Kaspersky:Το 80% των Υπεύθυνων Ασφάλειας Πληροφοριών στην Ευρώπη θεωρούν ότι οι παραβιάσεις είναι αναπόφευκτες

Το 80% των Υπεύθυνων Ασφάλειας Πληροφοριών στην Ευρώπη θεωρούν ότι οι παραβιάσεις είναι αναπόφευκτες, αλλά πάρα πολλοί είναι «κολλημένοι» σε έναν φαύλο κύκλο κινδύνου

Οι υπεύθυνοι του τομέα της πληροφορικής στις επιχειρήσεις παγκοσμίως έχουν βρεθεί σε αδιέξοδο αναφορικά με την καταπολέμηση του ψηφιακού εγκλήματος. Δεν έχουν επιρροή στα ανώτερα ηγετικά στελέχη και δυσκολεύονται να δικαιολογήσουν τους προϋπολογισμούς που χρειάζονται, καθιστώντας, αναπόφευκτα, τις επιχειρήσεις στις οποίες εργάζονται πιο ευάλωτες. Το φαινόμενο αυτό είναι ένα από τα ευρήματα μιας νέας έκθεσης της Kaspersky Lab, η οποία διαπίστωσε ότι το 80% των Υπεύθυνων Ασφάλειας Πληροφοριών (CISOs) στην Ευρώπη θεωρούν ότι οι παραβιάσεις της ψηφιακής ασφάλειας είναι αναπόφευκτες, ενώ κατά κύριο λόγο ανησυχούν για τις ομάδες εγκληματιών με οικονομικό κίνητρο.

Από το cloud στους κακόβουλους εισβολείς: η επιφάνεια επιθέσεων διευρύνεται στις σύγχρονες επιχειρήσεις

Η άνοδος των ψηφιακών απειλών, σε συνδυασμό με τον ψηφιακό μετασχηματισμό που πολλές εταιρείες πραγματοποιούν επί του

παρόντος, καθιστά τον ρόλο του CISO όλο και πιο σημαντικό στη σύγχρονη επιχείρηση. Η Kaspersky Lab αναφέρει ότι η πίεση που δέχονται οι CISOs είναι τώρα μεγαλύτερη από ποτέ: το 57% θεωρεί ότι οι πολύπλοκες υποδομές που περιλαμβάνουν το cloud και η φορητότητα αποτελούν κορυφαία πρόκληση και το 50% ανησυχεί για τη συνεχιζόμενη αύξηση των ψηφιακών επιθέσεων.

Οι CISOs πιστεύουν ότι οι εγκληματικές συμμορίες με οικονομικό κίνητρο (40%) και οι κακόβουλες επιθέσεις (29%) είναι οι μεγαλύτεροι κίνδυνοι για τις επιχειρήσεις τους και αυτές είναι οι απειλές που είναι εξαιρετικά δύσκολο να αποφευχθούν: είτε επειδή εκκινούνται από «επαγγελματίες» είτε επειδή υποβοηθούνται από υπαλλήλους.

Οι προκλήσεις αιτιολόγησης του προϋπολογισμού αφήνουν τους CISOs να ανταγωνίζονται με άλλα τμήματα της εταιρείας

Οι προϋπολογισμοί που διατίθενται για την ψηφιακή ασφάλεια αναφέρθηκε ότι αυξάνονται. Περίπου οι μισοί (49%) CISOs αναμένουν ότι οι προϋπολογισμοί τους θα αυξηθούν στο μέλλον και το 49% των ερωτηθέντων αναμένει ότι οι προϋπολογισμοί θα παραμείνουν οι ίδιοι.

Ωστόσο, οι CISOs αντιμετωπίζουν σημαντικές προκλήσεις με τον προϋπολογισμό, επειδή είναι σχεδόν αδύνατο για αυτούς να προσφέρουν σαφή απόδοση επένδυσης (ROI) ή 100% προστασία ενάντια στις ψηφιακές επιθέσεις.

