Cisco Cybersecurity Solutions
Ολιστική προσέγγιση στην κυβερνοασφάλεια

Η επιτάχυνση του ψηφιακού μετασχηματισμού που έχει επέλθει λόγω πανδημίας έχει αυξήσει σημαντικά την παραγωγικότητα των οργανισμών ενώ παράλληλα προσθέτει νέες προκλήσεις για την ασφάλεια στον κυβερνοχώρο. Το AI και το cloud computing αποτελεί ασπίδα προστασία των επιχειρήσεων αλλά και όπλο στα χέρια των hackers. Παράλληλα αύξηση επιθέσεων malware, ransomware, phishing, νέες ευπαθιών και επιθέσεων εφοδιαστικής αλυσίδας διευρύνουν το τοπίο κινδύνου στον κυβερνοχώρο.

Η μετάβαση σε εφαρμογές SaaS, η αύξηση της απομακρυσμένης εργασίας, η αύξηση της κρυπτογραφημένης κίνησης έχουν δημιουργήσει πολλές προκλήσεις και προβλήματα που δεν μπορούν να αντιμετωπιστούν από τις κλασσικές αρχιτεκτονικές ασφαλείας που εφαρμόζουν όλες τις πολιτικών ασφάλειας κεντρικά λόγω πολυπλοκότητας, καθυστέρησης (latency), μη αποτελεσματικότητας και λιγότερης ασφάλειας στον κυβερνοχώρο. Γι' αυτό τον τελευταίο καιρό γίνεται συζήτηση για αρχιτεκτονικές ασφαλείας Zero Trust και SASE (Secure Access Service Edge) προκειμένου οι οργανισμοί θα θωρακίσουν την νέα περίμετρο (το τερματικό, τα δεδομένα, τις εφαρμογές τους στο cloud) με αποδοτικό τρόπο. Το SASE, ένας όρος που επινοήθηκε από την Gartner, δεν είναι μια νέα λύση και από τα μέσα του 2019 έχει γίνει ένα από τα πιο καυτά θέματα στη βιομηχανία Δικτύωσης και Κυβερνοασφάλειας και φέρνει τη Δικτύωση και την Ασφάλεια σε μια ενοποιημένη πλατφόρμα με στόχο να αυξήσει την επεκτασιμότητα, την ευελιξία και την ασφάλεια, μειώνοντας παράλληλα το συνολικό κόστος ιδιοκτησίας (TCO).

Σε αυτό το πλαίσιο η ανάπτυξη πρωτοπόρων και καινοτόμων λύσεων και υπηρεσιών ασφάλειας είναι ένας από τους στρατηγικούς πυλώνες της Cisco. Η αρχιτεκτονική ασφάλειας Cisco Zero Trust η οποία έχει αναγνωριστεί ως Leader σύμφωνα με την πρόσφατη ανάλυση Forrester Zero Trust Wave 2020 προσφέρει ολοκληρωμένη ασφάλεια για ασφαλή σύνδεση του εργατικου δυναμικού στο δίκτυο και στις εφαρμογές/δεδομενα και προσαρμόζεται δυναμικά για την αντιμετώπιση νέων επιπέδων κινδύνου παρεχοντας λύσεις όπως:

1. Το **Duo Security** προστατεύει με ολοκληρωμένη προσέγγιση μηδενικής αρχιτεκτονικής το εργατικό δυναμικό, και τις εφαρμογές διασφαλίζοντας ότι μόνο οι πιστοποιημένοι χρήστες με χρήση τεχνικών αυστηρής πιστοποίησης με Multifactor Authentication, Πρόσβαση χωρίς password (passwordless), SSO (single sign on) εχουν πρόσβαση σε οποιαδήποτε εφαρμογή του οργανισμού.

Ντίνα Συντίλα
Cyber Security Sales Specialist Leader Cisco, Greece, Portugal, Cyprus, Malta

Παράλληλα υπάρχει η δυνατότητα ελέγχου και της υγιεινής της συσκευής για παράδειγμα συμβατής με τις πολιτικές τις εταιρείας, εταιρικής η BYOD προτού εκχωρήσει πρόσβαση σε εφαρμογές – από οποιαδήποτε τοποθεσία, ακόμα και χωρίς την χρήση VPN.

2. Το Cisco Secure Workload εμποδίζει την εξάπλωση παραβιάσεων στα κέντρα δεδομένων και τα περιβάλλοντα στο cloud και προστατεύει μοναδικά τις κρίσιμες πληροφορίες με εντοπισμό ανωμαλίας στη συμπεριφορά επικοινωνίας προς κρίσιμες εφαρμογές, με χαρτογράφηση ευπάθειας σε συνδυασμό με μικροκατανομή (microsegmentation) που λειτουργεί σε οποιοδήποτε κέντρο δεδομένων, δημόσιο σύννεφο ή σε υβριδικά cloud καθώς και σε ιδιωτικά κέντρα δεδομένων καλύπτοντας και όλα τα περιβάλλοντα (bare metal, containers, VM)

3. Το Cisco SD-Access διασφαλίζει τις συνδέσεις χρηστών και συσκευών (IT, IOT) σε όλο το δίκτυό σας, και εμποδίζει την εξάπλωση παραβιάσεων εφαρμόζοντας ευέλικτη τμηματοποίηση (segmentation) για οποιαδήποτε συσκευή. Παράλληλα επιτυγχάνεται η ίδια εμπειρία και ασφάλεια από όπου συνδέεται ο χρήστης (LAN, WLAN, VPN).

