Προστατεύοντας το Σήμερα, Οργανώνοντας το Αύριο

Τελευταία ενημέρωση 04/02/2025

5ο ΠΑΝΕΛ Συζήτησης : **Επιβεβλημένη η συνεργασία μεταξύ Δημόσιου και Ιδιωτικού τομέα για την καταπολέμηση της κυβερνοαπάτης**

Η ενίσχυση της συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα για την αντιμετώπιση της κυβερνοαπάτης απασχόλησε, μεταξύ άλλων, τις εργασίες του 1ου Cyber Intelligence Summit για την κυβερνοπληροφορία και την κυβερνοασφάλεια, που διοργανώθηκε από τις εταιρείες Viewmax Media και Fnews Media στο Μέγαρο Μουσικής Αθηνών, υπό την αιγίδα του υπουργείου Ψηφιακής Διακυβέρνησης.

Ιωάννης Καλλιάς: *"Αυξάνεται η πολυπλοκότητα και η συχνότητα των περιστατικών κυβερνοαπάτης στην Ελλάδα"*
Δίνοντας τον ορισμό της κυβερνοαπάτης, κατά την τοποθέτησή του, ο κ. Ιωάννης Καλλιάς, country manager της TÜV AUSTRIA στην Ελλάδα και Executive Vice President Service Lines του TÜV AUSTRIA Group, προσδιόρισε πως πρόκειται για «απάτη που διαπράττεται μέσω του Διαδικτύου ή άλλων ψηφιακών μέσων και περιλαμβάνει δραστηριότητες, όπως η κλοπή ταυτότητας, το phishing και άλλες μορφές εξαπάτησης», προσθέτοντας ότι το 2024 η Ελλάδα κατέγραψε σημαντική αύξηση στις επιθέσεις ransomware, με περισσότερες από 700 αναφορές.
Ανέφερε επίσης μια σειρά χαρακτηριστικών παραδειγμάτων, όπως τη σημαντική κυβερνοεπίθεση που δέχθηκε τον Οκτώβριο του 2024 το Ελληνικό Ανοικτό Πανεπιστήμιο (ΕΑΠ), η οποία και επηρέασε τις ηλεκτρονικές του υποδομές. Σύμφωνα, δε, με έκθεση της Kaspersky, οι χρήστες στην Ελλάδα ήταν για το 2024 οι πλέον εκτεθειμένοι σε κυβερνοαπειλές παγκοσμίως.
«Αυτά τα περιστατικά καταδεικνύουν την αυξανόμενη πολυπλοκότητα και συχνότητα των κυβερνοεπιθέσεων και την κυβερνοαπάτης στην Ελλάδα και την Ευρώπη. Η υιοθέτηση προηγμένων λύσεων και πρακτικών ασφαλείας καθίσταται απαραίτητη για την προστασία των κρίσιμων υποδομών και των δεδομένων» σημείωσε.
Εξήγησε γιατί είναι απαραίτητη η συνεργασία δημόσιου και ιδιωτικού τομέα για την αντιμετώπιση της κυβερνοαπάτης, υπογραμμίζοντας πως «τομέα είναι ζωτικής σημασίας για την αντιμετώπιση της κυβερνοαπάτης, καθώς οι κυβερνοεγκληματίες εκμεταλλεύονται τα κενά ασφαλείας τόσο στις κρατικές δομές όσο και στις ιδιωτικές επιχειρήσεις».
Κατά τον ίδιο, οι κυβερνοαπάτες δεν κάνουν διακρίσεις μεταξύ δημόσιων και ιδιωτικών οργανισμών, καθώς πλήττουν κρίσιμες υποδομές τόσο του δημοσίου όσο και του ιδιωτικού τομέα.

Βασίλης Αλεξίου: *"Θωρακίζεται το Κοινοβούλιο έναντι των κυβερνοεπιθέσεων"*

Στο πλαίσιο της συζήτησης, την οποία συντόνισε η δημοσιογράφος Σόνια Χαϊμαντά, ο Chief Information Security Officer της Βουλής των Ελλήνων Βασίλης Αλεξίου, σημείωσε ότι το Κοινοβούλιο,

