Deloitte.

Δελτίο Τύπου

Παγκόσμια έρευνα της Deloitte "Future of Cyber": Μεγάλη αύξηση των κυβερνοεπιθέσεων λόγω του ψηφιακού μετασχηματισμού

- *Το 72% των συμμετεχόντων στην έρευνα αναφέρει ότι οι οργανισμοί τους αντιμετώπισαν από ένα έως δέκα περιστατικά κυβερνοεπιθέσεων μόνο μέσα στο περασμένο έτος.*
- *Παρά τους κινδύνους, οι επικεφαλής των οικονομικών επιτελείων δηλώνουν ότι θα συνεχίσουν να μεταφέρουν τα συστήματα οικονομικής πληροφόρησης των επιχειρήσεών τους στο cloud.*
- *Σχεδόν το 75% των συμμετεχόντων που σημείωσαν κερδοφορία ίση και μεγαλύτερη από 30 δισ. δολάρια δήλωσαν ότι φέτος θα επενδύσουν πάνω από 100 εκ. δολάρια για την κυβερνοασφάλεια.*

Αθήνα, 11 Νοεμβρίου 2021 - Η Deloitte δημοσίευσε πρόσφατα την παγκόσμια έκθεση "Future of Cyber" του 2021, στην οποία συμμετείχαν περίπου 600 υψηλόβαθμα (C-Level) στελέχη που διαθέτουν πρόσβαση στις λειτουργίες κυβερνοασφάλειας των οργανισμών τους. Στόχος της έκθεσης είναι να φέρει στο προσκήνιο τη συζήτηση γύρω από την εφαρμογή μέτρων κυβερνοασφάλειας στον πυρήνα κάθε επιχείρησης, καθώς και να προσφέρει χρήσιμα στοιχεία αναφορικά με το πώς θα μπορέσουν οι οργανισμοί να αυξήσουν την ορατότητα σύνθετων τεχνολογικών οικοσυστημάτων, αλλά και να εφαρμόσουν βέλτιστες πρακτικές ώστε να προετοιμαστούν για τις μελλοντικές προκλήσεις του κυβερνοχώρου.

Η έρευνα της Deloitte έδειξε ότι το 69% των παγκόσμιων ηγετών επιχειρήσεων που ερωτήθηκαν, σημείωσαν πως οι επιχειρήσεις τους βίωσαν σημαντική αύξηση των κυβερνοεπιθέσεων τη χρονιά που πέρασε, εν μέσω της επιτάχυνσης του ψηφιακού μετασχηματισμού. Ωστόσο, την ίδια στιγμή που οι κίνδυνοι αυξάνονται, οι ηγέτες σχεδιάζουν σημαντικές επενδύσεις στον ψηφιακό μετασχηματισμό. Συγκεκριμένα, σχεδόν καθολική είναι η στρατηγική των επικεφαλής των οικονομικών επιτελείων προς αυτή την κατεύθυνση, με το 94% να δηλώνει ότι σκοπεύει να μεταφέρει τα συστήματα οικονομικής πληροφόρησης σε περιβάλλον cloud. Μάλιστα, σύμφωνα με την έρευνα της Deloitte, ενώ δεν υπάρχουν απλές λύσεις, η ταυτόχρονη υιοθέτηση μιας σειράς μέτρων μπορεί να βοηθήσει μια επιχείρηση να εφαρμόσει την κυβερνοασφάλεια σε κάθε πτυχή της λειτουργίας της.
Σύμφωνα με την **Emily Mossburg**, Global Cyber Leader της Deloitte, οι επιχειρήσεις εργάζονται εντατικά αυτό το χρόνο για να παραμείνουν ανταγωνιστικές εν μέσω ταχύτατων τεχνολογικών αλλαγών καθώς η επιτάχυνση του ψηφιακού μετασχηματισμού έχει αυξήσει δραστικά την τρωτότητά τους σε κυβερνοεπιθέσεις. Η ίδια σημειώνει ότι ενώ οι πολυπλοκότητες αυξάνονται, οι ηγέτες οφείλουν να θέσουν σε προτεραιότητα την

εφαρμογή της κυβερνοασφάλειας σε κάθε πτυχή των επιχειρήσεων, ειδάλλως διακινδυνεύουν να υποστούν τις συνέπειες ανεπαρκούς προστασίας.

