ΕΝΩΣΗ
ΑΣΦΑΛΙΣΤΙΚΩΝ
ΕΤΑΙΡΙΩΝ
ΕΛΛΑΔΟΣ

CYBER INSURANCE

Ασφάλιση κατά των Κινδύνων Κυβερνοχώρου

Δεκέμβριος 2023

www.eaee.gr

Περιεχόμενα

Η ασφάλιση στην πράξη 4

Τι καλύπτεται με την ασφάλιση κατά κινδύνων του κυβερνοχώρου 5

Πιθανές εξαιρέσεις από την ασφάλιση κατά κινδύνων του κυβερνοχώρου 7

Αγορά ασφάλισης κατά κινδύνων του κυβερνοχώρου 8

Χρήσιμες συμβουλές για το πώς μπορείτε να ενισχύσετε την ανθεκτικότητα της επιχείρησής σας κατά κινδύνων του κυβερνοχώρου 11

Οι επιχειρήσεις στην Ελλάδα, όπως και σε όλον τον κόσμο, ανεξαρτήτως μεγέθους και αντικειμένου, γίνονται ολοένα και περισσότερο εξαρτημένες από τα πληροφοριακά τους συστήματα και τα δεδομένα που συγκεντρώνουν. Και ενώ τα ψηφιακά εργαλεία ενθαρρύνουν την καινοτομία, βελτιώνουν την αποτελεσματικότητα και μειώνουν το λειτουργικό κόστος, αποτελούν ταυτόχρονα ένα τεράστιο πεδίο εγκληματικής δράσης.

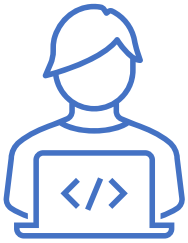
Οι κυβερνοεπιθέσεις και οι παραβιάσεις δεδομένων βρίσκονται καθημερινά στην επικαιρότητα.

Είναι επομένως πολύ σημαντικό **να εξετάσετε ΣΗΜΕΡΑ την ανθεκτικότητα της επιχείρησής σας** στον κυβερνοχώρο και να λάβετε όλα τα απαραίτητα μέτρα για την αποτελεσματική θωράκισή της.

Η κυβερνοασφάλεια δεν πρέπει να θεωρείται ως ένα καθαρά τεχνικό ζήτημα που απασχολεί μόνο το τμήμα πληροφορικής μιας εταιρίας. Πρέπει να αποτελεί μέρος του συνολικού προγραμματισμού διαχείρισης και αντιμετώπισης κρίσεων για όλο τον κύκλο ζωής μιας επιχείρησης.

Η **ασφάλιση κατά των κινδύνων του κυβερνοχώρου** αποτελεί **πολύτιμο εργαλείο** για την επιχείρησή σας σε αυτήν την προσπάθεια.

Η **προστασία** που σας **παρέχει η ασφάλιση** έχει **δύο μορφές**:



Οι ασφαλιστές κατανοούν τους κινδύνους στον κυβερνοχώρο και μπορούν να υποστηρίξουν αποτελεσματικά την επιχείρησή σας στην **πρόληψη** αυτών των κινδύνων, βοηθώντας σας να αντιληφθείτε έγκαιρα τα τρωτά σημεία και να λάβετε τα κατάλληλα μέτρα για τη βελτίωση και ενίσχυση της ψηφιακής της ανθεκτικότητας.

Και εάν τα πράγματα – παρόλα αυτά - δεν πάνε καλά και η απειλή γίνει πραγματικότητα, η ασφάλιση προσφέρει **ισχυρό δίχτυ προστασίας** στην επιχείρησή σας και με μια εξειδικευμένη ομάδα ειδικών αναλαμβάνει να βοηθήσει τη συνέχιση λειτουργίας της και τη διαχείριση της αβεβαιότητας, ενώ φυσικά θα αναλάβει και τις οικονομικές επιπτώσεις της κυβερνοεπίθεσης.

