Προστατεύοντας το Σήμερα, Οργανώνοντας το Αύριο

Τελευταία ενημέρωση 04/02/2025

2ο ΠΑΝΕΛ Συζήτησης : **Εθνική Άμυνα και διεθνείς συνεργασίες στην Κυβερνοασφάλεια**

Νικόλαος Kikis: Για το ΝΑΤΟ, η κυβερνοεπιθεση σε έναν ισούται με κυβερνοεπίθεση σε όλους
Στην Εθνική Άμυνα και τις διεθνείς συνεργασίες στην Κυβερνοασφάλεια αφιερώθηκε πάνελ στο 1ο Cyber Intelligence forum 2025 με τη συμμετοχή του Προϊστάμενου Τμήματος Κυβερνοάμυνας του Υπουργείου Άμυνας της Κυπριακής Δημοκρατίας, **Χρίστου Καλλονά**, του πρώην διευθυντή της Διεύθυνσης Κυβερνοάμυνας ΓΕΕΘΑ, ειδικού στα αντικείμενα κυβερνοασφάλειας και επιχειρήσεων κυβερνοχώρου, Πλοιάρχου (Μ) ε.α. **Σπύρου Παπαγεωργίου** ΠΝ και ο Strategic Leader in Technology **Christopher Woods**.

Στο πλαίσιο του συνεδρίου 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, παρεμβάσεις έκαναν ακόμη η Πρόεδρος της Επιτροπής Κεφαλαιαγοράς **Βασιλική Λαζαράκου**, ο πρώην DoD/Intelligence Community Senior Executive and ιδρυτής του Kryptos Consulting Group, **Νικόλαος Kikis** και ο Διευθύνων Σύμβουλος της MITACS **Kelvin Moore** μέσω διαδικτυακής παρουσίας.

Β. Λαζαράκου: Ο χρηματοπιστωτικός τομέας μπορεί να βρεθεί μπροστά στις εξελίξεις
Στην παρέμβασή της, η Πρόεδρος της Επιτροπής Κεφαλαιαγοράς Βασιλική Λαζαράκου απαρίθμησε μία σειρά κινήσεων της Επιτροπής για την προώθηση της ατζέντας της κυβερνοασφάλειας. Ειδική αναφορά έκανε στο νέο Κανονισμό DORA που καθορίζει ενιαίες απαιτήσεις σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών που υποστηρίζουν τις επιχειρηματικές διαδικασίες στον χρηματοπιστωτικό τομέα.
«Πρόκειται για την κύρια νομοθεσία του χρηματοοικονομικού τομέα που εναρμονίζει τους κανόνες ψηφιακής επιχειρησιακής ανθεκτικότητας», εξήγησε. Όπως επισήμανε, αυτός τέθηκε σε εφαρμογή στην χώρα μας στις 17 Ιανουαρίου 2025 και επί του παρόντος τρέχουν οι διαδικασίες από το Υπουργείο Εθνικής Οικονομίας και Οικονομικών, προκειμένου να ξεκαθαριστούν οι αρμοδιότητες και οι διαδικασίες, ούτως ώστε να προχωρήσουν οι προσαρμογές στην εθνική νομοθεσία μέσα στο προσεχές διάστημα.
Υπογράμμισε, εντούτοις, πως ήδη η Επιτροπή Κεφαλαιαγοράς ενημερώνει στις οντότητες που εποπτεύει προκειμένου να γνωρίζουν τις διαδικασίες και τις υποχρεώσεις τους, εφόσον προκύψει κάποιο περιστατικό κυβερνοασφάλειας.
Όσον αφορά στο κόστος που θα έχει για τις εταιρείες η προσαρμογή στον νέο Κανονισμό, τόνισε πως είναι κρίσιμο να υπάρχουν συστήματα πρόβλεψης κινδύνων και ενίσχυσης της κυβερνοασφάλειας, καθώς αποτελεί «ένα αναπτυξιακό εργαλείο που στηρίζει την αξιοπιστία των παρεχόμενων

υπηρεσιών, δημιουργώντας προστιθέμενη αξία στις επιχειρήσεις», τόνισε, υπογραμμίζοντας τη σημασία της ταχύτητας κανονιστικής συμμόρφωσης.
«Είναι σημαντικό όλοι να τρέξουμε με γρήγορους ρυθμούς, όπως γίνεται σε όλη την Ευρώπη», είπε η κ. Λαζαράκου, εκφράζοντας την πεποίθηση ότι ο χρηματοπιστωτικός τομέας μπορεί να βρεθεί μπροστά στις εξελίξεις.