Ο ψηφιακός μετασχηματισμός ενισχύει την ανάγκη για στρατηγική κυβερνοασφάλειας
Με περισσότερες από τις μισές επιχειρήσεις να βιώνουν αύξηση των απειλών μέσα στο 2020, οι κίνδυνοι βρίσκονται σε υψηλότερα επίπεδα από ποτέ, καθώς η υιοθέτηση μοντέλων απομακρυσμένης και υβριδικής εργασίας εφαρμόζεται ολοένα και περισσότερο σε επιχειρήσεις σε όλο τον κόσμο. Οι οργανισμοί συνεχίζουν να αντιμετωπίζουν προκλήσεις στο να ισορροπήσουν μεταξύ των επενδύσεων στον ψηφιακό μετασχηματισμό για να παραμείνουν ανταγωνιστικοί και του να προστατεύσουν τα συστήματά τους από πιθανές επιθέσεις. Απαντώντας στην έρευνα της Deloitte, οι επικεφαλής Διευθύνσεων Πληροφορικής (CIOs) και Ασφάλειας (CISOs), αναγνωρίζουν σε ποσοστό 41% ότι η μεγαλύτερη πρόκληση που αντιμετωπίζουν είναι ο μετασχηματισμός και η απόκτηση ορατότητας σε αυξανόμενης πολυπλοκότητας υβριδικά οικοσυστήματα.

Το κύμα της «Μηδενικής Εμπιστοσύνης»
Όπως δείχνει η παγκόσμια έρευνα της Deloitte, τα σημεία που αποτελούν τις μεγαλύτερες προκλήσεις σε ό,τι αφορά τη διαχείριση των κινδύνων του κυβερνοχώρου είναι οι υβριδικές τεχνολογίες πληροφορικής σε ποσοστό 41% και η κυβερνο-υγιεινή (cyber hygiene) σε ποσοστό 26%. Ως εκ τούτου, οι επιχειρήσεις αξιοποιούν την πρακτική της Μηδενικής Εμπιστοσύνης (Zero Trust), δηλαδή μια αρχιτεκτονική που βασίζεται στη θεμελιώδη αρχή του «ποτέ μην εμπιστεύεσαι, πάντα να επιβεβαιώνεις», προκειμένου να γεφυρώσουν το χάσμα μεταξύ της επιχειρηματικής δραστηριότητας, της πληροφορικής και των τομέων του κυβερνοχώρου. Έτσι, επιτυγχάνεται η μείωση της επιχειρησιακής πολυπλοκότητας και η απλοποίηση ενσωμάτωσης διαφόρων οικοσυστημάτων. Οι επιχειρήσεις που αξιοποιούν την αρχή της «Μηδενικής Εμπιστοσύνης» οδηγούν τις εξελίξεις στον τομέα της οργανωτικής αλλαγής προκειμένου να επιτύχουν τον ψηφιακό μετασχηματισμό, χτίζοντας υποδομές ασφάλειας με τις οποίες μπορούν να χειριστούν την ταχύτητα αυτού του μετασχηματισμού.

Η επένδυση στην κυβερνοασφάλεια σημαίνει επένδυση στην ασφάλεια των πληροφοριακών συστημάτων (CISO)
Με τους κυβερνοεγκληματίες να γίνονται ολοένα και πιο ικανοί, οι επιχειρήσεις τείνουν να αυξάνουν τους προϋπολογισμούς τους για την κυβερνοασφάλεια. Σχεδόν το 75% των συμμετεχόντων ηγετών με πάνω από 30 δισ. δολάρια σε κέρδη συνολικά, δήλωσαν ότι θα επενδύσουν περισσότερα από 100 εκ. δολάρια στην κυβερνοασφάλεια φέτος. Ενώ αυτές οι επενδύσεις μοιράζονται σχετικά ισορροπημένα, η έρευνα κατέδειξε ότι μεγαλύτερη προσοχή δίνεται σε ζητήματα ανίχνευσης και παρακολούθησης απειλών, μετασχηματισμού του κυβερνοχώρου και προστασίας δεδομένων.

Η σύγκλιση της τεχνολογικής ικανότητας και η αύξηση των κυβερνοαπειλών αλλάζουν το ρόλο των επικεφαλής ασφάλειας πληροφοριών. Όσο η τεχνολογία ενσωματώνεται ολοένα και περισσότερο καθημερινά στις δραστηριότητες των επιχειρήσεων, τόσο ενισχύονται οι ευθύνες των επικεφαλής. Σύμφωνα με την έρευνα της Deloitte, σημειώνεται αύξηση της απευθείας αναφοράς των επικεφαλής ασφάλειας πληροφοριών (CISOs) στους επικεφαλής των επιχειρήσεων (CEOs) από 32% το 2019 σε 42% το 2021 στις ΗΠΑ, ενώ φτάνει στο 33% σε παγκόσμιο επίπεδο. Αυτή η τάση ενισχύει τη διαφάνεια επιχειρηματικών πρωτοβουλιών

και τη δέσμευση σε περισσότερα επίπεδα, κυρίως σε επίπεδο C-Level, η οποία είναι κρίσιμη για την αντιμετώπιση κυβερνοαπειλών και για τη δημιουργία αυθεντικών και ασφαλών εμπειριών για τους πελάτες.

