

Issue

TECH INSURANCE – ΕΡΓΑΛΕΙΟ ΟΙΚΟΝΟΜΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ & ΑΝΑΠΤΥΞΗΣ ΕΡΓΑΣΙΩΝ ΤΩΝ ΕΤΑΙΡΙΩΝ ΤΕΧΝΟΛΟΓΙΑΣ



Η

τεχνολογία αποτελεί αναπόσπαστο μέρος των επιχειρηματικών λειτουργιών μιας εταιρίας τεχνολογίας (και όχι μόνο) και οι κίνδυνοι που συνδέονται με κυβερνοεπιθέσεις, περιστατικά παραβίασης ασφάλειας και μη δυνατότητας παροχής και υποστήριξης παρεχόμενων υπηρεσιών συνεχώς αυξάνονται. Για να αντιμετωπίσουν τους παραπάνω κινδύνους, πολλές εταιρείες τεχνολογίας στρέφονται στις δύο βασικές κατηγορίες ασφάλισης - την ασφάλιση τεχνολογικών σφαλμάτων και παραλείψεων (Tech E&O) και την ασφάλιση κινδύνων διαδικτύου (Cyber Insurance). Στη συνέχεια θα δούμε πιο αναλυτικά τις κατηγορίες ασφάλισης που πρέπει να έχουν οι εταιρίες τεχνολογίας και **γιατί πρέπει να επενδύουν σε ασφαλιστικά προϊόντα Tech Insurance** που συνδυάζουν αυτές τις κατηγορίες ασφάλισης για να διαχειριστούν αποτελεσματικά τους τεχνολογικούς κινδύνους που απειλούν

τις παρεχόμενες υπηρεσίες και προϊόντα και να αυξάνουν τις πωλήσεις των προϊόντων και υπηρεσιών.

Παρακάτω θα δούμε τις διαφορές μεταξύ της ασφάλισης επαγγελματικής ευθύνης λόγω τεχνολογικών σφαλμάτων ή παραλείψεων (Tech E&O) και της ασφάλισης κινδύνων διαδικτύου (Cyber Insurance) με σκοπό να βοηθήσουμε τις εταιρίες τεχνολογίας να κατανοήσουν γιατί είναι απαραίτητη η επένδυση σε ασφαλιστικά προϊόντα **Tech Insurance**.

1. Ασφάλιση Επαγγελματικής Ευθύνης εταιριών Τεχνολογίας.

Η ασφάλιση Τεχνολογίας E&O παρέχει κάλυψη για επιχειρήσεις που παρέχουν προϊόντα ή υπηρεσίες τεχνολογίας, όπως ανάπτυξη λογισμικού, παροχή λογισμικού ως υπηρεσία (SaaS), συμβουλευτικές υπηρεσίες πληροφορικής, φιλοξενία στο cloud και άλλες. Καλύπτει αξιώσεις για αμέλεια, λάθη ή παραλείψεις κατά την παροχή αυτών των υπηρεσιών.



ών ή προϊόντων που προκαλούν οικονομική ζημία σε έναν πελάτη.

Βασικά στοιχεία κάλυψης της ασφάλισης Επαγγελματικής Ευθύνης εταιριών Τεχνολογίας:

- **Αμέλεια κατά την παροχή υπηρεσιών:** Καλύπτει αξιώσεις που προκύπτουν από την αποτυχία παροχής/παράδοσης των υποσχεμένων τεχνολογικών προϊόντων & υπηρεσιών.
- **Σφάλματα σε λογισμικό ή συστήματα:** Παρέχει κάλυψη για οικονομικές απώλειες που προκύπτουν από σφάλματα λογισμικού, λάθη ή αποτυχίες στο σχεδιασμό ή την υλοποίηση συστημάτων.
- **Συμβατικές υποχρεώσεις:** Καλύπτει τις ευθύνες από ακούσιες παραβιάσεις της σύμβασης, όταν μια εταιρεία τεχνολογίας αποτυγχάνει να τηρήσει τους συμφωνηθέντες όρους κατά την παροχή τεχνολογικών υπηρεσιών ή προϊόντων.
- **Οικονομικές απώλειες τρίτων:** Προστατεύει από αξιώσεις πελατών που υφίστανται οικονομική ζημία λόγω επαγγελματικών λαθών, σφαλμάτων ή παραλείψεων μιας εταιρείας τεχνολογίας.

Η ασφάλιση επαγγελματικής ευθύνης, δεν καλύπτει συνήθως κινδύνους στον κυβερνοχώρο, όπως περιστατικά παραβιάσεις ασφάλειας και απώλειες δεδομένων ή επιθέσεις ransomware που επηρεάζουν την ίδια την επιχείρηση για αυτό το λόγο θα πρέπει οι εταιρίες τεχνολογίας να επενδύσουν και στην ασφάλιση του κυβερνοχώρου.

2. Ασφάλιση στον κυβερνοχώρο: Προστασία από περιστατικά παραβίασης ασφάλειας, απώλειες δεδομένων και επιθέσεις στον κυβερνοχώρο.

