Προστατεύοντας το Σήμερα, Οργανώνοντας το Αύριο

Τελευταία ενημέρωση 04/02/2025

3ο ΠΑΝΕΛ Συζήτησης : **Περισσότερες συνέργειες και βελτιστοποίηση διαδικασιών για τη θωράκιση των οργανισμών του μέλλοντος απέναντι στις κυβερνοαπειλές**

Η αντιμετώπιση των κυβερνοεπιθέσεων στον ιδιωτικό τομέα και η διαδικασία ανάκαμψης τέθηκαν στο επίκεντρο της τέταρτης θεματικής του 1ου Cyber Intelligence Summit, που πραγματοποιήθηκε στο Μέγαρο Μουσικής Αθηνών από τις εταιρείες Viewmax Media και Fnews Media υπό την αιγίδα του υπουργείου Ψηφιακής Διακυβέρνησης.

Στην έναρξη του πάνελ, έγιναν παρεμβάσεις από τον **Γιώργο Μπαλαφούτη**, Director, Security CSU Technical Strategy Excellence της MICROSOFT GLOBAL και τον **Δημήτρη Πατσό**, Senior Specialist, security της MICROSOFT HELLAS. Στη συζήτηση, υπό τον συντονισμό του επικεφαλής Υπηρεσιών Κυβερνοασφάλειας της EY (CESA), **Παναγιώτη Παπαγιαννακόπουλου**, συμμετείχαν ο **Bill Karnazes**, Chief Operations Officer της VIOHALCO, ο **Νικόλαος Πέππας,** Group Chief Information Security Officer της HELLENiQ ENERGY και ο **Δημήτρης Σταυρόπουλος**, Chief Information Security Officer της ALPHA BANK

Από τα κίνητρα των κυβερνοεπιθέσεων ξεκίνησε την παρουσίασή του ο **Γιώργος Μπαλαφούτης**, director, security CSU Technical Strategy Excellence της MICROSOFT GLOBAL, βάζοντας στη συζήτηση το ακρωνύμιο «CHEW». Όπως εξήγησε, αυτό αποτυπώνει σκοπούς εγκληματικούς και οικονομικού οφέλους, κοινωνικοπολιτικό ακτιβισμό, κατασκοπεία και κυβερνοπόλεμο.
Απαρίθμησε ποικίλους τρόπους «ψαρέματος» των χρηστών, βάσει του Microsoft Digital Defense Report, προκειμένου να υποκλαπούν ακολούθως προσωπικά τους στοιχεία και κωδικοί και συνέστησε σε όλους να χρησιμοποιούν ισχυρά και περίπλοκα passwords. «Αν αποκτήσεις πρόσβαση στο e-mail κάποιου, είναι σαν να έχεις αποκτήσει πρόσβαση στη ζωή του», είπε χαρακτηριστικά.

Όπως αποκάλυψε, μέσα σε ένα έτος χάθηκαν παγκοσμίως 8 τρισεκατομμύρια ευρώ από το κυβερνοέγκλημα, σε όρους οικονομικούς και παραγωγικότητας, ενώ συνέστησε να έχουμε ιδιαίτερη προσοχή κάθε φορά που σερφάρουμε στο Διαδίκτυο. «Ακόμη κι όταν πηγαίνετε στο εστιατόριο και σκανάρετε μέσω QR Code το μενού, θα πρέπει να είστε προσεκτικοί, γιατί κάποιοι μπορεί να έχουν κολλήσει πάνω στον κωδικό ένα δικό τους ανάλογο αυτοκόλλητο, το οποίο θα οδηγήσει μεν πραγματικά στο μενού, αλλά ουσιαστικά κατευθύνει σε ιστοσελίδα κακόβουλου χειριστή», σημείωσε.
Επέστησε την προσοχή στον κίνδυνο των deep fakes, αλλά και της δυνατότητας επιρροής ακόμα και σε εκλογικά αποτελέσματα, φέρνοντας ως παράδειγμα τις πρόσφατες αμερικανικές εκλογές. «Καλό είναι να σκεφτόμαστε πιο κανάλι επιβεβαίωσης μπορώ να αξιοποιήσω, για να αποφύγω το λάθος», υπογράμμισε.

