Διαδικτυακές απειλές στην ενέργεια

Το 80% των επιχειρήσεων στην Ευρώπη έχουν βιώσει τουλάχιστον ένα περιστατικό παραβίασης

ΤΑ CYBER ATTACKS ΣΤΟΝ ΤΟΜΕΑ ΤΩΝ ΥΠΟΔΟΜΩΝ ΜΠΟΡΟΥΝ ΝΑ ΕΠΗΡΕΑΣΟΥΝ ΤΙΣ ΚΑΘΗΜΕΡΙΝΕΣ ΛΕΙΤΟΥΡΓΙΕΣ ΕΝΟΣ ΟΡΓΑΝΙΣΜΟΥ

Της Έφης Π. Κουτσοβασίλη,
Εντεταλμένης Συμβούλου, Μέλους Δ.Σ.,
Eurobrokers Μεσίτες Ασφαλίσεων Α.Ε.

Οι ηλεκτρονικοί και οι διαδικτυακοί κίνδυνοι αποτελούν μια πραγματικότητα στον κόσμο των πληροφοριακών συστημάτων. Κάθε εταιρεία που ασχολείται με ηλεκτρονικά δεδομένα ανεξάρτητα από το εάν αυτά βρίσκονται σε υπολογιστές, servers ή το διαδίκτυο μπορεί να βρεθεί αντιμέτωπη με αντίστοιχες περιπτώσεις.

Η Ευρωπαϊκή Ένωση έχει αποφασίσει να κάνει περισσότερα για να αποτρέψει τις επιπτώσεις σε κρίσιμες υποδομές και τις παρεμβάσεις, εφαρμόζοντας το Γενικό Κανονισμό για την προστασία των δεδομένων (GDPR), που εκτός των υποδομών που χρειάζεται να αναπτύξει κάθε επιχείρηση για την προστασία των δεδομένων που διαχειρίζεται, απαιτεί και γνωστοποίηση των περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων εντός 72 ωρών στην αρμόδια αρχή.

Το 80% των επιχειρήσεων στην Ευρώπη έχουν βιώσει τουλάχιστον ένα περιστατικό παραβίασης της ασφάλειας στον κυβερνοχώρο.

Σημαντική παράμετρος για τους οργανισμούς που δραστηριοποιούνται στον ενεργειακό τομέα είναι η εξέταση δεδομένων σχετικά με την έκθεσή τους στον κυβερνοχώρο. Δύο είναι οι βασικές κατηγορίες που εξετάζονται στον κυβερνοχώρο σε σχέση με τα περιστατικά παραβίασης συστημάτων και απώλειας δεδομένων.

Υποδομή:

Οι απειλές του κυβερνοχώρου στον τομέα της υποδομής είναι εκείνες που μπορούν να επηρεάσουν τις καθημερινές λειτουργίες ενός οργανισμού με αποτελέσματα τη μερική απώλεια λειτουργικότητας έως τον τερματισμό λειτουργίας. Η παραγωγή ενέργειας και η διανομή αυξάνεται με πολύπλοκα συστήματα πληροφορικής. Τα συστήματα λογισμικού ελέγχου εισόδου (ICS), γνωστά και ως συστήματα SCADA (Supervisory Control and Data Acquisition) είναι ιδιαιτέρως ευάλωτα σε επιθέσεις στον κυβερνοχώρο. Οι περισσότεροι εμπειρογνώμονες συμφωνούν ότι η διακοπή λειτουργίας του δικτύου εξαιτίας παραβίασης ασφάλειας είναι σχετικά εύκολη για όσους έχουν τη θέληση, τους πόρους και το χρόνο που χρειάζονται.

Ασφάλεια δεδομένων:

Οι οργανισμοί του ευρύτερου δημοσίου, βιομηχανίες και διεθνείς οργανισμοί επιβάλλουν αυστηρούς κανόνες στις εταιρείες ενέργειας για την προστασία των προσωπικών δεδομένων που συλλέγουν, αποθηκεύουν, διατηρούν, μεταφέρουν ή χρησιμοποιούν, ανεξάρτητα από το αν οι πληροφορίες αυτές αφορούν υπαλλήλους του πελάτη ή και τρίτους, δεν έχει σημασία, οι οργανισμοί υποχρεούνται να ενημερώνονται σε περίπτωση παραβίασης.