Η έρευνα δείχνει ότι μέσα στην επόμενη τριετία οι CIOs και CISOs θα συνεχίσουν να δίνουν προτεραιότητα στην κυβερνοασφάλεια, με το 64% να προτεραιοποιεί τις ικανότητες ασφάλειας, το 59% την ενίσχυση της ιδιωτικότητας, το 50% την ικανότητα συμμόρφωσης και το 45% τη βελτίωση της επιχειρησιακής αποτελεσματικότητας και πληροφόρησης, ως τους κύριους λόγους υιοθέτησης νέων τεχνολογιών.

Με αφορμή τη δημοσιοποίηση της έρευνας, ο **κος Χρήστος Βιδάκης, Risk Advisory Partner, Cyber Leader της Deloitte Greece**, σχολίασε: *«Η νέα παγκόσμια έρευνα της Deloitte για το μέλλον της κυβερνοασφάλειας στην οποία συμμετείχαν άνω των 600 στελεχών παγκοσμίως, μεταξύ των οποίων και στελέχη ελληνικών επιχειρήσεων, επιβεβαιώνει την τάση που υπάρχει και στην ελληνική αγορά, η οποία θέτει την κυβερνοασφάλεια ως έναν από τους τρεις κυριότερους επιχειρηματικούς κινδύνους. Στην εποχή του ψηφιακού μετασχηματισμού, η οποία έχει αναδειχθεί ως πυλώνας ανάπτυξης και των ελληνικών επιχειρήσεων, συχνά διαφαίνεται ότι η τεχνολογική καινοτομία και η κουλτούρα, η οποία τη συνοδεύει, αναπτύσσεται με ταχύτερο ρυθμό από την ικανότητά μας να κατανοούμε, να μετράμε και να ανταποκρινόμαστε στους κινδύνους του κυβερνοχώρου. Δεν είναι τυχαίο λοιπόν το γεγονός ότι το 70% των ερωτηθέντων ανέφεραν άνοδο στον αριθμό των περιστατικών κυβερνοασφάλειας τα τελευταία δυο χρόνια, ενώ ένας στους τρεις αναδεικνύουν τη διαθεσιμότητα των λειτουργιών ως την πιο σημαντική επίπτωση αυτών. Σήμερα, σύμφωνα με την έρευνα, οι προϋπολογισμοί των επιχειρήσεων είναι ισόποσα μοιρασμένοι στους διαφόρους τομείς κυβερνοασφάλειας. Ωστόσο, ένας στους τρεις θεωρεί ότι πρέπει να υπάρξει καλύτερη προτεραιοποίηση στη διανομή των πόρων. Σ' αυτόν τον τομέα, έδαφος κερδίζει η υιοθέτηση της προσέγγισης Zero Trust. Συνεπώς, με την απόλυτη ασφάλεια να μην είναι ρεαλιστική, η συνεργασία των επιχειρήσεων και ο διαμοιρασμός της γνώσης σε θέματα κυβερνοασφάλειας φαντάζει μονόδρομος».*

Η μεθοδολογία της έρευνας

Σημειώνεται ότι στην έρευνα 2021 Future of Cyber που πραγματοποιήθηκε από την Deloitte Global και τη Wakefield Research, συμμετείχαν σχεδόν 600 στελέχη C-Level που ερωτήθηκαν σχετικά με την κυβερνοασφάλεια σε επιχειρήσεις με τουλάχιστον 500 εκ. δολάρια σε κέρδη ετησίως, μεταξύ των οποίων υπήρχαν σχεδόν 200 CISOs, 100 CIOs, 100 CFOs και 100 CMOs. Η έρευνα πραγματοποιήθηκε διαδικτυακά μεταξύ 6 Ιουνίου και 24 Αυγούστου 2021.

Μπορείτε να επισκεφτείτε το ακόλουθο link για τα πλήρη αποτελέσματα της Deloitte Global's 2021 Future of Cyber Survey, www.deloitte.com/futureofcyber

Για περισσότερες πληροφορίες

Deloitte, Κέλλυ Κουφοπούλου, Manager, Brand & Communications
email: kkoufopoulou@deloitte.gr