άρθρο

CROMAR

Ανθεκτικότητα στον κυβερνοχώρο και ο ρόλος του διοικητικού συμβουλίου

Νίκος Γεωργόπουλος
Digital Risks Insurance Broker, Cromar Insurance Brokers

Στον ταχέως εξελισσόμενο ψηφιακό κόσμο, η ανθεκτικότητα στον κυβερνοχώρο (cyber resilience) έχει αναδειχθεί σε κρίσιμο ζήτημα για τα διοικητικά συμβούλια. Η αυξανόμενη συχνότητα και η πολυπλοκότητα των απειλών στον κυβερνοχώρο καθιστούν αναγκαία την υιοθέτηση στρατηγικής κυβερνοασφάλειας για κάθε εταιρεία. Για τα μέλη του διοικητικού συμβουλίου η κατανόηση και η εποπτεία της ανθεκτικότητας στον κυβερνοχώρο δεν είναι απλώς μια τεχνική αναγκαιότητα, αλλά μια θεμελιώδης πτυχή της εταιρικής διακυβέρνησης, που επηρεάζει τη φήμη, την οικονομική υγεία, τη λειτουργική συνέχεια της εταιρείας και ενισχύει τη θέση της στην αγορά, αυξάνοντας την αποτίμησή της και τα κέρδη των μετόχων.

Κατανόηση της ανθεκτικότητας στον κυβερνοχώρο

Η ανθεκτικότητα στον κυβερνοχώρο αναφέρεται στην ικανότητα μιας εταιρείας να προετοιμάζεται, να ανταποκρίνεται και να ανακάμπτει μετά από περιστατικά παραβίασης ασφάλειας. Σε αντίθεση με την παραδοσιακή ασφάλεια στον κυβερνοχώρο, η οποία επικεντρώνεται κυρίως στην πρόληψη επιθέσεων, η ανθεκτικότητα στον κυβερνοχώρο περιλαμβάνει ένα ευρύτερο πεδίο εφαρμογής, συμπεριλαμβανομένης της ικανότητας διατήρησης των βασικών λειτουργιών κατά τη διάρκεια και μετά από ένα περιστατικό παραβίασης ασφάλειας. Αυτή η προσέγγιση διασφαλίζει ότι η εταιρεία μπορεί να αντέξει και να ανακάμψει γρήγορα από περιστατικά παραβίασης ασφάλειας, ελαχιστοποιώντας τον αντίκτυπο στις επιχειρηματικές της λειτουργίες.

Ο ρόλος του διοικητικού συμβουλίου

Το διοικητικό συμβούλιο διαδραματίζει καθοριστικό ρόλο στη διαμόρφωση της στρατηγικής ανθεκτικότητας μιας εταιρείας στον κυβερνοχώρο. Οι αρμοδιότητές του περιλαμβάνουν:

- **Εποπτεία των κινδύνων:** Το διοικητικό συμβούλιο πρέπει να διασφαλίζει ότι οι κίνδυνοι στον κυβερνοχώρο εντοπίζονται, αξιολογούνται και αντιμετωπίζονται αποτελεσματικά. Αυτό περιλαμβάνει την κατανόηση των κινδύνων

που απειλούν την εταιρεία, συμπεριλαμβανομένων των πιθανών απειλών, των τρωτών σημείων και των επιπτώσεων των περιστατικών παραβίασης ασφάλειας στις επιχειρηματικές λειτουργίες.

- **Στρατηγική ενσωμάτωση:** Η ανθεκτικότητα στον κυβερνοχώρο πρέπει να ενσωματωθεί στη συνολική επιχειρηματική στρατηγική. Το διοικητικό συμβούλιο θα πρέπει να αντιμετωπίζει την ασφάλεια στον κυβερνοχώρο ως στρατηγικό περιουσιακό στοιχείο, που μπορεί να προσφέρει ανταγωνιστικό πλεονέκτημα. Αυτό απαιτεί την ευθυγράμμιση των πρωτοβουλιών για την ασφάλεια στον κυβερνοχώρο με τους επιχειρηματικούς στόχους και τη διασφάλιση ότι η ανθεκτικότητα στον κυβερνοχώρο λαμβάνεται υπόψη σε όλες τις στρατηγικές αποφάσεις.

- **Κατανομή πόρων:** Πρέπει να διατίθενται επαρκείς πόροι για επενδύσεις στην κυβερνοασφάλεια. Το διοικητικό συμβούλιο θα πρέπει να διασφαλίζει ότι η εταιρεία επενδύει σε τεχνολογίες ασφάλειας, εξειδικευμένο προσωπικό και προγράμματα συνεχούς κατάρτισης. Η επένδυση αυτή είναι ζωτικής σημασίας για την οικοδόμηση ενός ισχυρού πλαισίου ανθεκτικότητας στον κυβερνοχώρο.

