Δελτίο Τύπου

Ημερομηνία:	29 Οκτωβρίου 2020
Υπεύθυνος επικοινωνίας:	Κάλλια Μυλωνάκη Τηλ: 210 8114386 e-mail: kallia.mylonaki@pwc.com

Ετήσια μελέτη της PwC Digital Trust Insights 2021

Η πανδημία έχει οδηγήσει το 96% των στελεχών στην αναθεώρηση της στρατηγικής κυβερνοασφάλειας

Σύμφωνα με την ετήσια μελέτη της PwC «Digital Trust Insights series - *Global Digital Trust Insights 2021: Cybersecurity comes of age*» ο τομέας της κυβερνοασφάλειας βρίσκεται σε φάση ωρίμανσης. Βάσει της μελέτης η οποία περιλαμβάνει συμπεράσματα σχετικά με την υφιστάμενη κατάσταση και τις αλλαγές του μέλλοντος, η κυβερνοασφάλεια βρίσκεται σε κρίσιμη καμπή για τον κλάδο, τις εταιρείες και τους ανθρώπους,

Τα σχόλια των ερωτηθέντων 3.249 ερωτηθέντων εστίασαν σε πέντε βασικούς τομείς: την αναβάθμιση της στρατηγικής για την κυβερνοασφάλεια, την θωράκιση των ομάδων κυβερνοασφάλειας για το μέλλον, τη βέλτιστη αξιοποίηση των προϋπολογισμών για την κυβερνοασφάλεια, τις επενδύσεις για αντιμετώπιση όσων επιτίθενται και τη βελτίωση της ανθεκτικότητας.

Αναβάθμιση της στρατηγικής για την ασφάλεια στον κυβερνοχώρο

Συντριπτικό ποσοστό της τάξης του 96% των ερωτηθέντων ανέφεραν ότι σχεδιάζουν να τροποποιήσουν τη στρατηγική τους για την κυβερνοασφάλεια λόγω του COVID-19, με το 50% να δηλώνει ότι είναι πιο πιθανόν πλέον να λαμβάνουν υπόψη τους την κυβερνοασφάλεια σε κάθε επιχειρηματική απόφαση, σε σύγκριση με 25% πέρυσι. Επιπλέον, 51% των CEO δηλώνουν ότι είναι πιο πιθανόν να έχουν συχνές αλληλεπιδράσεις με τον Υπεύθυνο Ασφάλειας Πληροφοριών (CISO). Κατά τους τρεις πρώτους μήνες της πανδημίας, όπως ανέφεραν οι CEO, οι επιχειρήσεις τους επιτάχυναν την ψηφιοποίησή τους με εκπληκτική ταχύτητα, μεταβαίνοντας κατευθείαν στο δεύτερο ή τρίτο έτος των πενταετών πλάνων τους.

Η ανάπτυξη ενός ταχύτερου και πιο αποτελεσματικού τρόπος δράσης αποτελεί υψηλή προτεραιότητα για το 29% των στελεχών, ενώ σε ποσοστό 31% εκσυγχρονίζονται με βάση τις νέες δυνατότητες που παρέχει

η τεχνολογία. Περισσότεροι από το ένα τρίτο (35%) δηλώνουν ότι επιταχύνουν την αυτοματοποίηση για να μειώσουν τα κόστη.

Ο Μιχάλης Σαμιωτάκης, Senior Manager, Technology Consulting, Cybersecurity σχολίασε: «Δεδομένων των πρωτοφανών επιδράσεων του COVID-19, πολλές επιχειρήσεις χρειάστηκε να επανεξετάσουν και να επαναπροσδιορίσουν την στρατηγική τους για την κυβερνοασφάλεια λαμβάνοντας υπόψη το νέο «ψηφιακό περιβάλλον»που διαμορφώνεται με αιχμή την ανάπτυξη κατάλληλων υποδομών «απομακρυσμένης εργασίας» και την "ψηφιοποίηση" των καναλιών επικοινωνίας, υπηρεσιών και συναλλαγών. Η ταχεία υλοποίηση των δράσεων μετασχηματισμού εγείρει ωστόσο κινδύνους κυβερνοασφάλειας τους οποίους οι CISO καλούνται να διαχειριστούν ενώ παράλληλα στηρίζουν την ψηφιακή στρατηγική των οργανισμών τους. Ο εξελισσόμενος ρόλος του CISO και η σημασία του για την εταιρεία δεν υπήρξε ποτέ πιο κρίσιμος τόσο για την επιβίωση όσο και για την ανάπτυξή της"

