Προστατεύοντας το Σήμερα, Οργανώνοντας το Αύριο

*Τελευταία ενημέρωση 04/02/2025*

6ο ΠΑΝΕΛ Συζήτησης : **Ψηφιακός μετασχηματισμός και κυβερνοασφάλεια: Ποια η εικόνα στη χώρα**

Ο καθοριστικός ρόλος του ψηφιακού μετασχηματισμού στην άμυνα κατά των κυβερνοεπιθέσεων αναδείχθηκε στο πλαίσιο του 1ου Cyber Intelligence forum 2025 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.

Τις κρίσιμες παραμέτρους του ζητήματος παρουσίασαν σε πάνελ που συντόνισε η **Όλγα Γιαννιάδη**, ο Διοικητής της Εθνικής Αρχής Κυβερνοασφάλειας **Μιχάλης Μπλέτσας**, ο Managing Director της TÜV AUSTRIA Trust-IT **Τρύφων Άμερ**, ο Security Lead της ACCENTURE **Κωνσταντίνος Βουζόπλης**, ο Chief Information Security Officer της ALPHA BANK **Δημήτρης Σταυρόπουλος** και ο Senior Specialist, security της MICROSOFT HELLAS **Δημήτρης Πατσός**.

Σε παρέμβασή της, η Group Director της SPACE HELLAS, **Νάντια Λιάπη** εστίασε στην ανάγκη συνεργασίας δημόσιου και ιδιωτικού τομέα στον χώρο αντιμετώπισης, απόκρουσης και διαχείρισης κυβερνοεπιθέσεων. Εστίασε στην ανάγκη των οργανισμών για υψηλού επιπέδου υπηρεσίες «ασπίδα», που ειδοποιούν εγκαίρως για το τι συμβαίνει και πώς πρέπει να αντιμετωπιστεί, όπως αυτές που προσφέρει η SPACE HELLAS με 40 χρόνια παρουσίας στην ελληνική αγορά και 1.000 εργαζόμενους. Υπογράμμισε την αναγκαιότητα για ένα εθνικό Κέντρο Αναφοράς Κυβερνοασφάλειας (SOC), που θα προστατεύει τις εθνικές σημαντικές και ουσιαστικές υποδομές. Σημείωσε πως όταν δημιουργηθεί θα είναι το πιο σημαντικό σημείο συντονισμού σε εθνικό επίπεδο και συνεργασίας με την ΕΕ.
«Ο καθένας από εμάς είναι τόσο δυνατός όσο πιο δυνατός είναι ο πιο αδύναμος κρίκος του», είπε χαρακτηριστικά η κυρία Λιάπη, επισημαίνοντας ότι η Ελλάδα, ειδικά από τον Αύγουστο και μετά, έχει πληγεί ανεπανόρθωτα από κυβερνοεπιθέσεις σε μικρότερους και μεγάλους οργανισμούς, που βρέθηκαν εκτός λειτουργίας, έχασαν δεδομένα και πόρους.
«Βελτιστοποιούμε πόρους, μειώνουμε τον χρόνο απόκρισης, ενώνουμε δυνάμεις. Είναι πολύ σημαντικό όλοι εμείς από την αγορά που γνωρίζουμε πώς το διαχειριζόμαστε αυτό, έχουμε ανθρώπους και ισχυρά εργαλεία, να ενισχύσουμε την προσπάθεια του εθνικού SOC», είπε, κάνοντας λόγο για μια επωφελή συνεργασία για όλα τα μέρη.
Ως σοβαρό κίνητρο για τη συνεργασία των επιχειρήσεων με το δημόσιο σε ένα τέτοιο εγχείρημα, έθεσε την οικονομική ενίσχυση του R&D, ώστε να δημιουργηθούν πλατφόρμες και εργαλεία ελληνικής κατασκευής, ενώ υπογράμμισε την κρισιμότητα της πιστοποίησης για όσους οργανισμούς συμβάλλουν σε αυτό.

**Μ. Μπλέτσας:** "*Θα είχαν αποφευχθεί επιθέσεις αν είχαμε ήδη σε εφαρμογή τα μέτρα της NIS2*"

Σύμφωνα με τον Μιχάλη Μπλέτσα, Διοικητή της Εθνικής Αρχής Κυβερνοασφάλειας, ο οποίος συμμετείχε διαδικτυακά στη συζήτηση που ακολούθησε, οι επιθέσεις που ο ίδιος έχει δει από την ανάληψη των καθηκόντων του τον περασμένο Μάιο θα είχαν αποφευχθεί αν είχαν τεθεί ήδη σε εφαρμογή τα μέτρα που προβλέπει η κοινοτική οδηγία NIS2. Όπως εξήγησε, η οδηγία κάνει υποχρεωτική την αναφορά πραγματικών περιστατικών, αυξάνει τον αριθμό και το πεδίο της εποπτείας για την κυβερνοασφάλεια, τους φορείς που πρέπει να συμμορφώνονται κανονιστικά και το επίπεδο ευθύνης στους οργανισμούς ενώ θέτει οριζόντια μέτρα στα κράτη – μέλη της ΕΕ.
«Στην ουσία τους αναγκάζει να λάβουν πιο αυστηρά υπόψιν τους την κυεβρνοασφάλεια», σημείωσε. Τόνισε, δε, πως από τα βασικότερα προβλήματα στον τομέα της κυβερνοασφάλειας είναι η έλλειψη μίας πλήρους εικόνας της πραγματικής κατάστασης στη χώρα προκειμένου να υπάρξουν ρυθμιστικές και εποπτικές βελτιώσεις. Εντούτοις, υπογράμμισε τη σημασία της οδηγίας NIS2 προκειμένου να ξεπεραστούν προσκόμματα στο εθνικό δίκαιο για την ανάγκη πολλαπλής ταυτοποίησης χρηστών ειδικά σε φορείς του δημοσίου.

