Issue

Σχέδιο Αντιμετώπισης Περιστατικών Παραβίασης Ασφάλειας

Ένα σχέδιο αντιμετώπισης περιστατικών παραβίασης ασφάλειας (Incident Response Plan) είναι ένας γραπτός οδικός χάρτης με τη βοήθεια του οποίου οι επιχειρήσεις ανακαλύπτουν, αξιολογούν και ανταποκρίνονται σε ένα περιστατικό παραβίασης ασφάλειας των συστημάτων τους ή απώλειας δεδομένων των πελατών τους.

Ο πρωταρχικός στόχος του Πλάνου Αντιμετώπισης Περιστατικών είναι να διαχειριστεί η επιχείρηση αποτελεσματικά, τα περιστατικά που σχετίζονται με την παραβίαση ιδιωτικότητας ή ασφάλειας, να περιορίσει τη ζημιά, να αυξήσει την εμπιστοσύνη των πελατών και των μετόχων της επιχείρησης που αντιμετώπισε το περιστατικό, να ικανοποιήσει τις νομικές υποχρεώσεις που δημιουργούνται λόγω του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και να μειώσει το κόστος του περιστατικού στα οικονομικά αποτελέσματα της επιχείρησης και στη φήμη της. Τα πιο αποτελεσματικά πλάνα συντάσσονται για να ενεργοποιηθούν από υποτιθέμενα ή πραγματικά περιστατικά παραβίασης ασφάλειας και περιλαμβάνουν όλα τα τμήματα μιας επιχείρησης, τα συστήματά της και τα δεδομένα που διαχειρίζεται, τα οποία μπορεί να βρίσκονται, σε βάσεις δεδομένων της, σε κινητές συσκευές, σε διάφορες συσκευές όπως φωτοαντιγραφικά, συσκευές fax ή scanners.

Είναι πλέον κοινά παραδεκτό ότι κάποια στιγμή όλες οι επιχειρήσεις θα κληθούν να αντιμετωπίσουν ένα περιστατικό παραβίασης ασφάλειας και το Πλάνο Αντμετώπισης Περιστατικών θα τις βοηθήσει αποτελεσματικά.

Ας δούμε από τι αποτελείται ένα τέτοιο σχέδιο:

1. Δημιουργία Ομάδας Αντιμετώπισης Περιστατικών

Η ομάδα αυτή περιλαμβάνει στελέχη από τα τμήματα της εταιρίας που πρέπει να συμμετέχουν στην αντιμετώπιση ενος τέτοιου περιστατικού:

- Νομική Υπηρεσία
- Information Security/ Information technology
- Risk Management
- Κανονιστική Συμμόρφωση
- Δημοσίων Σχέσεων & Επικοινωνίας
- Εξυπηρέτησης Πελατών
- Οικονομική Διεύθυνση
- HR
- Marketing
- Business Continuity

– Η ομάδα πρέπει να συνεδριάζει σε τακτικά χρονικά διαστήματα και να εκπονεί ασκήσεις προσομοίωσης διάφορων σεναρίων ώστε τα μέλη της να είναι σε ετοιμότητα για την αντιμετώπιση περιστατικών.

Νίκος Γεωργόπουλος
MBA , cyRM, CDPO
Cyber Risks Insurance Advisor - Cromar coverholder at Lloyd's - Co Founder The DPO Academy

Η ομάδα αυτή συντονίζεται από τον **Incident Response Manager ή τον Data Protection Officer** (αν αυτοί οι δύο είναι διαφοτερικά πρόσωπα) ο οποίος θα φροντίζει για την συνεχή ετοιμότητά της και θα δίνει την κατάλληλη πληροφόρηση στον Διευθύνοντα Σύμβουλο κατά την εξέλιξη ενός περιστατικού παραβίασης.

– Τι θα πρέπει να γνωρίζουν τα μέλη της ομάδας αυτής:

Είναι πολύ σημαντικό να γνωρίζουν τα μέλη της ομάδας **τι είδους πληροφορίες διατηρεί η εταιρία**, ποιοι τις διαχειρίζονται, που είναι αποθηκευμένες **και ποιές είναι οι ευθύνες** της λόγω των κατηγοριών των δεδομένων που επεξεργάζεται. Πιο συγκεκριμένα θα πρέπει να γνωρίζουν:

- Τι είδος πληροφορίες διατηρεί η εταιρία για το ανθρώπινο δυναμικό της, τους πελάτες της, τους συνεργάτες της, τους προμηθευτές της
- Που είναι αποθηκευμένες αυτές οι πληροφορίες;
- Ποια συστήματα χρησιμοποιούνται για την διαχείρισή τους, και ποιες πολιτικές ασφάλειας πληροφοριών εφαρμόζονται για αυτά και αν είναι ενημερωμένες;
- Ποια μέλη της Ομάδας είναι υπεύθυνα για τα συστήματα αυτά;
- Υπάρχουν συνεργασίες με τρίτους (Processors) οι οποίοι διαχειρίζονται δεδομένα και εμπιστευτικές πληροφορίες της εταιρίας;

– Συνεργασία Ομάδας Διαχείρισης με εξωτερικούς παρόχους υπηρεσιών διαχείρισης περιστατικών παραβίασης

Τα μέλη της ομάδας που ανήκουν στην εταιρία συνεργάζονται με:

- Εξωτερικούς εξειδικευμένους Νομικούς Συμβούλους οι οποίοι θα μπορούν να γνωρίζουν και να διαχειριστούν τις υποχρεώσεις της εταιρίας.
- Εξωτερικούς συνεργάτες (Forensics Investigators, επικοινωνιολόγους) οι οποίοι μπορούν να προσφέρουν εξειδικευμένη γνώση.
- την ασφαλιστική εταιρία αν η εταιρία είναι ασφαλισμένη με **ασφάλιση Cyber Insurance**

2. Κατηγοριοποίηση επικινδυνότητας Περιστατικού

Τα συμβάντα ασφαλείας ποικίλουν σε επικινδυνότητα, αιτίες, τρόπους, αριθμό. Είναι απαραίτητη η κατηγοριοποίησή τους, έτσι ώστε να είναι σαφές σε όλους τους εμπλεκομένους ποιες συγκεκριμένες ενέργειες πρέπει να υλοποιήσουν ανά περίπτωση.

3. Ενεργοποίηση επικοινωνιακού πλάνο αντιμετώπισης του περιστατικού

Το επικοινωνιακό πλάνο αντιμετώπισης περιστατικού είναι πολύ σημαντικό για την επικοινωνιακή διαχείριση της εταιρικής επωνυμίας και του μυνήματος που πρέπει να σταλλεί σε πελάτες, προμηθευτές , συνεργάτες , εποπτικές αρχές, με την χρήση των κατάλληλων μέσων επικοινωνίας

Δεν πρέπει να υπάρξει πανικός

Με την εκδήλωση του περιστατικού θα πρέπει:

- Να ειδοποιήσουμε τα μέλη της Ομάδας Αντιμετώπισης Περιστατικών.
- Να προσδιορίσουμε το είδος των δεδομένων,την ποσότητα και τα συστήματα που έχουμε πρόβλημα και να φροντίσουμε να σταματήσουμε την διαρροή με την βοήθεια ειδικών
- Να ενημερώσουμε τους εξειδικευμένους νομικούς συμβούλους μας
- **Να ενημερώσουμε την ασφαλιστική μας εταιρία αν έχουμε ασφάλιση Cyber Insurance**
- Να ενημερώσουμε τις αρμόδιες αρχές που επιβάλλει η νομοθεσία και τους τρίτους που επηρεάζονται από το περιστατικό αν αυτό κριθεί απαραίτητο
- Να ακολουθήσουμε το επικοινωνιακό πλάνο που έχουμε δημιουργήσει

Ασφάλιση Cyber Insurance & Πλάνο Αντιμετώπισης Περιστατικών

Η ασφάλιση Cyber Insurance είναι ένα κρίσιμο κομμάτι της συνολικής στρατηγικής για τη διαχείριση των κινδύνων. Ενώ η ασφάλιση δεν μπορεί να εμποδίσει ένα περιστατικό ασφαλείας, μπορεί να εκτός από την οικονομική προστασία της εταιρίας να κάνει το Πλάνο Αντιμετώπισης Περιστατικών της εταιρίας αποτελεσματικό με την παροχή βοήθειας μέσω εξειδικευμένων παρόχων οι οποίοι έχουν αντιμετωπίσει μεγάλο αριθμό περιστατικών παραβίασης ασφάλειας διεθνώς.

Αν θέλετε να δημιουργήσετε το Πλάνο Αντιμετώπισης Περιστατικών της εταιρίας σας χρησιμοποιήστε υποδείγματα που βρίσκονται στην εκπαιδευτική μηχανή www.cyberinsurancequote.gr και πιο συγκεκριμένα στο link. https://www.cyberinsurancequote.gr/insurance/incident-plan/ . ITSecurity