Στο 22% οι κυβερνοεπιθέσεις στις κατασκευές λόγω έλλειψης προϋπολογισμού, στο 4% σε μεταφορές & logistics

2023/12/05 14:34 στην κατηγορία LOGISTICS

Σύμφωνα με πρόσφατη έρευνα της Kaspersky, το 14% των εταιρειών στην Ευρώπη έχει βιώσει περιστατικά στον κυβερνοχώρο λόγω ανεπαρκών επενδύσεων στον τομέα τα τελευταία δύο χρόνια.

Ανησυχητικό είναι το γεγονός ότι, ο κατασκευαστικός κλάδος ήρθε αντιμέτωπος με τον μεγαλύτερο αριθμό περιστατικών στον κυβερνοχώρο λόγω ακατάλληλης κατανομής του προϋπολογισμού **(22%).**

Όσον αφορά τα οικονομικά τους, το 22% των εταιρειών στην Ευρώπη παραδέχεται ότι δεν διαθέτει τον προϋπολογισμό για επαρκή μέτρα ασφάλειας στον κυβερνοχώρο.

Η Kaspersky πραγματοποίησε έρευνα[1] για να ανακαλύψει τις απόψεις των επαγγελματιών IT Security που εργάζονται για μικρομεσαίες επιχειρήσεις παγκοσμίως σχετικά με τον ανθρώπινο αντίκτυπο στην ψηφιακή ασφάλεια μιας εταιρείας.

Η έρευνα – με στόχο τη συλλογή πληροφοριών σχετικά με διάφορες ομάδες ανθρώπων που επηρεάζουν την ασφάλεια στον κυβερνοχώρο – εξέτασε τόσο το προσωπικό στο εσωτερικό της εταιρείας όσο και τους εξωτερικούς συνεργάτες.

Ανέλυσε επίσης τον αντίκτυπο που έχουν οι υπεύθυνοι λήψης αποφάσεων στην ασφάλεια στον κυβερνοχώρο όσον αφορά την κατανομή του προϋπολογισμού.

Η ανεπαρκής κατανομή του προϋπολογισμού για την ασφάλεια στον κυβερνοχώρο οδήγησε το 14% των εταιρειών στην Ευρώπη να υποστεί περιστατικά στον κυβερνοχώρο τα τελευταία δύο χρόνια. Η κατάσταση είναι διαφορετική για κάθε κλάδο.

