Παρακολούθηση Ηλεκτρονικών & Διαδικτυακών Κινδύνων

Βασικές αρχές και πρακτική καθοδήγηση για τα Διοικητικά Συμβούλια

Περίληψη

Η κυβερνοασφάλεια είναι ένας τομέας με ραγδαία ανάπτυξη και ταυτόχρονα μία απειλή που καλούνται όλο και πιο συχνά να αντιμετωπίσουν οι περισσότερες εταιρίες και οργανισμοί σήμερα. Τα Διοικητικά Συμβούλια είναι περισσότερο από ποτέ επιφορτισμένα με την ανεύρεση λύσεων και τρόπους αντιμετώπισης αυτών των απειλών.

Ο οδηγός που παρέχεται από τον διεθνή οργανισμό Internet Security Alliance αποτελεί μία προσπάθεια παρουσίασης και εξήγησης του κινδύνου που διατρέχουν οι εταιρίες σε ενδεχόμενη κυβερνοεπίθεση. Αυτή η προσπάθεια γίνεται, έτσι ώστε τα μέλη των Διοικητικών Συμβουλίων να μπορέσουν με τη σειρά τους να κατανοήσουν τους πιθανούς κινδύνους και να λάβουν τα απαραίτητα μέτρα για να εξασφαλίσουν, σε συνεργασία με τη διοίκηση της εκάστοτε εταιρίας, ότι διαθέτουν ισχυρούς μηχανισμούς αντιμετώπισης και διαχείρισης κρίσεων από ανάλογες επιθέσεις.

Ο οδηγός που συντάχθηκε από την ISA σε συνεργασία με την Ecoda (European Voice of Directors) και την AIG προτείνει την αδιάκοπη εφαρμογή ενιαίων μέτρων για τα μέλη των Διοικητικών Συμβουλίων, μέτρα κοινά σε παγκόσμιο επίπεδο. Ακολουθεί η περίληψη 5 συστάσεων για την διαχείριση κυβερνοεπιθέσεων μαζί με βασικά μέτρα και ορισμένα πρακτικά εργαλεία.

Ολόκληρο τον οδηγό μπορείτε να τον βρείτε εδώ

Σύσταση 1

Τα διευθυντικά στελέχη πρέπει να κατανοήσουν τη σοβαρότητα της κυβερνοασφάλειας καθώς και ότι η κυβερνοεπίθεση αποτελεί κίνδυνο για το σύνολο της εταιρίας και δεν αποτελεί αποκλειστικό πρόβλημα του τμήματος της Πληροφορικής της εταιρίας.

Βασικές προτάσεις:

•Η κυβερνοασφάλεια δεν πρέπει να θεωρείται ως ένα καθαρά τεχνικό ζήτημα που απασχολεί το τμήμα της Πληροφορικής μίας εταιρίας.

•Η κυβερνοασφάλεια πρέπει να αποτελεί μέρος του προγραμματισμού διαχείρισης και αντιμετώπισης Κρίσεων για όλο τον κύκλο ζωής μίας επιχείρησης.

•Η επίβλεψη και ο προγραμματισμός για την αντιμετώπιση ενδεχομένων κινδύνων πρέπει να εντάσσεται στις αρμοδιότητες του Διοικητικού Συμβουλίου.

•Το Διοικητικό Συμβούλιο δεν πρέπει να εφαρμόζει το ίδιο σχέδιο αντιμετώπισης κρίσεων σε όλες τις περιπτώσεις, αντιθέτως κάθε είδος ενδεχόμενης κρίσης πρέπει να έχει το δικό της αντίστοιχο σχέδιο αντιμετώπισης κινδύνων.

•Το Διοικητικό Συμβούλιο πρέπει να εφαρμόζει την απαραίτητη πολιτική στην εταιρία προκειμένου να διασφαλίζει ότι όλοι οι υπάλληλοι κατανοούν τη σοβαρότητα της κυβερνοασφάλειας καθώς και τους κινδύνους μιας κυβερνοεπίθεσης.

•Η διοίκηση της εταιρίας είναι υπεύθυνη να παρέχει όλες τις απαραίτητες πληροφορίες στο προσωπικό για την πρόληψη, την διαπίστωση και τους τρόπους αντιμετώπισης τέτοιων επιθέσεων καθώς και το σχέδιο διαχείρισης κρίσεων της εταιρίας που είναι διαθέσιμο σε ανάλογη περίπτωση.

