Δελτίο Τύπου

Ημερομηνία:	8 Μαρτίου 2022
Υπεύθυνος επικοινωνίας:	Κάλλια Μυλωνάκη Τηλ: 210 8114386 e-mail: kallia.mylonaki@pwc.com

Οι εταιρείες ενδέχεται να παραβλέπουν τους πιο σημαντικούς κινδύνους για την κυβερνοασφάλεια

«Τυφλό σημείο» οι απειλές που προέρχονται από τρίτους, σύμφωνα με έρευνα της PwC

Η πλειονότητα των επιχειρήσεων δεν διαχειρίζεται επαρκώς τους κινδύνους που αφορούν στην κυβερνοασφάλεια και προέρχονται από τρίτα μέρη, καθώς οι κίνδυνοι αυτοί επισκιάζονται από την πολυπλοκότητα των διαδικασιών και λειτουργιών καθώς και των δικτύων των προμηθευτών τους. Το συμπέρασμα αυτό προκύπτει από την έρευνα της PwC «2022 Global Digital Trust Insights Survey». Στην μελέτη συμμετείχαν 3.600 CEO καθώς και άλλα ανώτερα στελέχη από όλο τον κόσμο, 60% των οποίων δηλώνουν πως δεν κατανοούν πλήρως τους κινδύνους παραβίασης δεδομένων μέσω τρίτων, ενώ αντίστοιχα κατανοούν λίγο ή και καθόλου τους κινδύνους αυτούς σε ποσοστό 20%.

Τα ευρήματα αυτά κρούουν τον κώδωνα του κινδύνου σε ένα περιβάλλον όπου το 60% των ανώτερων στελεχών αναμένουν αύξηση του κυβερνοεγκλήματος το 2022. Επίσης, αναδεικνύουν τις προκλήσεις που αντιμετωπίζουν οι επιχειρήσεις στην προσπάθεια τους να εξασφαλίσουν συνθήκες εμπιστοσύνης αναφορικά με τα δεδομένα τους, διασφαλίζοντας ότι είναι ακριβή, επιβεβαιωμένα και ασφαλή, ώστε οι πελάτες τους αλλά και κάθε άλλος εμπλεκόμενος να έχει τη βεβαιότητα ότι οι πληροφορίες τους είναι επαρκώς προστατευμένες.

Αξίζει να σημειωθεί ότι 56% των ερωτηθέντων αναφέρουν ότι οι οργανισμοί τους αναμένουν αύξηση στις κακόβουλες επιθέσεις και παραβιάσεις δεδομένων που πραγματοποιούνται μέσω της εφοδιαστικής αλυσίδας λογισμικού (software supply chain), ωστόσο μόλις το 34% έχουν αξιολογήσει επισήμως την έκθεση της επιχείρησής τους στον κίνδυνο αυτό. Αντίστοιχα, σε ποσοστό 58% αναμένουν κατακόρυφη άνοδο στις επιθέσεις στις υπηρεσίες τους στο cloud, μόλις όμως 37% δηλώνουν ότι κατανοούν τους κινδύνους του cloud βασιζόμενοι σε επίσημες αξιολογήσεις.

Ο **Sean Joyce, Global & US Cybersecurity & Privacy Leader της PwC Ηνωμένων Πολιτειών** σχολιάζει: «Οι επιχειρήσεις ενδέχεται να είναι ευάλωτες σε επιθέσεις ακόμα και όταν τα δικά τους συστήματα κυβερνοάμυνας είναι επαρκή - ένας επιτιθέμενος υψηλού επιπέδου αναζητεί τον πιο αδύναμο κρίκο, και

κάποιες φορές αυτός βρίσκεται ανάμεσα στους προμηθευτές της επιχείρησης. Είναι απαραίτητη η αύξηση της ορατότητας και η διαχείριση των σχέσεων και εξαρτήσεων μιας εταιρείας από τρίτους. Ωστόσο, σύμφωνα με την έρευνά, λιγότεροι από τους μισούς ερωτηθέντες έχουν ανταποκριθεί στις κλιμακούμενες απειλές που ανακύπτουν από τα πολύπλοκα επιχειρηματικά οικοσυστήματα».