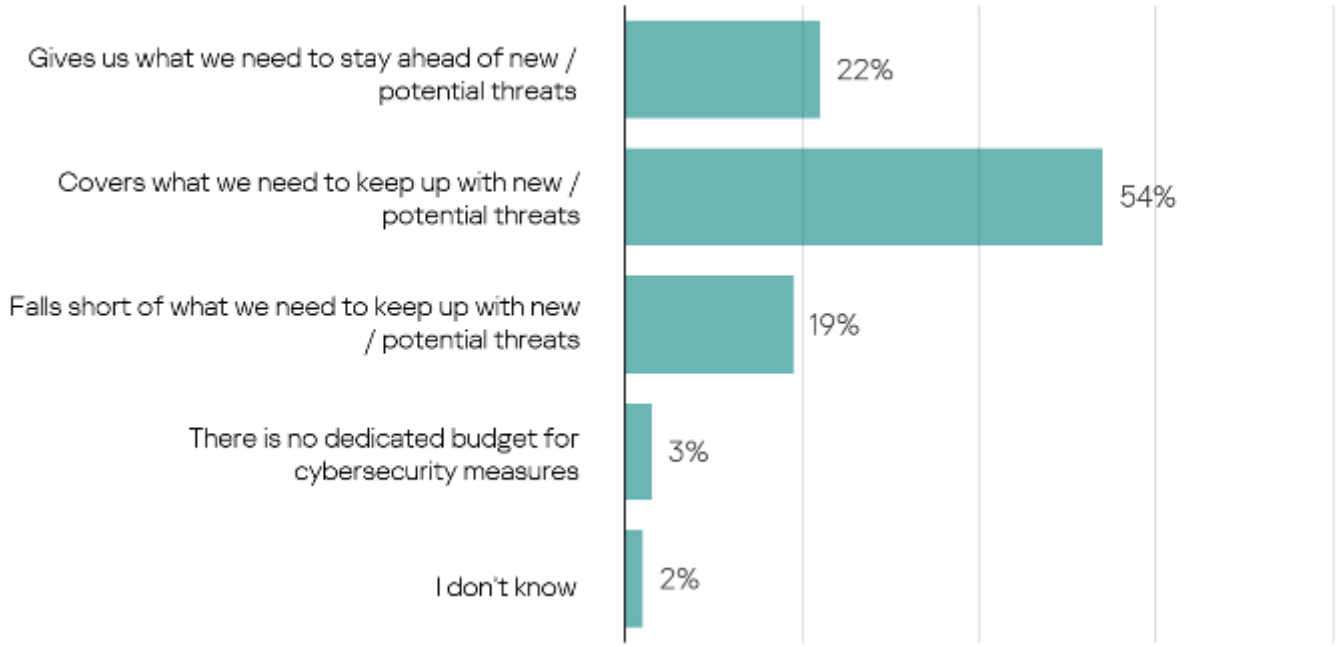
Ενώ ο κατασκευαστικός κλάδος αντιμετώπισε τον μεγαλύτερο αριθμό παραβιάσεων στον κυβερνοχώρο λόγω έλλειψης προϋπολογισμού (22%), ορισμένες βιομηχανίες εμφάνισαν μικρότερο αριθμό περιστατικών στον κυβερνοχώρο από το ποσοστό της περιοχής (14%): χρηματοπιστωτικές υπηρεσίες (10%), τηλεπικοινωνίες (7%) και **μεταφορές & logistics (4%).**

Όταν ρωτήθηκαν σχετικά με τον προϋπολογισμό για τα μέτρα ασφάλειας στον κυβερνοχώρο, σχεδόν 8 στους δέκα (76%) ερωτηθέντες στην Ευρώπη δήλωσαν ότι είναι εξοπλισμένοι για να συμβαδίσουν ή ακόμη και να παραμείνουν μπροστά από νέες απειλές.

Ωστόσο, το 22% των εταιρειών δεν τα πάνε τόσο καλά – το 19% αναφέρει ότι δεν διαθέτει επαρκή κεφάλαια για να προστατεύσει σωστά την υποδομή της εταιρείας.

Ταυτόχρονα, εξακολουθούν να υπάρχουν εταιρείες χωρίς κατανομή κόστους για την ασφάλεια στον κυβερνοχώρο – το 3% ισχυρίστηκε ότι δεν διαθέτει ειδικό προϋπολογισμό για τις ανάγκες προστασίας στον κυβερνοχώρο.

Ο πιο επιτυχημένος κλάδος όσον αφορά τη σωστή κατανομή χρημάτων για την ασφάλεια στον κυβερνοχώρο είναι οι χρηματοπιστωτικές υπηρεσίες – το 96% των ερωτηθέντων που εργάζονται σε αυτόν τον τομέα ισχυρίζονται ότι οι οργανισμοί τους είναι έτοιμοι να συμβαδίσουν και να παραμείνουν μπροστά από όλες τις νέες απειλές.



Θα λέγατε ότι ο προϋπολογισμός για μέτρα ασφάλειας στον κυβερνοχώρο στην εταιρεί σας…;

Πολλές εταιρείες είναι πρόθυμες να λάβουν μέτρα για την ενίσχυση της κυβερνοασφάλειάς τους τα επόμενα 1-1,5 χρόνια.

Ένας από τους πιο δημοφιλείς τομείς επενδύσεων είναι το λογισμικό ανίχνευσης απειλών (36%) και η εκπαίδευση, όπου το 31% των εταιρειών σχεδιάζει να διαθέσει προϋπολογισμούς για εκπαιδευτικά προγράμματα για επαγγελματίες στον τομέα της ασφάλειας στον κυβερνοχώρο και το 33% για την εκπαίδευση γενικού προσωπικού.