Για παράδειγμα, το 36% των CISOs δηλώνουν ότι δεν μπορούν να εξασφαλίσουν τους προϋπολογισμούς για την ασφάλεια στον τομέα της πληροφορικής, επειδή δεν μπορούν να εγγυηθούν ότι θα υπάρξει παραβίαση. Και όταν οι προϋπολογισμοί ασφάλειας θεωρούνται από μια επιχείρηση, ως μέρος των συνολικών δαπανών πληροφορικής, οι CISOs βρίσκονται αντιμέτωποι με άλλα τμήματα προκειμένου να εξασφαλίσουν τον απαραίτητο προϋπολογισμό. Ο δεύτερος πιο πιθανός λόγος για να μην λάβουν τον απαραίτητο προϋπολογισμό είναι ότι η ασφάλεια είναι μερικές φορές μέρος των συνολικών δαπανών πληροφορικής. Επιπλέον, ένας στους τρεις

CISOs (33%) δήλωσε ότι ο προϋπολογισμός θα μπορούσε να διατεθεί για ψηφιακά, cloud ή άλλα έργα πληροφορικής αντ' αυτού – τα οποία μπορεί να είναι σε θέση να αποδείξουν μια σαφέστερη ROI.

Οι CISOs χρειάζονται κοινό σε επίπεδο διοικητικού συμβουλίου, καθώς ο ψηφιακός μετασχηματισμός θα τεθεί σε ισχύ

Οι ψηφιακές επιθέσεις μπορούν να έχουν δραστικές συνέπειες για τις επιχειρήσεις: περισσότεροι από ένας στους τρεις ερωτηθέντες στην έρευνα της Kaspersky Lab αναγνώρισε τις ζημιές στη φήμη (28%) και τις οικονομικές (25%) ως τις πιο κρίσιμες συνέπειες μιας ψηφιακής επίθεσης.

Ωστόσο, παρά τον αρνητικό αντίκτυπο μιας ψηφιακής επίθεσης, μόνο το 26% των υπεύθυνων ασφάλειας του τομέα της πληροφορικής που συμμετείχαν στην έρευνα είναι μέλη του διοικητικού συμβουλίου στις αντίστοιχες επιχειρήσεις. Από εκείνους που δεν είναι μέλη του διοικητικού συμβουλίου, ένας στους τέσσερις (25%) πιστεύει ότι θα έπρεπε να είναι.

Η πλειονότητα των υπευθύνων της ασφάλειας πληροφορικής (58%) πιστεύει ότι εμπλέκονται επαρκώς στη λήψη επιχειρηματικών αποφάσεων τη δεδομένη στιγμή. Ωστόσο, καθώς ο ψηφιακός μετασχηματισμός καθίσταται καθοριστικός για τη στρατηγική κατεύθυνση των μεγάλων επιχειρήσεων, το ίδιο θα πρέπει να ισχύει και για την ψηφιακή ασφάλεια. Ο ρόλος του CISO πρέπει να αναπτυχθεί ώστε να αντικατοπτρίζει αυτές τις αλλαγές, δίνοντάς τους τη δυνατότητα να επηρεάζουν τις αποφάσεις.

Ο Maxim Frolov, VP Global Sales, στην Kaspersky Lab, δήλωσε: «*Ιστορικά, οι προϋπολογισμοί για την ψηφιακή ασφάλεια θεωρήθηκαν ως δαπάνες χαμηλής προτεραιότητας, αλλά αυτό δεν ισχύει πλέον. Η επιφάνεια των επιθέσεων ενάντια στις σύγχρονες επιχειρήσεις αυξάνεται, όπως και η συχνότητα και ο αντίκτυπος των ψηφιακών επιθέσεων και το κόστος των περιστατικών στον κυβερνοχώρο. Το αποτέλεσμα είναι ότι όλο και περισσότερα ανώτατα στελέχη αντιμετωπίζουν πλέον την ασφάλεια πληροφορικής*

ως επένδυση».

Και συνέχισε: «*Σήμερα, οι κίνδυνοι για την ασφάλεια στον κυβερνοχώρο βρίσκονται στην κορυφή της ατζέντας των Διευθύνοντων Συμβούλων, των CFOs και των Risk Officers. Στην πραγματικότητα, ο προϋπολογισμός για τον κυβερνοχώρο δεν είναι απλώς ένας τρόπος πρόληψης των παραβιάσεων και των καταστροφικών κινδύνων που συνδέονται με αυτούς – είναι ένας τρόπος για να προστατεύσουμε τη συνέχεια της επιχείρησης, καθώς και τις βασικές επενδύσεις μιας εταιρείας*».

Εδώ μπορείτε να βρείτε την πλήρη έκθεση.