Νικόλαος Kikis: Για το NATO, η κυβερνοεπίθεση σε έναν ισούται με κυβερνοεπίθεση σε όλους
«Η κυβερνοεπίθεση σε έναν ισούται με κυβερνοεπίθεση σε όλους», υπογράμμισε ο πρώην DoD/Intelligence Community Senior Executive and ιδρυτής του Kryptos Consulting Group, Νικόλαος Kikis, παρουσιάζοντας αναλυτικά τις δράσεις και τα προγράμματα που υλοποιεί το NATO για την προώθηση της κυβερνοασφάλειας στα κράτη-μέλη του, κάνοντας λόγο για μία «συλλογική κυβερνοάμυνα».

Ο κ. Kikis τόνισε πως «χωρίς εκπαίδευση και εμπιστοσύνη μπορούν να γίνουν πολύ άσχημα πράγματα στον κυβερνοχώρο», εξαίροντας τον κρίσιμο ρόλο του Κέντρου Αριστείας Συνεργατικής Κυβερνοάμυνας (CCDCoE) του NATO, που συνέβαλε στην αντιμετώπιση κυβερνοεπιθέσεων από τη Ρωσία κατά της Ουκρανίας. Υπογράμμισε την κρισιμότητα της συνεργασίας και του διαμερισμού πληροφοριών, με δημόσιους φορείς αλλά και με τον ιδιωτικό τομέα, καθώς οι κυβερνοεπιθέσεις γίνονται όλο και πιο σύνθετες και περίπλοκες κάνοντας πιο περίπλοκη τη διαχείρισή τους.
Καταλήγοντας, ο κ. Kikis σημείωσε πως η Ελλάδα και η Κύπρος βρίσκονται σε ένα κρίσιμο σταυροδρόμι, καλώντας τις δύο χώρες να συνεργαστούν περαιτέρω και παράλληλα να εντείνουν την συνεργασία τους με το NATO, προκειμένου να αυξήσουν την ανθεκτικότητά τους έναντι πιθανών κυβερνοεπιθέσεων.

Christopher Woods: Η εθνική άμυνα δεν αφορά πλέον μόνο τα φυσικά αλλά και τα ψηφιακά όρια των κρατών. Περισσότερες από 1,5 εκατ. ήταν οι παραβιάσεις από κακόβουλες επιθέσεις το 2024 που οδήγησαν σε παραβιάσεις σε εκατοντάδες χιλιάδες αρχείων ανέφερε ο Christopher Woods, Strategic Leader in Technology με μεγάλη εμπειρία στις ΗΠΑ στον τομέα της εθνικής ασφάλειας. «Είμαστε όλοι τόσο συνδεδεμένοι, που η κυβερνοασφάλεια αποτελεί κίνδυνο για όλους μας. Είναι σημαντικό να συνεχίσουμε να προσαρμοζόμαστε και να καινοτομούμε για να διασφαλίσουμε το ψηφιακό μας μέλλον», είπε χαρακτηριστικά.
Όπως τόνισε, καθώς αυξάνεται η παγκόσμια διασύνδεση αποτελεί κοινή αποστολή η ενδυνάμωση των αμυνών για την αντιμετώπιση ψηφιακών απειλών, υπογραμμίζοντας πως η εθνική άμυνα δεν αφορά πλέον μόνο τα φυσικά αλλά και τα ψηφιακά όρια των κρατών. Εστίασε, δε, στην ανάγκη προστασίας των κρίσιμων υποδομών για κάθε χώρα, με τη διεθνή συνεργασία να είναι ζωτικής σημασίας.
Παρουσιάζοντας τις βασικότερες κυβερνοαπειλές αναφέρθηκε στην άνοδο της χρήσης εργαλείων Τεχνητής Νοημοσύνης, στα τρωτά σημεία κρίσιμων υποδομών, όπως της ενέργειας ή υγείας, της εφοδιαστικής αλυσίδας που είναι όλο και πιο συνδεδεμένες, η Κβαντική υπολογιστική και η