Η διοίκηση πρέπει επίσης να λαμβάνει υπόψη της όχι μόνο το δικό της λειτουργικό δίκτυο πληροφοριών αλλά και τον ευρύτερο κυβερνοχώρο μέσα στον οποίο λειτουργεί.

Εργαλεία

Εργαλείο Α για πιθανές ερωτήσεις που πρέπει να συμπεριληφθούν στην αξιολόγηση του Διοικητικού Συμβουλίου και αυτοαξιολόγηση προκειμένου να προσμετρηθεί η κατανόηση της σοβαρότητας των κυβερνοεπιθέσεων καθώς και το επίπεδο ενημέρωσης του συμβουλίου για αυτές τις επιθέσεις.

Εργαλείο Β για μία λίστα ερωτήσεων σχετικά με τις κυβερνοεπιθέσεις που μπορούν οι διευθυντές να θέσουν στην διοίκηση της εταιρίας. Οι ερωτήσεις αυτές αφορούν τη στρατηγική που θα ακολουθήσει η εταιρία, την αξιολόγηση κινδύνου, τα μέτρα πρόληψης που έχει εφαρμόσει, την αντιμετώπιση τέτοιων περιστατικών καθώς και την ανταπόκριση (χρόνος ενημέρωσης) μετά από ενδεχόμενη κυβερνοεπίθεση.

Εργαλείο C για σχετικές ερωτήσεις που οι διευθυντές μπορούν να θέσουν προκειμένου να διεξάγουν ακριβείς και εμπεριστατωμένες μελέτες για την πρόληψη και αποφυγή κυβερνοεπιθέσεων.

Εργαλείο D για μέτρα πρόληψης ενδεχόμενων κυβερνοεπιθέσεων κατά τη διάρκεια συγχωνεύσεων και εξαγορών.

Εργαλείο Ε για αναφορές σε διεθνή πρότυπα.

Σύσταση 2

Οι διευθυντές πρέπει να κατανοούν τις έννομες συνέπειες και τον αντίκτυπο των κινδύνων στον κυβερνοχώρο που μπορεί να έχουν στη φήμη της εταιρίας.

Βασικές προτάσεις:

•Η κυβερνοασφάλεια δεν επηρεάζει μόνο τη φήμη της εκάστοτε εταιρίας, αλλά και την ευθύνη των μελών των Διοικητικών Συμβουλίων.

•Τα μέλη των Διοικητικών Συμβουλίων πρέπει να γνωρίζουν τις ισχύουσες νομοθεσίες σε εθνικό και Ευρωπαϊκό επίπεδο, καθώς και σε επίπεδο βιομηχανικού τομέα στον οποίο δραστηριοποιείται η εταιρία προκειμένου να μπορούν να ασκούν με κατάλληλο τρόπο το "καθήκον επιμέλειας" τους.

Σύσταση 3

Τα μέλη του Διοικητικού Συμβουλίου και τα λοιπά διευθυντικά στελέχη θα πρέπει να εξασφαλίζουν επαρκή πρόσβαση σε τεχνογνωσία και εξειδικευμένο προσωπικό στον τομέα της κυβερνοασφάλειας καθώς και να διασφαλίζουν την κατάλληλη υποβολή εκθέσεων σχετικά με την πρόσβαση σε εξειδικευμένο προσωπικό σε θέματα κυβερνοασφάλειας και στις κατάλληλες αναφορές για την πρόληψη, διαχείριση και αντιμετώπιση των κυβερνοεπιθέσεων

Βασικές προτάσεις:

- Τα μέλη των Διοικητικών Συμβουλίων πρέπει να εφαρμόζουν τις ίδιες αρχές διερεύνησης εποικοδομητικής κριτικής και για την λήψη στρατηγικών αποφάσεων.
- Το Διοικητικό Συμβούλιο οφείλει να διατυπώνει με σαφήνεια τις απαιτήσεις που έχει από την διοίκηση της εταιρίας και να είναι σαφές όσον αφορά τις πληροφορίες τις οποίες επιθυμεί να λαμβάνει.
- Ακόμα και αν έχει καταρτιστεί ειδική ομάδα για την κυβερνοασφάλεια, όλα τα μέλη του Διοικητικού Συμβουλίου πρέπει να ενημερώνονται με τριμηνιαίες εκθέσεις από τη διοίκηση της εταιρίας.
- Η κυβερνοασφάλεια δεν θα πρέπει να αντιμετωπίζεται ως αυτοτελής κίνδυνος, αλλά θα πρέπει να ενσωματώνεται σε όλες τις στρατηγικές αποφάσεις της εταιρίας.