**Τ. Άμερ:** *"Ευκαιρία ο ψηφιακός μετασχηματισμός για την προώθηση της κυβερνοασφάλειας"*

Δίνοντας μία εικόνα της αγοράς, ο Τρύφων Άμερ, Managing Director της TÜV AUSTRIA Trust-IT σημείωσε πως πάνω από το 80% της ελληνικής αγοράς μικρομεσαίων επιχειρήσεων (ΜμΕ) δεν θέτουν από την αρχή στην ατζέντα του ψηφιακού τους μετασχηματισμού την επένδυση στην κυβερνοασφάλεια που καταλήγει να τους απασχολεί μόνο μετά από κάποια επίθεση.
Στο πλαίσιο αυτό υπογράμμισε την ανάγκη ενημέρωσης, υιοθέτησης προτύπων ISO και εναρμόνισης με την οδηγία NIS2 και της ανάπτυξης προληπτικών λειτουργιών και παρακολούθησης των συστημάτων τους σε πραγματικό χρόνο. Επιπλέον, τόνισε πως οι περισσότερες εταιρείες εστιάζουν στον τομέα του IT, ενώ ο ψηφιακός μετασχηματισμός αποτελεί μία ευκαιρία προκειμένου να ασφαλιστεί και η OT υποδομή με μία ενιαία στρατηγική μαζί με τις IT υποδομές.

**Κ. Βουζόπλης**: *"Κρίσιμος παράγοντας η εκπαίδευση του προσωπικού"*
Από την πλευρά του, ο Security Lead της ACCENTURE Κωνσταντίνος Βουζόπλης τόνισε πως η ενσωμάτωση προβλέψεων κυβερνοασφάλειας από την αρχή κάθε νέας δραστηριότητας των εταιρειών αποτελεί κομβικό σημείο για την προώθηση της ανθεκτικότητας των οργανισμών. Στο πλαίσιο αυτό ανέφερε πως η ACCENTURE προτείνει το μοντέλο security by design θέτοντας τον παράγοντα ασφάλειας από το πρώτο βήμα κάθε νέας λειτουργίας.
Τέλος, υπογράμμισε τον κρίσιμο ρόλο της εκπαίδευσης του προσωπικού των εταιρειών σε θέματα κυβερνοασφάλειας, σημειώνοντας πως οι περισσότερες επιθέσεις ransomware βασίζονται στον ανθρώπινο παράγοντα. Όπως είπε, «το να εκπαιδεύσουμε το προσωπικό αποτελεί τον πιο δυνατό μηχανισμό για την δημιουργία ενός ισχυρού τείχους προστασίας».

**Δ. Σταυρόπουλος:** *"Ανάγκη συνεργασίας όλων των τμημάτων του κάθε οργανισμού"*

Σύμφωνα με τον Δημήτρη Σταυρόπουλος, Chief Information Security Officer της ALPHA BANK τον τελευταίο χρόνο καταγράφεται αύξηση στην κακόβουλη λειτουργία. Όπως είπε, το κρίσιμο σε τέτοιες συνθήκες είναι να καταγράφεται όχι απλώς από την αρχή της δυσλειτουργίας, αλλά να μπορούν και όλοι οι εμπλεκόμενοι να αντιλαμβάνονται τις συμβαίνει και να μπορούν να ενημερώσουν τον οργανισμό άμεσα και αποτελεσματικά. Όπως είπε, ένα τέτοιο επίπεδο συνεργασίας με το business και 3rd parties αποτελεί κομβικό παράγοντα για την διασφάλιση της ανθεκτικότητας του οργανισμού.

**Δ. Πατσός**: *"Μείωση 20% του χρόνου αντιμετώπισης περιστατικών κυβερνοεπιθέσεων με εργαλεία Τεχνητής Νοημοσυνης"*

Ο Senior Specialist, security της MICROSOFT HELLAS Δημήτρης Πατσός εστίασε στον τομέα της αξιοποίησης των εργαλείων της Τεχνητής Νοημοσύνης στην κυβερνοασφάλεια, σημειώνοντας πως οδήγησε στην αύξηση κατά 50% της ποιότητας των υπηρεσιών τους. Ο κ. Πατσός τόνισε ότι αρκετοί ελληνικοί οργανισμοί μπήκαν νωρίς στο τρένο της Τεχνητής Νοημοσύνης. Όπως είπε, η αξιοποίηση των εργαλείων αυτών οδηγούν σε μείωση κατά 20% του χρόνου της αντιμετώπισης περιστατικών κυβερνοεπιθέσεων ενώ αυξάνει και την αυτοματοποίηση.