διευρυμένη χρήση του Internet of Things. Ειδική αναφορά έκανε στις επιθέσεις Ransomware τονίζοντας ότι το 2024 καταγράφηκε άνοδος 20% στις σχετικές επιθέσεις κυρίως σε απλούς πολίτες.
Kelvin Moore: Στα 265 δισ. δολάρια εκτιμάται το κόστος από επιθέσεις Ransomware το 2031
Στα 265 δισ. δολάρια εκτιμάται το κόστος από επιθέσεις Ransomware ως το 2031, με μία νέα επίθεση να συμβαίνει κάθε δύο δευτερόλεπτα σημείωσε από την πλευρά του ο Διευθύνων Σύμβουλος της MITACS Kelvin Moore μέσω διαδικτυακής παρουσίας. «Χρειαζόμαστε κάτι παραπάνω από antivirus και firewalls. Αυτό είναι δυναμικά και έξυπνα συστήματα που μπορούν να ανιχνεύσουν, να ανταποκριθούν και να αναλύσουν τις επιθέσεις σχεδόν σε πραγματικό χρόνο», τόνισε.
Ο κ. **Kelvin Moore** εστίασε στην ανάγκη αυτοματοποίησης της αντιμετώπισης των επιθέσεων με τη χρήση εργαλείων Τεχνητής Νοημοσύνης (AI), καθώς και διαρκούς εκπαίδευσης και παροχής πιστοποιήσεων στους επαγγελματίες κυβερνοασφάλειας. Ακόμη, έθεσε ως προϋπόθεση τις ελκυστικές αμοιβές και τις ευκαιρίες ανέλιξης για τα στελέχη στον τομέα της κυβερνοασφάλειας, προκειμένου επιχειρήσεις και οργανισμοί να διατηρήσουν τα κορυφαία ταλέντα.
«Πρέπει να ενισχυθεί η κουλτούρα της γνώσης και διαμοιρασμού πληροφορίας», είπε ο CEO της MITACS, υπογραμμίζοντας την ανάγκη εκπαίδευσης του συνόλου των στελεχών κάθε εταιρείας.
Χρίστος Καλλονάς: Η ύπαρξη εθνικής στρατηγικής αποτελεί τον βασικότερο πυλώνα για την κυβερνοασφάλεια ενός κράτους

Στη συζήτηση που ακολούθησε με συντονιστή τον δημοσιογράφο Κώστα Παπαχλιμίντζο, ο Χρίστος Καλλονάς, Προϊστάμενος Τμήματος Κυβερνοάμυνας του Υπουργείου Άμυνας της Κυπριακής Δημοκρατίας, αναφέρθηκε αναλυτικά στο πλαίσιο διασυνοριακής προστασίας και στρατηγικής αντιμετώπισης της κυβερνοασφάλειας που προωθεί η Ε.Ε., ενώ παρουσίασε και τις σχετικές πρωτοβουλίες που έχει αναλάβει η Κυπριακή Δημοκρατία.
«Η ύπαρξη εθνικής στρατηγικής αποτελεί τον βασικότερο πυλώνα για την κυβερνοασφάλεια ενός κράτους», τόνισε υπογραμμίζοντας, εντούτοις, την ανάγκη οι στρατηγικές αυτές να εναρμονίζονται με τα αντίστοιχα ευρωπαϊκά πρότυπα. Ειδική αναφορά έκανε στην πρώτη εθνική άσκηση κυβερνοασφάλειας που υλοποίησε η Κύπρος τον περασμένο Σεπτέμβριο στον τομέα των μεταφορών που συνέβαλε ουσιαστικά στον εντοπισμό και στη διόρθωση προβλημάτων ενισχύοντας την συνεργασία διάφορων τομέων.

Σπύρος Παπαγεωργίου: Κρίσιμη η ανάπτυξη μοντέλων και στρατηγικών προληπτικής κυβερνοάμυνας
Σύμφωνα με τον Πλοίαρχο (Μ) ε.α. Σπύρο Παπαγεωργίου ΠΝ – πρώην διευθυντή της Διεύθυνσης Κυβερνοάμυνας ΓΕΕΘΑ, ειδικό στα αντικείμενα κυβερνοασφάλειας και επιχειρήσεων κυβερνοχώρου οι απειλές, γίνονται όλο και πιο σύνθετες απαιτώντας την ανάπτυξη μοντέλων και στρατηγικών προληπτικής κυβερνοάμυνας που εδράζεται στον έλεγχο των δικτύων και τον διαμοιρασμό των συλλεγόμενων πληροφοριών, προκειμένου να μπορούν και άλλοι οργανισμοί να προετοιμαστούν για σχετικές γνωστές και άγνωστες απειλές.
Μιλώντας για τις αλλαγές που φέρνουν τα μοντέλα Τεχνητής Νοημοσύνης, ο κ. Παπαγεωργίου ανέφερε πως μπορούν να συμβάλλουν ουσιαστικά στην ταχύτατη ανάλυση συμπεριφορών

εντοπίζοντας επιθέσεις, ωστόσο αξιοποιούνται, με την ίδια ταχύτητα και από επιτεθέμενους που εντοπίζουν τρωτά σημεία και τρόπους να ξεπερνούν τα εμπόδια που θέτουν τα συστήματα ασφαλείας.
Κλείνοντας αναφέρθηκε στην αξία που θα είχε η δημιουργία μίας Ακαδημίας Κυβερνοχώρου για την εκπαίδευση εξειδικευμένων στελεχών στα πρότυπα αντίστοιχων οργανισμών στις ΗΠΑ.