Εργαλεία

Εργαλείο Α για τις κατάλληλες ερωτήσεις προς την ανώτατη διοίκηση αναφορικά με τη διαχείριση κυβερνοεπιθέσεων.

Εργαλείο Β για πιθανές ερωτήσεις και παραδείγματα εκθέσεων και πινάκων μετρήσεων για τους κινδύνους στον κυβερνοχώρο.

Σύσταση 4

Τα μέλη των Διοικητικών Συμβουλίων πρέπει να διασφαλίσουν ότι η διοίκηση της εταιρίας θα θεσπίσει ένα πλαίσιο για την πρόληψη, την αντιμετώπιση και τη διαχείριση των κινδύνων στον κυβερνοχώρο ενσωματώνοντάς το στην εταιρική κουλτούρα μέσω της ανάπτυξης των εξής δεξιοτήτων: την πρόληψη, τον εντοπισμό, την ανταπόκριση, την παρακολούθηση και την ενημέρωση σε όλα τα επίπεδα.

Οι διαθέσιμοι πόροι, (εργαζόμενοι, επενδύσεις, αναβάθμιση συστημάτων, κ.λπ.), που θα δαπανούνται πρέπει να είναι επαρκείς και να κατανέμονται κατάλληλα από τις στρατηγικές που υιοθετεί η εκάστοτε εταιρία.

Βασικές προτάσεις:

- Η διοίκηση της εταιρίας θα πρέπει να καταρτίσει ένα επιχειρησιακό τεχνικό σχέδιο (κινητά τηλέφωνα, τεχνητή νοημοσύνη κ.ά.) παράλληλα με ένα πιο συστηματικό σχέδιο δράσης για να διευκολύνει την επίβλεψη των κινδύνων στον κυβερνοχώρο.
- Η διοίκηση της εταιρίας πρέπει να έχει ολοκληρωμένη προσέγγιση για τους πιθανούς κινδύνους στον κυβερνοχώρο προκειμένου να καταστήσει σαφές πλαίσιο ανάληψης ευθυνών, διαδικασιών και οδηγιών επικοινωνίας.
- Η διοίκηση της εταιρίας θα πρέπει να επιλέξει μία συγκεντρωτική προσέγγιση «από τη βάση προς τα πάνω» στην αντιμετώπιση τέτοιων καταστάσεων.
- Το Διοικητικό Συμβούλιο μαζί με τα λοιπά διευθυντικά στελέχη της εταιρίας πρέπει να δώσει το στίγμα και να αναπτύξει την κατάλληλη κουλτούρα και την ευαισθητοποίηση σε θέματα κυβερνοεπιθέσεων.

Σύσταση 5

Οι συζητήσεις των Διοικητικών Συμβουλίων σχετικά με τους κινδύνους στον τομέα της κυβερνοασφάλειας θα πρέπει να περιλαμβάνουν στρατηγικές για τη διαχείρισή τους (περιορισμός κυβερνοεπιθέσεων, μετακύλισης κινδύνων μέσω της ασφάλισης ή μέσω συνεργασιών, κ.ά.).

Βασικές προτάσεις:

- Το Διοικητικό Συμβούλιο θα πρέπει να εξετάζει τις επενδύσεις για την αναβάθμιση της ηλεκτρονικής ασφαλείας των πληροφοριακών συστημάτων και να στρέφεται σε προσεγγίσεις που βασίζονται περισσότερο στην διαχείριση κινδύνων.
- Ο τομέας της κυβερνοασφάλειας πρέπει να αρχίσει να αντιμετωπίζεται σε επίπεδο πρόληψης και αντιμετώπισης μελλοντικών απωλειών.

Για περισσότερες πληροφορίες σχετικά με τον οδηγό παρακαλούμε επικοινωνήστε με το Internet Security Alliance

Mark Camillo
Head of Cyber, EMEA
AIG
T +44 (0)20 7651 6304
M +44 (0)78 6026 1692
mark.camillo@aig.com

Sebastian Hess
Cyber Risk Advisor, EMEA
AIG
T +49 69 97113-572
M +49 159 04611288
sebastian.hess@aig.com

Larry Clinton
President
Internet Security Alliance
T (001) 703-907-7090
lclinton@isalliance.org

Béatrice Richez-Baum
Director General
ecoDa
T +32 2 231 58 11
M +32 498 502 687
beatrice.richez-baum@ecoda.org