Σχετικά με το πώς περιορίζουν οι εταιρείες τους κινδύνους που προκύπτουν από τρίτους, οι πιο συχνές απαντήσεις αφορούσαν στον έλεγχο ή την επιβεβαίωση της συμμόρφωσης των προμηθευτών τους (46%), την κοινή χρήση πληροφοριών με τρίτους καθώς και την παροχή βοήθειας προς αυτούς για τη βελτίωση της στάσης τους ως προς την κυβερνοασφάλεια (42%) και την αντιμετώπιση των δυσκολιών σε σχέση με το κόστος ή τον χρόνο που επενδύουν προκειμένου να εξασφαλίσουν ανθεκτικότητα απέναντι στις κυβερνοαπειλές (40%). Ωστόσο, η πλειοψηφία δεν έχει προσδιορίσει τα κριτήρια απέναντι σε τρίτα μέρη (58%), δεν έχει αναθεωρήσει τις συμβάσεις (60%), ούτε έχει αυξήσει την αυστηρότητα της δέουσας επιμέλειας (62%) αναφορικά με τον εντοπισμό απειλών που σχετίζονται με τρίτους.

Απλοποιώντας την κυβερνοασφάλεια

Σχεδόν τα τρία τέταρτα των ερωτηθέντων ανέφεραν ότι η πολυπλοκότητα των λειτουργιών και διαδικασιών εγείρει κινδύνους για την κυβερνοασφάλεια και την προστασία των δεδομένων. Αντίστοιχα, η διακυβέρνηση και οι υποδομές δεδομένων (77% έκαστο) αποτελούν τους δύο τομείς που θεωρείται πως χαρακτηρίζονται από μη απαραίτητη πολυπλοκότητα, η οποία και μπορεί να αποφευχθεί.

Η απλοποίηση σίγουρα είναι δύσκολη, αλλά υπάρχει μια σειρά από αποδείξεις ότι προσφέρει σημαντικά οφέλη. Ενώ τρεις στους 10 ερωτηθέντες συνολικά απάντησαν ότι οι επιχειρήσεις τους είχαν εξορθολογίσει τις λειτουργίες τους τα τελευταία δύο χρόνια, εκείνοι που είχαν σημειώσει την «μεγαλύτερη βελτίωση» στην έρευνα (το 10% με τις κορυφαίες επιδόσεις στα αποτελέσματα κυβερνοασφάλειας) ήταν πέντε φορές πιο πιθανόν να έχουν εξορθολογίσει τις λειτουργίες σε όλο το εύρος της επιχείρησης. Αυτό το 10% των οργανισμών, ήταν επίσης 10 φορές πιο πιθανόν να έχει υιοθετήσει επισήμως πρακτικές διασφάλισης εμπιστοσύνης δεδομένων και 11 φορές πιο πιθανόν να κατανοεί σε υψηλό επίπεδο τους κινδύνους κυβερνοασφάλειας και προστασίας δεδομένων όσον αφορά τα τρίτα μέρη.

Η συμμετοχή των CEO μπορεί να κάνει τη διαφορά

Σημαντική διαφοροποίηση προέκυψε ανάμεσα στα στελέχη και τους CEO αναφορικά με την στήριξη που παρέχει ο CEO στην κυβερνοασφάλεια, με τους ίδιους να θεωρούν ότι συμμετέχουν και υποστηρίζουν την υιοθέτηση και επίτευξη των στόχων για την κυβερνοασφάλεια περισσότερο από ότι οι ομάδες τους. Δεν υπάρχει όμως διαφωνία ως προς το ότι η ενεργή δραστηριοποίηση του CEO στην υιοθέτηση και επίτευξη των στόχων κυβερνοασφάλειας είναι καθοριστικός παράγοντας. Τα στελέχη στην ομάδα με τη «μεγαλύτερη βελτίωση» αναφέρουν μεγαλύτερη πρόοδο στα αποτελέσματα όσον αφορά στην κυβερνοασφαλεια, στις περιπτώσεις κατά τις οποίες ήταν 12 φορές πιο πιθανόν να έχουν την ευρεία και σε βάθος στήριξη των CEO τους. Τα περισσότερα στελέχη επίσης θεωρούν ότι η εκπαίδευση των CEO και των διοικητικών συμβουλίων προκειμένου να ανταποκρίνονται καλύτερα στις υποχρεώσεις τους ως προς την κυβερνοασφάλεια είναι το πιο σημαντικό βήμα για μια πιο ασφαλή ψηφιακή κοινωνία έως το 2030.

