Δελτίο Τύπου

Ημερομηνία:	01 Νοεμβρίου 2023
Υπεύθυνος επικοινωνίας:	Kate Σάπαρη kate.sapari@pwc.com Βάσω Γρίβα vasso.griva@pwc.com

Ετήσια Μελέτη της PwC: Global Digital Trust Insights 2024

Οι επικεφαλής των επιχειρήσεων δηλώνουν απροετοίμαστοι απέναντι στις νέες τεχνολογικές προκλήσεις, όπως το Generative AI

- **Η τεχνολογία και οι ψηφιακές εφαρμογές αξιολογήθηκαν ως ο κορυφαίος κίνδυνος, σε σχεδόν διπλάσιο ποσοστό συγκριτικά με τις φυσικές καταστροφές, την πανδημία και την ανισότητα**
- **Οι προϋπολογισμοί που αφορούν επενδύσεις στον κυβερνοχώρο το 2024 αυξάνονται με υψηλότερο ρυθμό σε σύγκριση με πέρυσι**
- **Η πλειονότητα των ερωτηθέντων (52%) απάντησε ότι αναμένει αύξηση των κυβερνοεπιθέσεων μέσα στον επόμενο χρόνο**
- **7 στους 10 (69%) συμμετέχοντες στην έρευνα δηλώνουν ότι ο Οργανισμός τους θα χρησιμοποιήσει εργαλεία που αξιοποιούν την Τεχνητή Νοημοσύνη για σκοπούς κυβερνοάμυνας τους επόμενους 12 μήνες**
- **Οι κυβερνοεπιθέσεις που αφορούν τον κλάδο της υγείας είναι κατά 25% πιο κοστοβόρες σε σχέση με άλλους κλάδους, καθώς η αξία τους ανέρχεται σε 5,3 εκατομμύρια δολάρια κατά μέσο όρο**

Σημαντική αύξηση στο ποσοστό των επιχειρήσεων που έπεσαν θύμα παραβίασης δεδομένων με κόστος άνω του 1 εκατομμυρίου δολαρίων κατέγραψε η έρευνα Global Digital Trust Insights της PwC, με το σχετικό ποσοστό να εκτινάσσεται σε 36% έναντι 27% έναν χρόνο νωρίτερα.

Σύμφωνα με την ίδια έρευνα που διεξήχθη μεταξύ 3.800 επικεφαλής επιχειρήσεων και κορυφαίων στελεχών τεχνολογίας σε 71 χώρες, οι εταιρείες αντιμετωπίζουν την άνοδο του Generative AI με ένα μείγμα σκεπτικισμού και ενθουσιασμού. Παράλληλα, πολλές επιχειρήσεις αυξάνουν σημαντικά τις επενδύσεις τους στην κυβερνοασφάλεια, προκειμένου να προστατευθούν από κυβερνοεπιθέσεις.

Σχεδόν τα δύο τρίτα (64%) των ερωτηθέντων δήλωσαν ότι αύξησαν τον τζίρο τους το περασμένο έτος, ενώ 8 στους 10 (82%) αναμένουν αύξηση αυτού το επόμενο έτος. Την ίδια στιγμή, 8 στους 10 (79%) αναμένουν αύξηση των επενδύσεων σε ψηφιακές δράσεις και εργαλεία, έναντι ποσοστού 65% το 2023. Ταυτόχρονα, οι οργανισμοί που επενδύουν σε στρατηγικούς μετασχηματισμούς κυβερνοασφάλειας παρά σε μεμονωμένες επενδύσεις, καταγράφουν σημαντικά οφέλη και αποτελούν αραιότερα θύματα κυβερνοεπιθέσεων. Αναφορικά με τις εταιρείες που έπεσαν θύματα κυβερνοεπίθεσης ύψους άνω του 1 εκατ. Ευρώ, αυτές σχεδιάζουν σε ποσοστό 88% να αυξήσουν τον προϋπολογισμό της κυβερνοασφάλειας, ενώ αντίστοιχα, οργανισμοί με κύκλο εργασιών άνω των 5 δισ. δολαρίων σχεδιάζουν αύξηση του σχετικού προϋπολογισμού σε ποσοστό 83%.