Από την πλευρά του, ο Senior Specialist, Security της MICROSOFT HELLAS, **Δημήτρης Πατσός** σημείωσε πως «είμαστε ένας φορέας που βασίζονται πάνω μας εκατομμύρια οργανισμοί, δημόσιοι και ιδιωτικοί. Εντοπίσαμε 750.000 υπηρεσίες που δεν πληρούσαν τα κριτήρια ασφάλειας», κάνοντας λόγο για μια άσκηση που αξίζει να τρέξουν όλοι οι οργανισμοί. «Ενημερώνουμε τους οργανισμούς με τους οποίους συνεργαζόμαστε. Τα συμπεράσματα στα οποία καταλήγουμε, είναι διαθέσιμα προς αυτούς. Μοιραζόμαστε συνέργειες απλόχερα. Η

Ελλάδα έχει καινοτομήσει στην υιοθέτηση τεχνολογιών τεχνητής νοημοσύνης στην κυβερνοασφάλεια, είμαστε από τους πρωτοπόρους παγκοσμίως».
Σημείωσε, δε, ότι με τη χρήση της Τεχνητής Νοημοσύνης (AI) μπορούμε να αντεπεξέλθουμε αποτελεσματικότερα στις κυβερνοεπιθέσεις, κάτι που έχει φανεί ξεκάθαρα τους τελευταίους περίπου 18 μήνες. «Μέσα σε λιγότερο από 15 λεπτά μπορούμε να εντοπίζουμε ένα περιστατικό και να βγάζουμε ενέργειες», σημείωσε, ενώ εστίασε και στη βελτίωση της αποδοτικότητας των ομάδων εργασίας, ειδικά από τη στιγμή που υπάρχει μεγάλο κενό εργαζομένων στον κλάδο.
Αναφέρθηκε στις τεράστιες προκλήσεις στο γεωστρατηγικό περιβάλλον, με τις κυβερνοαπειλές και τους υβριδικούς πολέμους, αλλά και στην ανάπτυξη της τεχνολογίας με την κβαντομηχανική, το cloud κλπ. για την άμυνα των οργανισμών μας. «Απαιτείται βαθύτερη συνεργασία και περισσότερες συνέργειες. Εμείς συνεργαζόμαστε με μεγάλες ομάδες/οργανισμούς που εμπιστεύονται την πλατφόρμα της Microstoft, οπότε καταλαβαίνετε την ευθύνη που έχουμε», υπογράμμισε.

«Η κυβερνοασφάλεια αποτελεί μια πρόκληση λόγω μεγέθους και ποικιλομορφίας», είπε ο κ. **Bill Karnazes**, Chief Operations Officer της Viohalco, διευκρινίζοντας ότι «τα legacy συστήματα είναι μια πρόκληση αλλά έχουμε τα κατάλληλα εργαλεία διαχείρισης και αντιμετώπισης».
Αναφερόμενος στη NIS2 επισήμανε ότι: «μας επηρεάζει και προσαρμοζόμαστε σε αυτή», ενώ τόνισε «την ανάγκη επιχειρηματικής ανθεκτικότητας ως μέρος μιας προσέγγισης στη σύγκλιση IT και OT, αξιοποιώντας μια κοινή στρατηγική στις εταιρείες της Viohalco, ενισχύοντας την κουλτούρα κυβερνοασφάλειας».
«Πρέπει να υπάρχει σχέδιο δράσης, για την περίπτωση κυβερνοεπίθεσης, ώστε να "γλιτώνεις" χρόνο από περιττές επικοινωνίες», είπε. «Τα σενάρια απειλών και τα σχέδια λειτουργούν όσο παραμένουν ενημερωμένα, ενώ επιπλέον απαιτείται σημαντική επένδυση στο προσωπικό», καταλήγει ο κ. Karnazes

Από την πλευρά του, ο **Νικόλαος Πέππας**, Group Chief Information Security Officer της HELLENiQ ENERGY υπογράμμισε ότι η Κοινοτική Οδηγία NIS2 ήρθε για να υποχρεώσει τους οργανισμούς να προβούν σε κινήσεις που θα έπρεπε εδώ και καιρό να είναι υποχρεωτικές, ως προς την προστασία έναντι των κυβερνοεπιθέσεων. «Έχουμε ένα πρόγραμμα ψηφιακού μετασχηματισμού στον όμιλο, δίνοντας μεγάλη έμφαση στην ασφάλεια», τόνισε, δίνοντας τη διάσταση και της κοινωνικής ευθύνης για οργανισμούς που διαχειρίζονται κρίσιμες υποδομές.

Ο **Δημήτρης Σταυρόπουλος**, Chief Information Security Officer της ALPHA BANK, σημείωσε πως «έχουμε πλέον μεγαλύτερη ευχέρεια να καταλάβουμε ποιοι είναι οι κίνδυνοι που καλούνται να αντιμετωπίσουν οι πάροχοι και να τεστάρουμε την ανθεκτικότητά μας, χρησιμοποιώντας τις νέες μορφές παρείσφρησης. Επιχειρούμε να φέρουμε στο επίκεντρο της ενημέρωσης, που δίνουμε προς τη διοίκηση του ομίλου, τα πραγματικά προβλήματα που υπάρχουν και τους τρόπους αντιμετώπισης».