- **Κανονιστική συμμόρφωση:** Το διοικητικό συμβούλιο πρέπει να διασφαλίζει ότι η εταιρεία συμμορφώνεται με τους σχετικούς κανονισμούς (GDPR, NIS2, DORA κ.ά.) και τα πρότυπα κυβερνοασφάλειας. Αυτό περιλαμβάνει τη συνεχή ενημέρωση για τις εξελισσόμενες κανονιστικές απαιτήσεις και την εφαρμογή των απαραίτητων μέτρων για την εκπλήρωση των υποχρεώσεων συμμόρφωσης.

- **Ασφάλιση κινδύνων:** Το διοικητικό συμβούλιο πρέπει να διασφαλίζει ότι η εταιρεία έχει προβεί στη μεταφορά των κινδύνων που απομένουν σε ασφαλιστικές εταιρείες για την οικονομική προστασία της εταιρείας, την ομαλή συνέχιση των εταιρικών εργασιών μετά από ένα περιστατικό παραβίασης ασφάλειας και την προστασία των μετόχων.

Οικοδόμηση μιας εταιρείας ανθεκτικής στον κυβερνοχώρο

Για την οικοδόμηση μιας εταιρείας ανθεκτικής στον κυβερνοχώρο το διοικητικό συμβούλιο θα πρέπει να επικεντρωθεί στους παρακάτω βασικούς τομείς:

- **Δημιουργία κουλτούρας κυβερνοασφάλειας:** Η καλλιέργεια μιας κουλτούρας ευαισθητοποίησης σε θέματα κυβερνοασφάλειας είναι απαραίτητη. Το διοικητικό συμβούλιο θα πρέπει να προωθήσει την ευαισθητοποίηση σε θέματα κυβερνοασφάλειας σε όλα τα επίπεδα του οργανισμού, διασφαλίζοντας ότι οι εργαζόμενοι κατανοούν τον ρόλο τους στη διατήρηση της ανθεκτικότητας στον κυβερνοχώρο. Τα προγράμματα τακτικής εκπαίδευσης και ευαισθητοποίησης μπορούν να συμβάλουν στην ενσωμάτωση των πρακτικών ασφαλείας στην εταιρική κουλτούρα.

- **Συνεργασία και επικοινωνία:** Για να επιτευχθεί η ανθεκτικότητα στον κυβερνοχώρο απαιτείται σωστή επικοινωνία και συνεργασία σε ολό-

κληρο τον οργανισμό. Το διοικητικό συμβούλιο θα πρέπει να διευκολύνει την ανοικτή επικοινωνία μεταξύ του τμήματος πληροφορικής, της ομάδας κυβερνοασφάλειας και των άλλων επιχειρηματικών μονάδων. Αυτή η συνεργατική προσέγγιση διασφαλίζει ότι οι εκτιμήσεις για την ασφάλεια στον κυβερνοχώρο ενσωματώνονται σε όλες τις επιχειρηματικές διαδικασίες και αποφάσεις.

- **Πλάνο αντιμετώπισης περιστατικών:** Ο προληπτικός σχεδιασμός αντιμετώπισης περιστατικών είναι ζωτικής σημασίας για την ελαχιστοποίηση των επιπτώσεων των περιστατικών παραβίασης ασφάλειας. Το διοικητικό συμβούλιο θα πρέπει να διασφαλίζει ότι η εταιρεία διαθέτει ένα ολοκληρωμένο σχέδιο αντιμετώπισης περιστατικών, το οποίο περιλαμβάνει σαφείς ρόλους και αρμοδιότητες, πρωτόκολλα επικοινωνίας και διαδικασίες για τον περιορισμό και τον μετριασμό των επιπτώσεων περιστατικών παραβίασης ασφάλειας. Η τακτική διεξαγωγή ασκήσεων και προσομοιώσεων μπορεί να βοηθήσει στη δοκιμή και την τελειοποίηση του σχεδίου αντιμετώπισης περιστατικών.

- **Συνεχής βελτίωση:** Η ανθεκτικότητα στον κυβερνοχώρο είναι μια συνεχής διαδικασία, που απαιτεί συνεχή βελτίωση. Το διοικητικό συμβούλιο θα πρέπει να φροντίζει για την τακτική αξιολόγηση των κινδύνων, τη διαχείριση τρωτών σημείων και των ελέγχων ασφαλείας. Με τη συνεχή παρακολούθηση και βελτίωση της κατάστασης της κυβερνοασφάλειας της εταιρείας, το διοικητικό συμβούλιο μπορεί να διασφαλίσει ότι η εταιρεία παραμένει ανθεκτική.