Υγεία, Τεχνολογία, Επικοινωνίες και Χρηματοπιστωτικές υπηρεσίες: οι κλάδοι που αντιμετωπίζουν τη μεγαλύτερη απειλή από κινδύνους στον κυβερνοχώρο

Μεταξύ των επιμέρους κλάδων, στην τριάδα εκείνων που έχουν πέσει θύματα παραβίασης δεδομένων βρίσκονται αυτός της υγείας, της τεχνολογίας, των ΜΜΕ και των τηλεπικοινωνιών καθώς και αυτός χρηματοπιστωτικών υπηρεσιών. Αντίστοιχα, σύμφωνα με την έρευνα, παρατηρείται σημαντική αύξηση των περιστατικών σε ετήσια βάση, ανεξαρτήτως κλάδου.

Με βάση τα ευρήματα, κατά το 2023 το μέσο κόστος μιας κυβερνοεπίθεσης παγκοσμίως ήταν 4,4 εκατ. δολάρια, ενώ ειδικά στον τομέα της υγείας το κόστος ήταν 25% υψηλότερο φτάνοντας τα 5,3 εκατ. δολάρια. Αντίστοιχα, σύμφωνα πάντα με την έρευνα, όσο αυξάνεται το μέγεθος της εταιρείας, αναλόγως αυξάνεται και το μέσο κόστος από τις κυβερνοεπιθέσεις. Εταιρείες με αξία μεγαλύτερη των 10 δισ. δολαρίων αναφέρουν ότι το σχετικό κόστος ανέρχεται σε 7,2 εκατ. δολάρια, ενώ εκείνες με αξία χαμηλότερη από 1 δισ. δολάρια αναφέρουν ζημιές 1,9 εκατ. δολαρίων κατά μέσο όρο.

Η άνοδος του «DefenseGPT»

Μεταξύ των κορυφαίων επιχειρήσεων, υπάρχει αυξανόμενη ανησυχία για την άνοδο του Generative AI (GenAI), καθώς σχετίζεται άμεσα με την ασφάλεια στον κυβερνοχώρο. Ένα άλλο κύμα απειλών στον κυβερνοχώρο μπορεί να προκύψει από το γεγονός ότι το GenAI μπορεί να συμβάλει στη δημιουργία μεγάλης κλίμακας προηγμένου τύπου επίθεσης, η οποία στοχεύει στα email των εταιρειών, αλλά και όσων επαφών διατηρούν στις βάσεις δεδομένων τους.

Οι Επικεφαλής Ψηφιακής Ασφάλειας (CISO) και οι Διευθυντές Πληροφορικής (CIO) θα πρέπει να λάβουν υπόψη τους την εκτίμηση του 52% των ερωτηθέντων ότι το GenAI θα μπορούσε να οδηγήσει σε καταστροφικές κυβερνοεπιθέσεις τους επόμενους 12 μήνες. Την ίδια στιγμή, σχεδόν 8 στους 10 (77%) συμφώνησαν ότι χρειάζεται να υιοθετηθούν πλαίσια για την ηθική και υπεύθυνη χρήση της νέας αυτής τεχνολογίας.

Συγχρόνως, σύμφωνα πάντα με την έρευνα, τα τρία τέταρτα των ερωτηθέντων σε κορυφαίες θέσεις επιχειρήσεων εξέφρασαν ενθουσιασμό για τις δυνατότητες του GenAI:

● Το 77% συμφώνησε ότι «το Generative AI θα βοηθήσει τον οργανισμό μας να αναπτύξει νέους επιχειρηματικούς τομείς εντός των επόμενων τριών ετών».

● Το 74% συμφώνησε ότι «η προσωπική χρήση του Generative AI από τους εργαζόμενους θα οδηγήσει σε απτές αυξήσεις στην παραγωγικότητά τους μέσα στους επόμενους 12 μήνες».

● Το 75% συμφώνησε πως «οι παραγωγικές διαδικασίες που βασίζονται στην τεχνητή νοημοσύνη σε έναν οργανισμό θα αυξήσουν την παραγωγικότητα των εργαζομένων μέσα στους επόμενους 12 μήνες».