Θωράκιση των ομάδων κυβερνοασφάλειας για το μέλλον με το απαραίτητο προσωπικό

Με 3,5 εκατομμύρια θέσεις εργασίας στην κυβερνοασφάλεια που αναμένεται να καλυφθούν έως το 2021, το πρόβλημα που ταλανίζει τον κλάδο της κυβερνοασφάλειας είναι η έλλειψη εξειδικευμένων εργαζομένων. Σε ποσοστό 51% τα στελέχη ανέφεραν ότι σχεδιάζουν να προσλάβουν προσωπικό πλήρους απασχόλησης στην κυβερνοασφάλεια κατά τη διάρκεια του επόμενου έτους, με περισσότερους από 22% να δηλώνουν ότι θα αυξήσουν το προσωπικό κατά 5% ή περισσότερο.

Οι θέσεις με το μεγαλύτερο ενδιαφέρον αφορούν σε αρχιτέκτονες λύσεων cloud 43%, υπεύθυνους ασφάλειας πληροφοριών 40% και ανάλυση δεδομένων 37%. Μια εναλλακτική λύση που έχουν αξιοποιήσει πολλές επιχειρήσεις για να καλύψουν τις κενές θέσεις, είναι οι εσωτερικές μετακινήσεις, μέσα από την αναβάθμιση δεξιοτήτων των υφιστάμενων εργαζομένων. Κάποιες εταιρείες έχουν ξεκινήσει να βασίζονται στο μοντέλο παροχής υπηρεσιών για να καλύψουν την άμεση ανάγκη για εξειδικευμένο ταλαντούχο προσωπικό.

Επανεξέταση των προϋπολογισμών για την κυβερνοασφάλεια

Περισσότερες από τις μισές εταιρείες (55%), δηλώνουν ότι ο προϋπολογισμός τους για την κυβερνοασφάλεια θα αυξηθεί το 2021. Ενώ ένας μεγαλύτερος προϋπολογισμός για την κυβερνοασφάλεια αποτελεί καλή είδηση, ο κλάδος θα πρέπει να αναμένει αλλαγές στον τρόπο διαχείρισής του στο μέλλον. Περισσότεροι από τους μισούς ερωτηθέντες (55%) εξέφρασαν χαμηλή εμπιστοσύνη ότι οι δαπάνες τους για την κυβερνοασφάλεια διατίθενται προς τους πιο σημαντικούς κινδύνους για την επιχείρηση. Σε ποσοστό 44%, αναφέρουν ότι σκέφτονται να αλλάξουν τη διαδικασία κατάρτισης του προϋπολογισμού τους, και κατά 37% συμφωνούν ότι η ποσοτικοποίηση των κινδύνων του κυβερνοχώρου μπορεί να βελτιώσει σημαντικά τον τρόπο με τον οποίο διαχειρίζονται τις δαπάνες για τους κινδύνους. Παρόλα αυτά, περισσότεροι από το ένα τρίτο συμφωνούν σαφώς ότι οι εταιρείες μπορούν να ενισχύσουν την στάση τους στο θέμα της κυβερνοασφάλειας ενώ ταυτόχρονα συγκρατούν τα κόστη χάρη στην αυτοματοποίηση και τον εξορθολογισμό της τεχνολογίας.

Εξισώνοντας τους όρους έναντι των κυβερνοεπιθέσεων

Η καινοτομία και η τεχνολογία αλλάζουν τον τρόπο με τον οποίο οι επιχειρήσεις εξισώνουν τους όρους έναντι των κυβερνοεπιθέσεων, με 43% των στελεχών να λένε ότι έχει βελτιωθεί η εμπειρία του πελάτη, και ότι ανταποκρίνονται πιο γρήγορα στα περιστατικά ασφαλείας . Τα προσδοκώμενα αποτελέσματα για τα επόμενα 2-3 χρόνια είναι: αυξημένη πρόληψη έναντι των επιθέσεων, ταχύτεροι χρόνοι ανταπόκρισης, βελτιωμένη εμπιστοσύνη των επικεφαλής σχετικά με την ικανότητα διαχείρισης απειλών και βελτιωμένη εμπειρία του πελάτη.

