

Issue

Αποτελεσματική διαχείριση κινδύνων με ασφάλιση Cyber Insurance

Η ασφάλιση Cyber Insurance αποτελεί ένα κρίσιμο κομμάτι της στρατηγικής για τη διαχείριση των κινδύνων που πρέπει να χρησιμοποιήσει ο Information Security Officer.

Tο νέο περιβάλλον στο οποίο καλούνται να δραστηριοποιηθούν οι επιχειρήσεις απαιτεί την συμμορφωσή τους με το νέο Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (GDPR) ο οποίος απαιτεί από τις εταιρείες:

- να έχουν εκπαιδεύσει κατάλληλα το ανθρώπινο δυναμικό τους
- να έχουν τα κατάλληλα μέτρα ασφαλείας και τις αναγκαίες πολιτικές για την προστασία των πληροφοριών
- να κάνουν αναλύσεις των επιπτώσεων που μπορούν να προκύψουν λόγω παραβίασης ιδιωτικότητας
- να σχεδιάζουν προϊόντα και υπηρεσίες λαμβάνοντας υπόψη την προστασία της ιδιωτικότητας
- να ενημερώνουν τις αρμόδιες αρχές εντός 72 ωρών από τον εντοπισμό συμβάντος παραβίασης συστημάτων και απώλειας δεδομένων
- να έχουν ορίσει υπεύθυνο για την προστασία των δεδομένων (Data Protection Officer)
- να έχουν πλάνο αντιμετώπισης περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων (Incident Response Plan)

Επίσης, ο νέος κανονισμός προβλέπει πρόστιμα τα οποία μπορούν να φθάσουν έως 4% του τζίρου της επιχείρησης.

Ο νέος Κανονισμός αναμένεται να αναγκάσει τις εταιρίες να συμμορφωθούν στα νέα δεδομένα και να προετοιμαστούν κατάλληλα επιλέγοντας προϊόντα και υπηρεσίες, προστασίας

των πληροφοριών που διαχειρίζονται, που θα τις βοηθήσουν να αντιμετωπίσουν αποτελεσματικά μελλοντικά περιστατικά. Λαμβάνοντας υπόψη ότι 100% ασφάλεια δεν υπάρχει θα πρέπει να εξετάσουν τη δυνατότητα μεταφοράς του κινδύνου που απομένει και δεν μπορούν να μειώσουν περαιτέρω σε ασφαλιστικά προϊόντα cyber insurance.

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 παραβίασης ασφαλείας, μπορεί εκτός από την κάλυψη των οικονομικών επιπτώσεων, να βοηθήσει και το πρόγραμμα ασφάλειας πληροφοριών της εταιρείας με την παροχή βοήθειας μέσω εξειδικευμένων παρόχων που παρέχουν τις κατάλληλες υποδομές και το κατάλληλο ανθρώπινο δυναμικό, όταν εμφανίζεται συμβάν μειώνοντας τις επιπτώσεις της παραβίασης στους πελάτες, τη φήμη της εταιρείας και το εμπορικό σήμα της.

Η ασφάλιση cyber insurance καλύπτει:

- Αστική Ευθύνη έναντι τρίτων οι οποίοι οι υπέστησαν ζημιά λόγω απώλειας των προσωπικών τους δεδομένων από την εταιρία στην οποία τα είχαν δώσει
- Έξοδα και Υπηρεσίες διαχείρισης περιστατικών παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών
- Διακοπή Εργασιών - καλύπτει απώλεια εισόδων λόγω διακοπής της επιχειρηματικής δραστηριότητας από περιστατικά παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών
- Κυβερνοεκβιασμό - κάλυψη για διαχείριση περιστατικών





Nίκος Γεωργόπουλος
Cyber Risks Insurance Advisor, Cromar coverholder at Lloyds
www.cyberinsurancequote.gr

εκβιασμού από απειλές που μπορεί να βλάψουν ένα δίκτυο ή να οδηγήσουν σε διαρροή εμπιστευτικών πληροφοριών

- Διοικητικά Πρόστιμα - που τυχόν επιβληθούν από αρμόδιες αρχές για περιστατικά απώλειας δεδομένων (data breach)



Με τη βοήθεια της ασφάλισης cyber insurance οι επιχειρήσεις θα προστατεύσουν τους ισολογισμούς τους και θα διαχειριστούν αποτελεσματικά τις συνέπειες των περιστατικών αυτών. Ας δούμε λίγο πραγματικά περιστατικά αποζημιώσεων cyber insurance από ασφαλιστικές εταιρίες στην Ευρώπη και στην Αμερική.