Η μη συμμόρφωση μπορεί να οδηγήσει σε κυβερνητικές έρευνες, πρόστιμα και ποινές, καθώς και σε ιδιωτικές διαφορές. Η επιχείρηση ενδέχεται να αντιμετωπίσει:

- Την απώλεια, κλοπή προσωπικών δεδομένων, παραβίαση πληροφοριών πελατών και πρόσβαση τρίτων σε ευαίσθητα και σημαντικά δεδομένα.
- Την υποχρέωση με βάση την ισχύουσα νομοθεσία ενημέρωσης των φυσικών προσώπων τα προσωπικά δεδομένα των οποίων χάθηκαν ή διέρρευσαν και της Αρχής Προστασίας Δεδομένων.

Ο ρόλος της ασφάλισης (Cyber Insurance)

Οι επιχειρήσεις που δραστηριοποιούνται στον ενεργειακό τομέα ενδέχεται να μη γνωρίζουν ότι έχουν μεγάλη έκθεση στους ηλεκτρονικούς και διαδικτυακούς κινδύνους.

Η ασφάλιση Cyber Insurance αποτελεί ένα κρίσιμο κομμάτι της στρατηγικής για τη διαχείριση των κινδύνων, που πρέπει να χρησιμοποιεί κάθε εταιρεία ώστε να καλύπτει τους κινδύνους εκείνους που δεν μπορεί να μειώσει με τις πολιτικές διαχείρισης κινδύνου που εφαρμόζει.

Γνωρίζοντας ότι δεν καλύπτονται στο 100% οι κίνδυνοι, η αναγκαιότητα μεταφοράς κινδύνου είναι από τις βασικές πρακτικές που ακολουθούν οι μεγαλύτερες εταιρείες ενέργειας παγκοσμίως. Ενώ η ασφάλιση Cyber Insurance δεν μπορεί να εμποδίσει ένα περιστατικό παραβίασης ασφάλειας δεδομένων, μπορεί να προετοιμάσει όμως, πέραν της κάλυψης των οικονομικών απωλειών, το πλάνο αντιμετώπισης περιστατικών παραβίασης συστημάτων και απώλειας προσωπικών δεδομένων, παρέχοντας επαγγελματίες με εμπειρία στη διαχείριση διαδικτυακών κινδύνων, μειώνοντας έτσι τις οικονομικές επιπτώσεις α) απέναντι τρίτων που μπορεί να διεκδικήσουν αποζημιώσεις για ζημιά και/ή ηθική βλάβη αλλά και β) γιατί θα καταβληθούν πρόσθετα έξοδα ώστε η επιχείρηση να εξακριβώσει την προέλευση και το μέγεθος της απώλειας/διαρροής των δεδομένων και να αποκαταστήσει την ασφάλεια του συστήματος, καθώς και τη φήμη της επιχείρησης.

Για την υποστήριξη όλων των παραπάνω η Eurobrokers με το διεθνές δίκτυο συνεργατών της, έχει θέσει στη χρήση των πελατών της στο χώρο της ενέργειας, εργαλεία προσέγγισης των κινδύνων, στο πλαίσιο της πλήρους καταγραφής τους, ώστε να υπολογιστεί ο βαθμός έκθεσής τους σε αυτούς τους κινδύνους.

Η Eurobrokers έχει μια ομάδα αφιερωμένη στην ασφαλιστική κάλυψη των κινδύνων που αντιμετωπίζουν οι οργανισμοί στον τομέα της ενέργειας.

Επιπρόσθετα, αντιλαμβάνεται πλήρως τους κινδύνους που αντιμετωπίζουν στον κυβερνοχώρο και μπορεί να προσφέρει πρόσβαση σε εξειδικευμένες υπηρεσίες πριν και μετά τις παραβιάσεις μέσω των συνεργατών της στη διεθνή αγορά. Επειδή οι εταιρείες κοινής ωφελείας και οι εταιρείες που δραστηριοποιούνται στο χώρο της ενέργειας κατηγοριοποιούνται ως υποδομές ζωτικής σημασίας, ο χειρισμός των εξαιρετικά ευαίσθητων πληροφοριών για να εξεταστεί η δυνατότητα μεταφοράς του κινδύνου σε ασφαλιστικά προϊόντα Cyber Insurance είναι αρκετά δύσκολος. Οι συνεργασίες με παρόχους υπηρεσιών ασφαλείας πληροφοριών, που θα έχουν την εμπειρία αξιολόγησης και χειρισμού αυτών των πληροφοριών για λογαριασμό των αναδόχων και πιθανών ασφαλισμένων είναι επιβεβλημένες. Στην εταιρεία μας με τις διεθνείς συνεργασίες μας έχουμε καταφέρει να αναπτύξουμε τέτοια facilities ενώ επενδύουμε στη συγκεκριμένη αγορά (Cyber Insurance) και ειδικά στο χώρο της ενέργειας αλλά και ευρύτερα μιας και αποτελεί μια μοναδική ευκαιρία για ανάπτυξη στις μέρες μας.