Σύμφωνα με τα αποτελέσματα της έρευνας, τα στελέχη από τις μεγάλες εταιρείες (με αξία άνω του 1 δισ. δολ.) είναι πιο πιθανό να αναφέρουν οφέλη από τη στρατηγική μεταστροφή σε προηγμένες τεχνολογίες και την αναδιάρθρωση των λειτουργιών ασφάλειας. Οι ερωτηθέντες από τις μεγαλύτερες επιχειρήσεις (με αξία άνω των 10 δισ. δολ.) ήταν επίσης πιο πιθανό να αναφέρουν οφέλη από την χρήση μοντέλων ασφάλειας και τεχνολογιών, συμπεριλαμβανομένης των Zero Trust, διαχειριζόμενων υπηρεσιών, και επιταχυνόμενη υιοθέτηση του cloud.

Τα ευρήματα αυτά υποδηλώνουν ότι η επένδυση σε τεχνολογίες, διαδικασίες, αλλά και στους ανθρώπους, είναι ουσιαστική για να πάρουν οι εταιρείες το προβάδισμα έναντι όσων τους επιτίθενται. Επιπλέον υπογραμμίζουν τη σημασία του CISO, ο οποίος μπορεί να παίξει σημαντικό ρόλο στον μετασχηματισμό.

Αύξηση της ανθεκτικότητας

Στη διάρκεια μιας χρονιάς γεμάτης από «πρωτιές»: στην οικονομία, τη δημόσια υγεία και το ηλεκτρονικό εμπόριο, υπήρξε μια αύξηση των περιστατικών εισβολών, ransomware, παραβίασης δεδομένων σε υγειονομικά και εκπαιδευτικά ιδρύματα, καθώς και phishing. Ως αποτέλεσμα, το 40% των στελεχών που ερωτήθηκαν είπαν ότι σχεδιάζουν να αυξήσουν τους ελέγχους ανθεκτικότητας για να διασφαλίσουν ότι οι κρίσιμες επιχειρησιακές διεργασίες θα συνεχίσουν να παρέχονται ακόμα και στην περίπτωση κάποιου ανατρεπτικού περιστατικού κυβερνοασφάλειας.

«Η οργάνωση της ασφάλειας της επόμενης γενιάς έχει τριπλή αποστολή: να χτίσει εμπιστοσύνη, να βελτιώσει την ανθεκτικότητα και να επιταχύνει την καινοτομία. Με λίγα λόγια, πρόκειται να διαφέρει πολύ από την οργάνωση της ασφάλειας σήμερα», λέει ο Sean Joyce, Global Cybersecurity, Privacy, and Forensics leader της PwC των ΗΠΑ.

Οι προβλέψεις για τους κινδύνους το 2021: Το Ίντερνετ των Πραγμάτων (IoT) και οι πάροχοι υπηρεσιών cloud βρίσκονται στην κορυφή της λίστας των «πολύ πιθανών» απειλών (από 33%) ενώ οι κυβερνοεπιθέσεις στις υπηρεσίες cloud είναι πρώτες στη λίστα των απειλών που θα έχουν «σημαντικά αρνητικό αντίκτυπο» (αναφέρθηκαν από το 24%).

Σημειώσεις για τους συντάκτες:

«Cybersecurity comes of age: Global Digital Trust Insights 2021» με βάση την έρευνα της PwC σε 3.249 επιχειρηματικά και τεχνολογικά στελέχη από ολόκληρο τον κόσμο. Για να λάβετε αντίγραφο ολόκληρης της έκθεσης, ανατρέξτε στη διεύθυνση https://www.pwc.com/us/en/services/consulting/cybersecurity/library/global-digital-trust-insights

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 157 χώρες με περισσότερα από 276.000 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.