Ο προληπτικός σχεδιασμός αντιμετώπισης περιστατικών είναι ζωτικής σημασίας για την ελαχιστοποίηση των επιπτώσεων των περιστατικών παραβίασης ασφάλειας. Το διοικητικό συμβούλιο θα πρέπει να διασφαλίζει ότι η εταιρεία διαθέτει ένα ολοκληρωμένο σχέδιο αντιμετώπισης περιστατικών.

Απαραίτητες οι γνώσεις κυβερνοασφάλειας στα μέλη του διοικητικού συμβουλίου

Η γνώση και η εμπειρία των μελών του διοικητικού συμβουλίου στον τομέα της κυβερνοασφάλειας, η συμμετοχή εξειδικευμένων στην κυβερνοασφάλεια μελών του ή εξειδικευμένων συμβούλων μπορούν να προσφέρουν πολύτιμες γνώσεις και καθοδήγηση. Οι σύμβουλοι κυβερνοασφάλειας μπορούν να βοηθήσουν τα μέλη του διοικητικού συμβουλίου να κατανοήσουν πολύπλοκα τεχνικά ζητήματα, να αξιολογήσουν την αποτελεσματικότητα των μέτρων κυβερνοασφάλειας και να λάβουν τεκμηριωμένες αποφάσεις σχετικά με τις στρατηγικές ανθεκτικότητας στον κυβερνοχώρο. Επιπλέον, το διοικητικό συμβούλιο θα πρέπει να προχωρήσει στη σύσταση ειδικής επιτροπής κυβερνοασφάλειας για την εποπτεία των ενεργειών που αφορούν την ανθεκτικότητα στον κυβερνοχώρο και τη διασφάλιση ότι η κυβερνοασφάλεια παραμένει κορυφαία προτεραιότητα.

Η ασφάλιση cyber insurance αυξάνει την ανθεκτικότητα των εταιρειών

Η ασφάλιση cyber insurance προσφέρει οικονομική προστασία και υπηρεσίες διαχείρισης περιστατικών παραβίασης ασφάλειας, μειώνοντας σημαντικά τον αντίκτυπο μιας επίθεσης και επιταχύνοντας την ανάκαμψη. Η συγκεκριμένη ασφάλιση καλύπτει, συνήθως, το κόστος που συνδέεται με περιστατικά παραβίασης ασφάλειας, απώλειας δεδομένων, επιθέσεων ransomware, μεταφοράς χρημάτων μετά από παραπλάνηση και άλλα περιστατικά στον κυβερνοχώρο.
Η ασφάλιση στον κυβερνοχώρο μπορεί να λειτουργήσει ως καταλύτης για τη βελτίωση της ανθεκτικότητας στον κυβερνοχώρο. Οι ασφαλιστές απαιτούν από τους αντισυμβαλλόμενους να πληρούν συγκεκριμένα πρότυπα κυβερνοασφάλειας ως προϋπόθεση για να παρέχουν ασφαλιστική κάλυψη. Αυτό αναγκάζει τους οργανισμούς να υιοθετούν βέλτιστες πρακτικές (χρήση MFA for remote access, εκπαίδευση του ανθρώπινου δυναμικού, τεσταρισμένες διαδικασίες ανάκτησης δεδομένων κ.ά.), να διενεργούν τακτικούς ελέγχους ασφαλείας και να διατηρούν ενημερωμένα σχέδια αντιμετώπισης περιστατικών.

Η επένδυση στην κυβερνοασφάλεια προστατεύει την αποτίμηση του οργανισμού και την κερδοφορία των μετόχων

Η ανθεκτικότητα στον κυβερνοχώρο αποτελεί μια κρίσιμη πτυχή της σύγχρονης εταιρικής διακυβέρνησης. Καθώς οι απειλές στον κυβερνοχώρο συνεχίζουν να εξελίσσονται, τα διοικητικά συμβούλια πρέπει να υιοθετούν μια στρατηγική προσέγγιση της ασφάλειας στον κυβερνοχώρο η οποία επικεντρώνεται στην πρόληψη. Με την κατανόηση των κινδύνων, την ενσωμάτωση της ανθεκτικότητας στον κυβερνοχώρο στην επιχειρηματική στρατηγική, την καλλιέργεια κουλτούρας ασφάλειας και τη διασφάλιση της συνεχούς βελτίωσης, τα διοικητικά συμβούλια μπορούν να συμβάλουν στην προστασία των οργανισμών τους από την απειλή περιστατικών παραβίασης ασφάλειας. Με τον τρόπο αυτό όχι μόνο προστατεύουν τα περιουσιακά στοιχεία και τη φήμη του οργανισμού, αλλά και ενισχύουν τη θέση του στην αγορά, αυξάνοντας την αποτίμησή του και τα κέρδη των μετόχων.