίες και ταχυμεταφορές, τη διαχείριση αποβλήτων, τα χημικά προϊόντα, τα τρόφιμα, τις κατασκευές και τη μεταποίηση, τους ψηφιακούς παρόχους (π.χ. πλατφόρμες κοινωνικής δικτύωσης) και τον τομέα της έρευνας. Υπεύθυνη για την εποπτεία της εφαρμογής της NIS2 στην Ελλάδα είναι η ΕΑΚ, που δημιουργήθηκε μόλις το 2024. «Η NIS2 και οι χρηματοδοτήσεις δημιουργούν το πλαίσιο, αλλά το αποτέλεσμα θα κριθεί στην εφαρμογή. Το ζητούμενο για όλους - επιχειρήσεις, δημόσια διοίκηση και δήμους - είναι κοινό: να προλαμβάνουν όσο μπορούν, να αντιδρούν έγκαιρα και να ανακαμπτουν με ασφάλεια» υπογραμμίζει ο υποδιοικητής της Αρχής. Η ΕΑΚ διαθέτει στην ιστοσελίδα της πλατφόρμα για την εγγραφή των επιχειρήσεων που αφορά η NIS2 στο αντίστοιχο μητρώο, αλλά και πλατφόρμα για τη δήλωση περιστατικών κυβερνοασφάλειας. Η αλήθεια, ωστόσο, είναι ότι μέχρι την επαρκή εφαρμογή της NIS2 υπάρχει μεγάλη απόσταση που πρέπει να διανυθεί. «Θα χρειαστούν περίπου 2-3 χρόνια για να υπάρχει επαρκής κάλυψη βάσει της NIS2. Η ΕΑΚ πείθει ώστε να γίνει το συντομότερο δυνατόν, όμως το σημαντικότερο είναι να το αντιληφθούν τα μέλη των διοικητικών συμβουλίων των εταιρειών που αφορά η Οδηγία», λέει ο Απόστολος Πανδρόυλας. Προσθέτει, δε, ότι η τεχνολογία είναι ώριμη και το οικοσύστημα των εταιρειών που δραστηριοποιούνται στην Ελλάδα έχουν τη δυνατότητα να δώσουν τις απαιτούμενες λύσεις.

«Οι κυριότερες αδυναμίες είναι η χρήση παλαιού λογισμικού, η καθυστέρηση στην εγκατάσταση ενημερώσεων ασφαλείας, οι ανεπαρκείς έλεγχοι πρόσβασης, η ελλιπής εκπαίδευση του προσωπικού και η απουσία δοκιμασμένων σχεδίων αντιμετώπισης περιστατικών», υπερθεματίζει ο Διομήδης Σπινέλλης, καθηγητής στο Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας του Οικονομικού Πανεπιστημίου Αθηνών