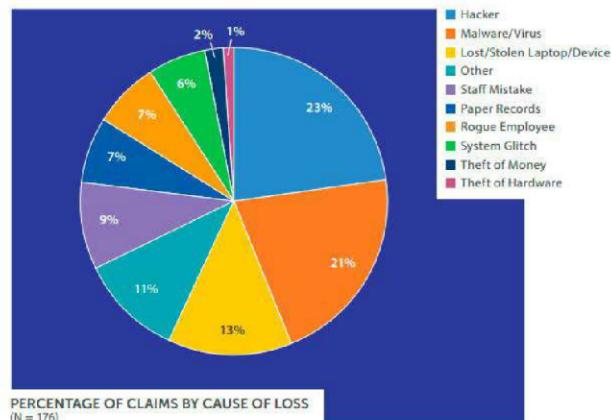
Στο γράφημα που ακολουθεί μπορούμε να δούμε αναλυτικά την κατανομή των αιτίων που οδήγησαν σε παραβίαση συστημάτων και απώλεια εμπιστευτικών πληροφοριών **ασφαλισμένων Ευρωπαϊκών εταιρειών** και ενεργοποίησαν ασφαλιστήρια Cyber Insurance της εταιρείας AIG.

Cyber claims received by AIG EMEA (2013-2016) - By type



Πιο αναλυτικά οι κυριότερες περιπτώσεις αποζημιώσεων ασφάλισης cyber insurance οφείλονται: το 16% οφείλεται σε περιστατικά ransomware & Cyber Extortion, το 14% σε απώλεια δεδομένων λόγω Hacking, το 10% σε μή εξουσιοδοτημένη πρόσβαση σε εταιρικά συστήματα, το 10% από malware/virus, το 8% σε περιστατικά απώλειας δεδομένων από αμέλεια εργαζομένων, το 6% σε περιστατικά άρνησης παροχής υπηρεσίας (DDoS), το 6% σε απώλεια laptops, tablets, κινητών τηλεφώνων, το 4% σε κυβερνοεκβιασμό, το 4% σε περιστατικά

παραβίασης νομοθεσίας για τα προσωπικά δεδομένα, το 4% σε αστοχίες συστημάτων και διαδικασίων, το 4% σε διακοπή εργασιών και το υπόλοιπο 9% σε άλλους παράγοντες. Ας δούμε και τι συνέβη στην **Αμερικανική αγορά cyber insurance** σε περιπτώσεις αποζημιώσεων ασφαλισμένων εταιριών σύμφωνα με την μελέτη της NetDiligence.



Πηγή: NetDiligence Cyber Claims Study 2016

Οι κυριότερες περιπτώσεις αποζημιώσεων ασφάλισης cyber insurance οφείλονται: το 23% σε περιστατικά Hacking, το 21% σε ιούς, το 13% σε απώλεια laptops, tablets, κινητών τηλεφώνων, το 9% σε ανθρώπινα λάθη των εργαζομένων, το 7% σε απώλεια πληροφοριών που ήταν αποθηκευμένες σε χαρτί, το 7% σε κακόβουλους εργαζόμενους, το 6% σε αστοχία συστημάτων ή διαδικασιών.

Βραβείο Καινοτομίας Lloyds Market Innovation 2016 για το www.cyberinsurancequote.gr

Για την πληροφόρηση των εταιρειών και των επαγγελματιών σχετικά με θέματα: προετοιμασία, εκπαίδευση ανθρώπινου δυναμικού, νομοθεσίας, κανονιστικής συμμόρφωσης, αντιμετώπισης πειριστατικών περιστατικών παραβίασης και την χρήση της ασφάλισης cyber insurance δημιουργήσαμε μία καινοτόμα εκπαιδευτική μπραντί www.cyberinsurancequote.gr η οποία βραβεύθηκε από την αγορά των Lloyd's με το βραβείο καινοτομίας για το έτος 2016. **IT Security**