Το GenAI μπορεί –χάρη στη σύνθεση μεγάλου όγκου δεδομένων από πολλαπλά συστήματα και πηγές- να υποστηρίξει οργανισμούς κατά τη διαχείριση περιστατικών, αναλύοντας ενδείξεις παραβίασης και ημερολόγια ασφάλειας. Επιπλέον, η τεχνολογία αυτή μπορεί να παρουσιάσει σύνθετες απειλές σε κατανοητή γλώσσα, να προτείνει στρατηγικές διαχείρισης σύνθετων απειλών, αλλά και να συμβάλλει σε σχετικές αναζητήσεις και έρευνες.

«Οι θεματοφύλακες της ψηφιακής εμπιστοσύνης»

Σύμφωνα με την έρευνα της PwC, απαιτούνται βελτιώσεις και συνέπεια στην κυβερνοασφάλεια. Λιγότερο από το ένα τρίτο των ερωτηθέντων αναφέρουν ότι εκτελούν σε τακτική βάση πρακτικές αιχμής στην κυβερνοασφάλεια.

Προκειμένου να διερευνηθεί περαιτέρω το παραπάνω, αναπτύχθηκε ένα μητρώο για να προσδιορίσει ποιοι οργανισμοί διαθέτουν ομάδες κυβερνοασφάλειας, οι οποίες επιδεικνύουν κορυφαίες πρακτικές σε σταθερή βάση. Με βάση δέκα (10) περιοχές βέλτιστων πρακτικών κυβερνοασφάλειας, μόλις το 5% των οργανισμών ανέφερε συνεπή εφαρμογή όλων, τους οποίους και αποκαλούμε «Θεματοφύλακες Ψηφιακής Εμπιστοσύνης».

Περισσότεροι από τους μισούς (53%) εξ αυτών έχουν έσοδα άνω των 5 δισ. δολαρίων και είναι περισσότερο πιθανό να είναι οργανισμοί με ταχείς ρυθμούς ανάπτυξης (άνω του 10%). Επιπλέον, είναι πιθανότερο για τους «Θεματοφύλακες Ψηφιακής Εμπιστοσύνης» τα κόστη των κυβερνοεπιθέσεων να είναι χαμηλότερα και να μην ξεπερνούν τα 100.000 δολάρια ανά περιστατικό. Τη στιγμή που για το 36% των υπολοίπων οργανισμών το κόστος τέτοιων περιστατικών ανέρχεται σε 1 εκατ. δολάρια, το ποσοστό αυτό μειώνεται στο 29% μεταξύ των «Θεματοφυλάκων Ψηφιακής Εμπιστοσύνης». Οι τελευταίοι είναι επίσης περισσότερο αισιόδοξοι σχετικά με τον πιθανό αντίκτυπο του Generative AI – πολλοί συμφωνούν ακράδαντα ότι θα αναπτύξει νέους επιχειρηματικούς τομείς (49% έναντι 33% συνολικά) και θα χρησιμοποιήσουν εργαλεία Generative AI για την άμυνα στον κυβερνοχώρο (44% έναντι 27%). Ακόμα, λιγότεροι από αυτούς φαίνεται να συμφωνούν με την εκτίμηση ότι «το GenAI θα οδηγήσει σε μια καταστροφική κυβερνοεπίθεση» (33% έναντι 22% συνολικά) ενώ είναι λιγότερο πιθανό να επιτρέψουν την ανάπτυξη των εργαλείων GenAI πριν εφαρμόσουν εσωτερικές πολιτικές (31% διαφωνούν έναντι 19% συνολικά και 53% συμφωνούν έναντι 63% συνολικά).

Οι επικεφαλής των επιχειρήσεων πολλαπλασιάζουν τις επενδύσεις στην κυβερνοασφάλεια

Παρά τη συνεχιζόμενη αύξηση των φυσικών καταστροφών που σχετίζονται με την κλιματική αλλαγή, τις επιπτώσεις της πανδημίας και την αυξανόμενη ανισότητα, οι ηγέτες των επιχειρήσεων κατέταξαν την ψηφιακή τεχνολογία ως τον κορυφαίο κίνδυνο τον οποίο καλούνται να μετριάσουν τους επόμενους 12 μήνες.

Συγκεκριμένα, οι τρεις κορυφαίες απειλές που σχετίζονται με τον κυβερνοχώρο είναι:

- απειλές σχετικές με το cloud,
- επιθέσεις σε συνδεδεμένες συσκευές IoT και

- λειτουργίες hack-and-leak.

