Προστατεύοντας το Σήμερα, Οργανώνοντας το Αύριο

Τελευταία ενημέρωση 04/02/2025

ΧΑΙΡΕΤΙΣΜΟΙ - ΟΜΙΛΙΕΣ : **Η κυβερνοασφάλεια μπορεί και πρέπει να αποτελέσει τομέα συνεργασίας Ελλάδας - Κύπρου**

Την κρισιμότητα συνεργασίας ανάμεσα σε Ελλάδα και Κύπρο σε θέματα κυβερνοασφάλειας υπογράμμισαν ο Υπουργός Ψηφιακής Διακυβέρνησης **Δημήτρης Παπαστεργίου** και ο Υφυπουργός Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής της Κυπριακής Δημοκρατίας Δρ. Νικόδημος Δαμιανού, κατά την έναρξη του 1ου Cyber Intelligence Summit για την κυβερνοπληροφορία και την κυβερνοασφάλεια, που διοργανώνεται από τις εταιρείες Viewmax Media και Fnews Media στο Μέγαρο Μουσικής Αθηνών υπό την αιγίδα του υπουργείου Ψηφιακής Διακυβέρνησης.

Στην ανάγκη οργάνωσης και πρόληψης ακολουθώντας τις ευρωπαϊκές κατευθύνσεις στάθηκε, κατά την τοποθέτησή του ο Υπουργός Ψηφιακής Διακυβέρνησης Δημήτρης Παπαστεργίου, υπογραμμίζοντας τη σημασία της συνεργασίας με την Κυπριακή Δημοκρατία πάνω σε ζητήματα κυβερνοασφάλειας. «Η κυβερνοασφάλεια μπορεί και πρέπει να αποτελέσει τομέα συνεργασίας», σημείωσε από την πλευρά του ο κ. Δαμιανού, τονίζοντας πως η έννοια ενιαίου αμυντικού χώρου ίσως να μπορεί να εφαρμοστεί και στον κυβερνοχώρο.
«Θα πρέπει να οργανωθούμε», υπογράμμισε ο Υπουργός Ψηφιακής Διακυβέρνησης Δημήτρης Παπαστεργίου, κατά την έναρξη του συνεδρίου, τονίζοντας πως η κυβερνοασφάλεια αποτελεί προτεραιότητα για τον δημόσιο και τον ιδιωτικό τομέα, καθώς οι υβριδικές απειλές γίνονται όλο και πιο «έξυπνες», αλλά και με πολλαπλασιαστικό πιθανό αρνητικό αντίκτυπο.

Ο Υπουργός Ψηφιακής Διακυβέρνησης προανήγγειλε ότι μέσα στο επόμενο διάστημα πρόκειται να τεθεί σε δημόσια διαβούλευση το νομοσχέδιο για την πλήρη και αποτελεσματική εφαρμογή στην ελληνική έννομη τάξη της «Πράξης για τη διακυβέρνηση δεδομένων» (Κανονισμός (ΕΕ) 2022/868), που παρουσιάστηκε κατά το πρόσφατο Υπουργικό Συμβούλιο.

Αναφερθείς στις κινήσεις που έχει υλοποιήσει η κυβέρνηση, με στόχο την ενδυνάμωση της κυβερνοασφάλειας τους δημοσίου τομέα, εστίασε στη δημιουργία της νέας Εθνικής Αρχής Κυβερνοασφάλειας, καθώς και στην ενσωμάτωση από τον περασμένο Νοέμβριο της νέας ευρωπαϊκής οδηγίας NIS2, η οποία θεσπίζει ένα ενιαίο νομικό πλαίσιο για τη διατήρηση της κυβερνοασφάλειας σε 18 κρίσιμους τομείς σε ολόκληρη την ΕΕ και καλεί τα κράτη μέλη να καθορίσουν εθνικές στρατηγικές κυβερνοασφάλειας και να συνεργαστούν με την ΕΕ για τη διασυνοριακή αντίδραση και επιβολή.

Όπως σημείωσε, κατά την ενσωμάτωση της οδηγίας διευρύνθηκαν οι τομείς αναφοράς με την προσθήκη και των φορέων της τοπικής αυτοδιοίκησης πρώτου βαθμού. Έκανε, επίσης, ειδική αναφορά στον ιδιωτικό τομέα, όπου εντοπίζονται τεράστιες απειλές και κίνδυνοι σε φορείς που θεωρούν μεν ότι είναι ασφαλείς αλλά δεν έχουν κάνει την απαραίτητη χαρτογράφηση του δικτύου τους και δεν έχουν διαγνώσει τους κινδύνους.
Τέλος, τόνισε την κρισιμότητα της συνεργασίας του δημοσίου με ειδικούς και εταιρείες που ειδικεύονται στον τομέα της πρόληψης και αντιμετώπισης των κινδύνων κυβερνοασφάλειας καθώς και με άλλα κράτη κάνοντας ειδική αναφορά στην Κύπρο.

