ODYSSEY™ cybersecurity

Το Παγκόσμιο Φαινόμενο των Κυβερνοεπιθέσεων και η Ελληνική Πραγματικότητα

Η αύξηση των κυβερνοεπιθέσεων αποτελεί ένα παγκόσμιο φαινόμενο με σοβαρές επιπτώσεις σε διάφορους τομείς της οικονομίας αλλά και της κοινωνίας, με την Ελλάδα να μην αποτελεί εξαίρεση, καθώς ο αριθμός των κυβερνοεπιθέσεων στη χώρα αυξάνεται με ανησυχητικούς ρυθμούς.

Η αύξηση σε αριθμούς

Το SOC της Odyssey εδώ και 21 χρόνια παρέχει υπηρεσίες Managed Detection and Response και εξυπηρετεί πελάτες 24/7 και 365 ημέρες το χρόνο σε όλες τις γεωγραφικές περιοχές του κόσμου. Σύμφωνα με τις στατιστικές αναφορές του και βάσει δεδομένων που προέρχονται αποκλειστικά από επιβεβαιωμένα περιστατικά και όχι από αποτυχημένες προσπάθειες κυβερνοεπιθέσεων, παρατηρεί ανοδική τάση σε συγκεκριμένους τύπους κυβερνοεπιθέσεων η οποία προβλέπεται να επιδεινωθεί. Επισημαίνει δε, την επείγουσα ανάγκη για ισχυρά μέτρα κυβερνοασφάλειας προκειμένου να προστατευθούν οι οργανισμοί από επερχόμενες απειλές. Ειδικότερα, παρατηρείται αύξηση 55% στις επιθέσεις που σχετίζονται με το Process Monitoring, 51% σε επιθέσεις τύπου Communication with C2C και 46% σε επιθέσεις Ransomware καθιστώντας την ανάγκη για προστασία, ύψιστης σημασίας.

Πίσω από την ραγδαία αύξηση

Οι λόγοι που οδηγούν σε αυτή την ταχεία αύξηση οφείλονται στην νέα εποχή με τον ψηφιακό μετασχηματισμό, τη μετάβαση στο cloud καθώς και το υβριδικό μοντέλο εργασίας, να έχουν αλλάξει το ψηφιακό μας οικοσύστημα, διευρύνοντας την ψηφιακή περίμετρο και δημιουργώντας νέα σημεία ευπάθειας. Αυτό καθιστά όλους τους οργανισμούς πιθανούς στόχους, ανεξαρτήτου μεγέθους και τομέα δραστηριότητας.

Πως μπορούν να προστατευτούν οι οργανισμοί

Η μεγαλύτερη πρόκληση που αντιμετωπίζει η χώρα μας, είναι η άγνοια στην ανώτερη διοίκηση πολλών οργανισμών, τόσο της σημαντικότητας ύπαρξης στρατηγικής για την κυβερνοασφάλεια όσο και του αποτελεσματικού τρόπου προσέγγισης της.

Είναι σημαντικό να κατανοήσουμε ότι η κυβερνοασφάλεια δεν αφορά μόνο την εφαρμογή μιας ενιαίας τεχνολογίας ή τη διεξαγωγή εκπαιδευτικών σεμιναρίων. Χωρίς 24ωρη παρακολούθηση, οι οργανισμοί δεν μπορούν να γνωρίζουν εάν δέχονται επίθεση ή εάν η ασφάλεια των δεδομένων τους διακυβεύεται.

Συνεπώς, για να μπορέσει μια στρατηγική να είναι αποτελεσματική και εφαρμόσιμη θα πρέπει να βασίζεται σε όλες τις λειτουργικές πτυχές του οργανισμού: Ανθρώπους, Διαδικασίες και Τεχνολογία.

Odyssey, ο στρατηγικός σας συνεργάτης στην κυβερνοάσφαλεια

Με πάνω από 150 άτομα εξειδικευμένο προσωπικό στην κυβερνοασφάλεια, εκ των οποίων μεγάλο ποσοστό να εδρεύει στον Ελλαδικό χώρο, η Odyssey αποτελεί έναν από τους μεγαλύτερους και πιθανώς παλαιότερους οργανισμούς στην ευρύτερη περιοχή. Με επιπλέον φυσική παρουσία σε Κύπρο, Σαουδική Αραβία, Αίγυπτο και Αγγλία εξυπηρετεί πελάτες ανεξαρτήτου τομέα και μεγέθους ανά το παγκόσμιο.

Η ολιστική προσέγγιση της Odyssey περιλαμβάνει πέντε πυλώνες λύσεων, υπηρεσιών και προϊόντων, όπως: Advisory Services (GRC), Integrated Solutions, Cloud Security, ClearSkies™ Threat & Vulnerability Management Platform και Managed Security/ Detection & Response Services (MSDR).

www.odysseycs.com