ως ευαίσθητος οργανισμός, θωρακίζεται έναντι των κυβερνοεπιθέσεων λαμβάνοντας μέτρα όπως οι μεγάλοι φορείς ανά τον κόσμο. «Από τον Μάρτιο του 2024 ξεκινήσαμε επαφές με την Εθνική Αρχή Κυβερνοασφάλειας, το ΓΕΕΘΑ και άλλους φορείς του Δημοσίου, με τους οποίους συνεχίζουμε να συνεργαζόμαστε ενώ ερχόμαστε σε επαφή και με μεγάλες ιδιωτικές εταιρείες, αναφορικά με τα νέα μέτρα που λαμβάνουν και αυτοί ως προς τις κυβερνοεπιθέσεις», σημείωσε.
Ανέφερε επίσης ότι οι υπεύθυνοι ασφαλείας φορέων του Δημοσίου, όπως είναι η Προεδρία της Κυβέρνησης, η Προεδρία της Βουλής, τα Υπουργεία εκπαιδεύονται συνεχώς πλέον ώστε να γνωρίζουν κάθε εξέλιξη στον τομέα της κυβερνοασφάλειας. Δεν παρέλειψε πάντως να αναφέρει ότι υπάρχουν και οργανισμοί «που δεν έχουν πάρει ούτε τα μισά μέτρα από αυτά που επιβάλλονται».

Ιωάννης Παυλόσογλου: *"Νέες τακτικές αποκτούν οι χάκερς μέσω της Τεχνητής Νοημοσύνης"*

Από την πλευρά του, ο επιχειρησιακός Υποδιοικητής της Εθνικής Αρχής Κυβερνοασφάλειας, Ιωάννης Παυλόσογλου, σε διαδικτυακή του παρέμβαση, είπε πως οι ψηφιακές απειλές συνεχώς αλλάζουν. Το θεσμικό πλαίσιο προβλέπει σίγουρα πιο αυξημένα μέτρα, αλλά και οι χάκερς λαμβάνουν τα δικά τους «μέτρα» και επιχειρούν να μπουν «όχι από την κύρια ηλεκτρονική πύλη μιας επιχείρησης, αλλά μέσω ενός τρίτου παρόχου, π.χ. μέσω μιας εταιρείας που κάνει συντήρηση σε ένα κτήριο του οργανισμού που θέλουν να πλήξουν. Πλέον έχουμε και επιθέσεις που αξιοποιούν την τεχνητή νοημοσύνη, αποκτώντας άλλες καίριες τακτικές επιθέσεων».

Αγγελική Δέλγα: *"Μηδενική ανεργία στον τομέα της κυβερνοασφάλειας"*

Η Αγγελική Δέλγα, Director, Cybersecurity, Technology Consulting EY, υπογράμμισε ότι τόσο ο δημόσιος όσο και ο ιδιωτικός τομέας αντιμετωπίζουν τις ίδιες προκλήσεις. «Την ίδια ώρα, η Εθνική Αρχή Κυβερνοασφάλειας έχει διανύσει αρκετό δρόμο ωριμότητας, αν και έχει να εκπληρώσει αρκετό έργο ακόμη. Βλέπω ότι έχει τη διάθεση να το πράξει», σημείωσε. Είπε επίσης ότι καλό θα ήταν όλες οι επιχειρήσεις και οι δημόσιοι οργανισμοί να επενδύσουν στην κυβερνοασφάλεια, καθώς αυτό μελλοντικά θα τους γλιτώσει από μεγάλα κόστη.
«Μια κυβερνοεπίθεση μπορεί να προκαλέσει πολύ σοβαρές ζημιές. Η δε ανεργία στην κυβερνοασφάλεια αυτή τη στιγμή είναι μηδενική. Δεν υπάρχει άνθρωπος που να έχει γνώσεις, εμπειρία ή και τα δύο μαζί στον συγκεκριμένο τομέα και να μην έχει δουλειά», ανέφερε.

Γεώργιος Μπανάβας: *"Να στρέψουμε υπέρ τις κυβερνοασφάλειας την Τεχνητή Νοημοσύνη"*

Τέλος, ο Γεώργιος Μπανάβας, διευθυντής της Επιτροπής Κεφαλαιαγοράς, Γραφείου Θεσσαλονίκης, τόνισε πως ο χρηματοοικονομικός χώρος είναι ένας ιδιαίτερος τομέας, καθώς διακινεί τεράστιες ποσότητες ψηφιακών δεδομένων και μεγάλης αξίας. «Τεχνολογίες όπως η τεχνητή νοημοσύνη θα πρέπει να τις στρέψουμε υπέρ της ασφάλειας από κυβερνοεπιθέσεις. Την ίδια ώρα, θα πρέπει στους επιχειρηματικούς ομίλους να υπάρχει συνέργεια μεταξύ των στελεχών που ασχολούνται με την κυβερνοασφάλεια και των στελεχών που θέτουν τους επιχειρηματικούς στόχους»