4. Οι παραπάνω τεχνολογίες συνεργάζονται και με άλλες τεχνολογίες Cisco και τρίτων, μέσω της προσέγγισης της πλατφόρμας μας για την ασφάλεια – SecureX. Το Cisco SecureX επιτρέπει την ενιαία διαχείριση όλων των λύσεων ασφαλειας της Cisco και αυτοματοποιεί τις ενοποιήσεις σε όλες τις λύσεις Cisco Security ενώ, απλοποιεί σημαντικά τις έρευνες και τις απαντήσεις απειλών επιτρέποντας μείωση στο χρόνο εντοπισμού και ανταπόκρισης σε επιθέσεις μέσω δυνατοτήτων αυτοματισμού (SOAR, XDR).

Συνδυάζοντας τις δυνατότητες αρχιτεκτονικής μηδενικής εμπιστοσύνης με λύσεις VPN, SDWAN, και ασφάλειας στο Cloud παρέχουμε μία ολοκληρωμένη λύση ασφαλειας τόσο των απομακρυσμένων χρηστών όσο και των περιφερειακών γραφείων στο πλαίσιο της αρχιτεκτονικής SASE. Πιο συγκεκριμένα:

1. Το **Cisco Umbrella** είναι μια SaaS λύση που βασίζεται στο cloud και που προστατεύει τους χρήστες και τις συσκευές (mobile, laptop, IOT) από εξελιγμένες επιθέσεις zero day, κακόβουλο λογισμικό, phishing ransomware, cryptomining κα ενω επιτρέπει να εφαρμοστούν πολιτικές content filtering είτε οι χρήστες βρίσκονται εντός είτε εκτός του εταιρικού δικτύου. Μέσω μίας ενιαίας λύσης παρέχονται υπηρεσίες DNS ασφαλείας, Cloud Proxy, CASB, Data Loss Prevention, FWaaS, προστασία από malware σε υπηρεσίες στο cloud όπως sharepoint, one drive κ.ά.

2. Το Cisco Secure Endpoint, Παρέχει δυνατότητες αναζήτησης απειλών και απόκρισης (AV/EDR) σε μια ενιαία λύση, αξιοποιώντας μηχανισμούς μηχανικής εκμάθησης/ AI σε συνδυασμό με ισχυρά εργαλεία όπως η τροχιά αρχείων/συσκευής μπορούν να σας δείξουν το πλήρες εύρος μιας απειλής και να προσδιορίσει όλες τις επηρεαζόμενες εφαρμογές και συστήματα. Παράλληλα επιτρέπει την σημαντική μείωση του μέσου χρόνου εντοπισμού (MTTD) και μέσου χρόνου απόκρισης (MTTP) σε επιθέσεις με τη χρήση των ενσωματωμένων δυνατοτήτων αυτοματισμού και δυνατοτήτων απόκρισης στο σύνολο των λύσεων ασφαλείας (XDR).

Τέλος είναι γνωστό ότι ο κλάδος της κυβερνοασφάλειας αντιμετωπίζει τεράστια έλλειψη δεξιοτήτων/ ανθρώπινων πόρων και οι περισσότεροι οργανισμοί πρέπει να είναι πιο αποδοτικοί με λιγότερο ανθρώπινο δυναμικό. Ενοποιημένες λύσεις ασφάλειας με δυνατότητες αυτοματισμού που στοχεύουν στη μείωση χρόνου αντιμετώπισης επιθέσεων οπως αυτές που προαναφέρθηκαν είναι σύμμαχοι των οργανισμών σε αυτή την κατεύθυνση.
Εκτός όμως από τις λύσεις και οι υπηρεσίες επιτρέπουν στους οργανισμούς να ανταπεξέρχονται γρήγορα στο συνεχώς εξελισσόμενο threat landscape. Εχουμε επεκτείνει το σύνολο των υπηρεσιών μας με υπηρεσίες διαχειριζόμενες από ειδικούς της Cisco για πελάτες που αντιμετωπίζουν κενό δεξιοτήτων ή που θέλουν να αναθέσουν τη διαχείριση σε ειδικούς της Cisco για την ασφάλεια στον κυβερνοχώρο για τον εντοπισμό και την απόκριση στα συμβάντα ασφάλειας μέσω υπηρεσιών Managed Detection & Response (εκτεταμένη ανίχνευση και απόκριση) καθώς και υπηρεσίες για διαχείριση της απομακρυσμένης πρόσβασης Cisco Secure Managed Remote Access.