Παρόλα αυτά, περισσότερες από το ένα τρίτο των εταιρειών δεν έχουν κάνει προσπάθειες διαχείρισης κινδύνου και μόνο μία στις τέσσερις έχει προβεί σε επενδύσεις προκειμένου να βελτιώσει την ανθεκτικότητά της στον κυβερνοχώρο.

Αναλυτικά, μόνο το 2% των οργανισμών βελτιώνονται συνεχώς σε όλους τους τομείς που σχετίζονται με την εξασφάλιση ανθεκτικότητας στον κυβερνοχώρο. Αντίστοιχα, περισσότερο από το 40% των ηγετών δήλωσε ότι δεν κατανοεί τους κινδύνους στον κυβερνοχώρο που ενέχουν οι αναδυόμενες τεχνολογίες, όπως εργαλεία εικονικού περιβάλλοντος, Generative AI, Enterprise Blockchain, Quantum Computing και Virtual Reality/Augmented Reality.

Παραλληλα, οι οργανισμοί καλούνται να υιοθετήσουν μια εργαλειοθήκη Υπεύθυνης Τεχνητής Νοημοσύνης που θα καθοδηγεί την αξιόπιστη και ηθική χρήση της. Αν και συχνά θεωρείται ως αμιγώς τεχνολογική λειτουργία, η ανθρώπινη επίβλεψη και παρέμβαση είναι απαραίτητες για την Τεχνητή Νοημοσύνη. Και μαζί με τους κινδύνους ασφάλειας και ιδιωτικότητας, πρέπει τώρα να ληφθούν υπόψη πρόσθετοι τομείς που περιλαμβάνουν κινδύνους δεδομένων, μεροληψίας, και χρήσης.

Αναβάθμιση δεξιοτήτων και επανεκπαίδευση

Σύμφωνα με την έρευνα, οι οργανισμοί θα πρέπει να επανεξετάσουν τις στρατηγικές απόκτησης και διατήρησης ταλέντων στην προσπάθειά τους να διατηρήσουν το εργατικό δυναμικό τους αφοσιωμένο και ενημερωμένο. Οι συμμετέχοντες στην έρευνα ανέφεραν ότι οι τρεις βασικές τους προτεραιότητες είναι:

- η αναβάθμιση και τεχνική κατάρτιση του τρέχοντος εργατικού δυναμικού αρκετά γρήγορα ώστε να συμβαδίζει με τις απαιτήσεις του οργανισμού,
- η επανεξισορρόπηση μεταξύ υπηρεσιών που διαχειρίζονται εσωτερικά και εξωτερικά και
- ο προσδιορισμός των κατάλληλων υποψηφίων για κάλυψη νέων θέσεων εργασίας.

Ειδικά σε περιπτώσεις οργανισμών που έχουν πέσει θύμα κυβερνοεπίθεσης με κόστος άνω του 1 εκατ. δολαρίων, είναι πιθανό να ταξινομήσουν τον ανταγωνισμό για προσέλκυση ταλέντου από την αγορά εργασίας ανάμεσα στις τρεις πρώτες προτεραιότητές τους.

Σχετικά με την έκθεση

Η έρευνα Digital Trust Insights 2024 κατέγραψε τις απόψεις των επικεφαλής επιχειρήσεων σε όλο τον κόσμο σχετικά με τις προκλήσεις και τις ευκαιρίες βελτίωσης και μετατροπής της κυβερνοασφάλειας στον οργανισμό τους, τους επόμενους 12 έως 18 μήνες. Η έρευνα βασίζεται σε 3.876 απαντήσεις από 71 περιοχές το διάστημα Μαΐου έως Ιουλίου 2023. Οι απαντήσεις στην έρευνα προέρχονται από διάφορους κλάδους και μεγέθη οργανισμών, με το 40% να προέρχεται από οργανισμούς με αξία άνω των 5 δις. δολαρίων. Το 88% των απαντήσεων (3.428) προέρχονται από εξωτερικό πάροχο πάνελ και το 12% (448) είναι η προσέγγιση του δικτύου της PwC.

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 152 χώρες με περισσότερα από 328.000 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.