Σε τρία σημεία που αλλάζουν σήμερα δραματικά σήμερα στον τομέα της κυβερνοασφάλειας αναφέρθηκε ο Υφυπουργός Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής της Κυπριακής Δημοκρατίας, Δρ. **Νικόδημος Δαμιανού**. Αρχικά, πρόκειται για τα εργαλεία και τις μεθόδους των κυβερνοεπιθέσεων. Όπως είπε, «τα εργαλεία που μπορεί να χρησιμοποιηθούν γίνονται πιο σύνθετα και εξελίσσονται δραματικά με τη χρήση των δυνατοτήτων της Τεχνητής Νοημοσύνης». Σε αυτό το πλαίσιο, εστίασε στη δυσκολία προστασίας από τα deep fakes, καθώς πλέον οι πόροι και υποδομές που παραδοσιακά είχαν στη διάθεσή τους οι εταιρείες γίνονται πλέον διαθέσιμα και στους κυβερνοεγκληματίες.

Ως δεύτερο επίπεδο, διέκρινε την επιφάνεια και το εύρος των κυβερνοεπιθέσεων, καθώς τα κράτη ψηφιοποιούνται, για παράδειγμα με ηλεκτρονική διακίνηση εγγράφων, ψηφιοποίηση υπηρεσιών, έξυπνες πόλεις, αυτόνομα οχήματα, διευρύνονται και τα πιθανά τρωτά σημεία για επιθέσεις. «Ζούμε σε εποχή που όρια ψηφιακού και πραγματικού κόσμου δεν είναι διακριτά», σημείωσε, τονίζοντας πως πλέον οι κυβερνοεπιθέσεις μπορούν να οδηγήσουν και σε επιπτώσεις στον φυσικό κόσμο όπως για παράδειγμα στον τομέα της ενέργειας. Τρίτον, Ο πιθανός αντίκτυπος που αλλάζει δραματικά: «Φανταστείτε κάποια από τις πλατφόρμες υπολογιστικού νέφους να καταστεί μη διαθέσιμη. Σκεφτείτε τον αντίκτυπο» ανέφερε ενδεικτικά τονίζοντας πως, παράλληλα, ο μακροπρόθεσμος αρνητικός αντίκτυπος για κυβερνήσεις είναι να επηρεάσουν αρνητικά την αξιοπιστία ψηφιακών λύσεων και να απωθήσουν τις επιχειρήσεις από το να τις αξιοποιήσουν για την ανάπτυξη αλλά και την προστασία τους.

«Στην Κύπρο έχουμε θέσει ως ύψιστη προτεραιότητα τα ζητήματα της κυβερνοασφάλειας», σημείωσε ο Υφυπουργός Έρευνας, Καινοτομίας και Ψηφιακής Πολιτικής της Κυπριακής Δημοκρατίας, αναπτύσσοντας ένα οριζόντιο πρόγραμμα αντιμετώπισης αλλά και πρόληψης με τη συνεργασία δημόσιου και ιδιωτικού τομέα. Στο πλαίσιο αυτό, η Κρατική Αρχή Ψηφιακής Ασφάλειας παρέχει λύσεις στήριξης επιχειρήσεων κατά την ψηφιακή τους μετάβαση, ενώ η κυβέρνηση προχωράει σε χρηματοδοτήσεις για ΜμΕ προκειμένου να προστατέψουν υποδομές και δεδομένα. Επιπρόσθετα, έχει υποβληθεί στην Βουλή των Αντιπροσώπων η ευρωπαϊκή οδηγία NIS2, ενώ τον περασμένο Δεκέμβριο εγκαινιάστηκε η ψηφιακή λύση Ψηφιακός Πολίτης, στα πρότυπα του Gov Wallet, επί της οποίας και θα ενισχυθεί η συνεργασία με το Υπουργείο Ψηφιακής Δικυβέρνησης, με πιθανό πρώτο βήμα τη διαλειτουργικότητα των δύο εφαρμογών. Τον περασμένο μήνα ξεκίνησε και η διάθεση της ηλεκτρονικής ταυτότητας.