Με αφορμή τα αποτελέσματα της έρευνας ο **Γιώργος Κολλιδάς, Partner, Advisory, Technology Leader της PwC Ελλάδας** επισημαίνει: «Η έρευνα καταδεικνύει ότι οι πιο εξελιγμένες επιχειρήσεις αντιλαμβάνονται την κυβερνοασφάλεια ως κάτι ευρύτερο από άμυνα και ελέγχους - θεωρούν ότι είναι το μέσο για την επίτευξη βιώσιμων επιχειρηματικών αποτελεσμάτων και την αύξηση της εμπιστοσύνης των πελατών τους. Ως επικεφαλής των επιχειρήσεων, οι CEO οφείλουν να δίνουν το κίνητρο και το όραμα προκειμένου οι ομάδες κυβερνοασφάλειάς τους να εστιάζουν στην μεγαλύτερη εικόνα και σε στόχους ανάπτυξης, παρά σε στενότερες και πιο βραχυπρόθεσμες προσδοκίες».

Τέλος.

Σημειώσεις για τους συντάκτες

Σχετικά με την Έρευνα

Στην έρευνα «2022 Global Digital Trust Insights» συμμετείχαν 3.602 στελέχη επιχειρήσεων στους τομείς της τεχνολογίας και της ασφάλειας (CEOs, corporate directors, CFOs, CISOs, CIOs και στελέχη C-Suite) ενώ πραγματοποιήθηκε τον Ιούλιο και τον Αύγουστο του 2021 από την PwC Research. 62% των ερωτηθέντων απασχολούνται σε εταιρείες με έσοδα US$ 1 δισ. και άνω και 33% σε εταιρείες με έσοδα US$ 10 δισ. και άνω. Οι ερωτηθέντες δραστηριοποιούνται σε μια σειρά κλάδων: τεχνολογία, μέσα ενημέρωσης, τηλεπικοινωνίες (23%), μεταποίηση (22%), χρηματοοικονομικές υπηρεσίες (20%), λιανεμπόριο και καταναλωτικές αγορές (16%), ενέργεια, ΥΚΩ και πόροι (8%), υγεία (7%) και κυβέρνηση και δημόσιες υπηρεσίες (3%). Ανά περιοχή μοιράζονται ως εξής: Δυτική Ευρώπη (33%), Βόρεια Αμερική (26%), Ασία Ειρηνικός (18%), Λατινική Αμερική (10 %), Ανατολική Ευρώπη (4%), Μέση Ανατολή (4%) και Αφρική (4%).

Σχετικά με την PwC

Στην PwC, στόχος μας είναι η δημιουργία κλίματος εμπιστοσύνης στην κοινωνία και η επίλυση σημαντικών προβλημάτων. Είμαστε ένα δίκτυο εταιρειών σε 156 χώρες με περισσότερα από 295.000 στελέχη που δεσμεύονται να παραδίδουν ποιοτικό έργο στις ελεγκτικές, φορολογικές και συμβουλευτικές υπηρεσίες που αναλαμβάνουν. Πείτε μας τι έχει αξία για σας και μάθετε ακόμα περισσότερα στην ιστοσελίδα μας www.pwc.com.

Η επωνυμία PwC αναφέρεται στο δίκτυο των εταιρειών μελών και/ή σε μία ή περισσότερες από τις εταιρείες μέλη, κάθε μία από τις οποίες αποτελεί μια ξεχωριστή νομική οντότητα. Για περισσότερες πληροφορίες, παρακαλούμε επισκεφθείτε το www.pwc.com/structure.