Η ασφάλιση στον κυβερνοχώρο έχει σχεδιαστεί για να καλύπτει τις οικονομικές απώλειες που προκύπτουν από περιστατικά παραβίασης ασφάλειας

στον κυβερνοχώρο. Η ασφάλιση είναι απαραίτητη για τις επιχειρήσεις που διαχειρίζονται προσωπικά δεδομένα πελατών ή εργαζομένων, και τις επιχειρήσεις που παρέχουν λογισμικό ως υπηρεσία ή υπηρεσίες Managed Security Services σε τρίτους.

Βασικά στοιχεία κάλυψης της ασφάλισης στον κυβερνοχώρο:

- **Αντιμετώπιση περιστατικών παραβίασης ασφάλειας και απώλειας δεδομένων:** Καλύπτει τα έξοδα που σχετίζονται με την αντιμετώπιση ενός περιστατικού παραβίασης ασφάλειας ή απώλειας δεδομένων.
- **Απώλειες Εσόδων λόγω διακοπής εργασιών:** Αποζημιώνει την επιχείρηση για διαφυγόντα έσοδα ή πρόσθετα έξοδα που προκύπτουν λόγω διακοπής λειτουργίας του δικτύου λόγω κυβερνοεπίθεσης ή ακόμη και σε περίπτωση που η διακοπή οφείλεται σε ανθρώπινο λάθος (Systems Failure).
- **Εκβιασμός στον κυβερνοχώρο/καταβολή λύτρων:** Καλύπτει το κόστος ανταπόκρισης σε απαιτήσεις εκβιασμού, όπως η καταβολή λύτρων ή η διαπραγμάτευση με εγκληματίες του κυβερνοχώρου.
- **Πρόστιμα Ρυθμιστικών Αρχών και κυρώσεις:** Πληρωμή Προστίμων που επιβάλλονται από τις ρυθμιστικές αρχές λόγω παραβιάσεων Οδηγιών ή Κανονισμών που εκάστοτε ισχύουν όπως ο GDPR, NIS2, DORA εφόσον αυτό αυτό επιτρέπεται από την ισχύουσα νομοθεσία.
- **Νομικά έξοδα υπεράσπισης και δικακωνομοί:** Καλύπτει νομικά έξοδα και διακανονισμούς που προκύπτουν από αγωγές που σχετίζονται με ένα περιστατικό στον κυβερνοχώρο, όπως ομαδικές αγωγές από πελάτες που επηρεάζονται από ένα περιστατικό παραβίασης δεδομένων.

Η ασφάλιση στον κυβερνοχώρο επικεντρώνεται ειδικά στην προστασία μιας

επιχείρησης από τους κινδύνους στον κυβερνοχώρο και τις άμεσες συνέπειές τους, όπως τα περιστατικά παραβίασης ασφάλειας και απώλειας δεδομένων και προσφέρει Υπηρεσίες Πρόληψης, Αντιμετώπισης Περιστατικών Παραβίασης Ασφάλειας και Οικονομική Προστασία. **Δεν έχει σχεδιαστεί για να καλύπτει αστοχίες κατά την εκτέλεση τεχνολογικών υπηρεσιών ή προϊόντων, για την κάλυψη των οποίων απαραίτητη είναι η ασφάλιση επαγγελματικής ευθύνης.** Για αυτό οι εταιρίες τεχνολογίας θα πρέπει να επιλέγουν ασφαλιστικά προϊόντα Tech Insurance τα οποία συνδυάζουν και τις δύο κατηγορίες ασφάλισης και επιπλέον προσφέρουν και καλύψεις Γενικής Αστικής Ευθύνης και Cyber Crime στο ίδιο ασφαλιστήριο συμβόλαιο.

ΤΙ ΠΡΟΣΦΕΡΕΙ Η ΑΣΦΑΛΙΣΗ TECH INSURANCE:

Η ασφάλιση Tech Insurance το οποίο είναι ένα Εργαλείο Διαχείρισης των Κινδύνων και Οικονομικής Προστασίας είναι απαραίτητο, για την **αύξηση των πωλήσεων της εταιρίας** γιατί πλέον η ύπαρξή της είναι **αναγκαία για την συμμετοχή της εταιρίας σε διαγωνισμούς υλοποίησης έργων τεχνολογίας και την συμμόρφωσή της με NIS2 και DORA.** Η συμμόρφωση με τις οδηγίες NIS2 και DORA είναι ζωτικής σημασίας για τις εταιρίες τεχνολογίας που αποτελούν προμηθευτές ή μέλος της εφοδιαστικής αλυσίδας εταιρικών πελατών. Συνοψίζοντας, η ασφάλιση Tech Insurance είναι **απαραίτητη για τις εταιρίες τεχνολογίας** που αποτελούν προμηθευτές ή μέλος της εφοδιαστικής αλυσίδας, καθώς παρέχει οικονομική προστασία από κυβερνοεπιθέσεις, **καλύπτει την επαγγελματική ευθύνη** τους, βοηθά στη **συμμόρφωση με κανονισμούς**, ενισχύει την ασφάλεια της αλυσίδας εφοδιασμού και αυξάνει την εμπιστοσύνη των πελατών.