Άλλα δημοφιλή μέτρα που σχεδιάζουν να λάβουν σύντομα οι οργανισμοί είναι η εισαγωγή λογισμικού προστασίας τερματικού σημείου (33%), η πρόσληψη επιπλέον επαγγελματιών IT (29%) και η υιοθέτηση λύσεων cloud SaaS (27%).

«Σήμερα, οι εταιρείες πρέπει να ευθυγραμμίσουν τις επενδύσεις στον κυβερνοχώρο με μια επιχειρηματική στρατηγική και να θεωρήσουν την ασφάλεια στον κυβερνοχώρο ως έναν από τους επιχειρηματικούς τους στόχους. Φυσικά, οι επενδύσεις πρέπει να δικαιολογούνται και να είναι αποτελεσματικές, οπότε το τμήμα ασφάλειας πληροφοριών αντιμετωπίζει επίσης το καθήκον της αύξησης της απόδοσης των επενδύσεων στην ασφάλεια των πληροφοριών και της υπεράσπισης των επενδύσεων στην ανώτερη διοίκηση ή στο διοικητικό συμβούλιο. Επίσης, εκτός από τη μείωση του MTTD και του MTTR, η ασφάλεια των πληροφοριών είναι επιφορτισμένη με τη μείωση του κόστους ενός περιστατικού ασφαλείας. Αυτές οι προκλήσεις μπορούν να αντιμετωπιστούν με τη χρήση διαφόρων σύγχρονων προσεγγίσεων και τεχνολογιών. Για παράδειγμα, επενδύουμε στην ανάπτυξη του χαρτοφυλακίου SASE καθώς και XDR και MDR με ενσωματωμένα TN, μηχανική μάθηση, αυτοματοποιημένη ανίχνευση και απόκριση, αυτοματοποιημένη διερεύνηση απειλών, out of the box ενσωματώσεις και πολλά άλλα. Για να διασφαλίσουμε τη διαφάνεια των διαδικασιών και να αποδείξουμε την αξία των λύσεών μας, παρέχουμε επίσης πίνακες εργαλείων CISO και C-level αναφορές, οι οποίοι περιλαμβάνουν πληροφορίες σχετικά με τον αριθμό των περιστατικών που αποτρέψαμε, πόσο γρήγορα διερευνήθηκαν τα περιστατικά και την αποτελεσματικότητα των λύσεων ασφάλειας στον κυβερνοχώρο που αναπτύχθηκαν. Επισημαίνουμε επίσης τους κινδύνους που αφορούν συγκεκριμένους πελάτες και τους δείχνουμε τάσεις ειδικά για τον κλάδο για να τους βοηθήσουμε να διαμορφώσουν την ασφάλεια στον κυβερνοχώρο τους, στοχεύοντας τις άμυνές τους γύρω από τους τρέχοντες κινδύνους και δικαιολογώντας τις επενδύσεις στην απαραίτητη τεχνολογία», σχολίασε ο Ivan Vassunov, VP, Corporate Products της Kaspersky.

[1] *Η έρευνα διεξήχθη σε 19 χώρες: Βραζιλία, Χιλή, Κίνα, Κολομβία, Γαλλία, Γερμανία, Ινδία, Ινδονησία, Ιαπωνία, Καζακστάν, Μεξικό, Ρωσία, Σαουδική Αραβία, Νότια Αφρική, Ισπανία, Τουρκία, Ηνωμένα Αραβικά Εμιράτα, Ηνωμένο Βασίλειο και ΗΠΑ.*

Η πλήρης έκθεση και περισσότερες πληροφορίες σχετικά με τον ανθρώπινο αντίκτυπο στην ασφάλεια στον κυβερνοχώρο στις επιχειρήσεις βρίσκονται εδώ.