Η ασφάλιση στην πράξη

Ασφαλισμένος, ελεύθερος επαγγελματίας, ανακαλύπτει ότι κατά τη διάρκεια της νύκτας το σύνολο των ηλεκτρονικών του αρχείων έχει κλειδωθεί και του ζητούνται λύτρα προκειμένου να επανέλθουν. Ο ασφαλισμένος ζητάει τη βοήθεια των ειδικών της ασφαλιστικής του εταιρίας προκειμένου να διαπιστώσει εάν οι hackers έχουν επιπλέον αντιγράψει τα αρχεία του. Δηλώνει ότι δεν θέλει να πληρώσει γιατί έχει backup, αλλά θέλει βοήθεια στο να καθαρίσουν τα μηχανήματα του και να μπει το backup. Ζητάει επίσης συμβουλές στο πως δεν θα επαναληφθεί ανάλογο περιστατικό στο μέλλον και τι βελτιώσεις πρέπει να κάνει στην υποδομή του. Η ασφαλιστική εταιρία με την εξειδικευμένη ομάδα συμβούλων που διαθέτει συνδράμει τον ασφαλισμένο της παρέχοντας χρήσιμες οδηγίες και υποστήριξη στα παραπάνω ζητήματα.

Ασφαλισμένη εταιρία εμπορίου έγινε στόχος ομάδας κυβερνοεγκληματιών, οι οποίοι κρυπτογραφήσαν το μεγαλύτερο μέρος του Data Center της εταιρίας με αποτέλεσμα τα ηλεκτρονικά συστήματα του οργανισμού να τεθούν εκτός λειτουργίας, και έτσι ο οργανισμός να μη μπορεί να υποστηρίξει τους πελάτες του είτε μέσω του shop είτε στα φυσικά καταστήματα. Ζητήθηκε ένα υπέρογκο ποσό λύτρων. Οι σύμβουλοι της ασφαλιστικής εταιρίας συνεργάστηκαν με τις ομάδες IT που είχε ορίσει ο ασφαλισμένος, διαπραγματεύτηκαν με τους hacker το ύψος των λύτρων, βεβαιωθήκαν ότι όντως τα αρχεία μπορούσαν να επανέλθουν και πλήρωσαν τελικά τα λύτρα που συμφωνήθηκαν σε crypto νομίσματα. Στη συνέχεια αντικαταστάθηκε κατεστραμμένος ηλεκτρονικός εξοπλισμός και περάστηκαν εκ νέου τα δεδομένα αφού αποκρυπτογραφήθηκαν επιτυχώς, διαδικασία ιδιαίτερα πολύπλοκη, και αφού ελέγχθηκαν για κρυμμένο malware.

Τι καλύπτεται με την ασφάλιση κατά κινδύνων του κυβερνοχώρου

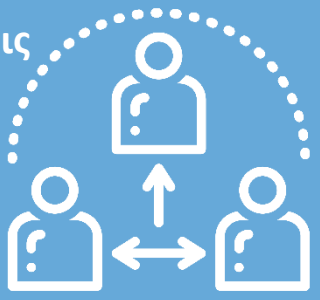
Απώλεια Προσωπικών & Εταιρικών Πληροφορίων

Η ασφάλιση κατά κινδύνων του κυβερνοχώρου καλύπτει τις απώλειες που σχετίζονται με ζημιά ή απώλεια πληροφοριών από συστήματα και δίκτυα πληροφορικής.

Καλύπτει μια άμεση οικονομική ζημία για εσάς ή την επιχείρησή σας που προκύπτει από ένα συμβάν στον κυβερνοχώρο. Ένα συμβάν στον κυβερνοχώρο είναι οποιαδήποτε πραγματική ή υπόνοια μη εξουσιοδοτημένης πρόσβασης στα συστήματα πληροφορικής, ηλεκτρονική επίθεση ή παραβίαση του απορρήτου. Η συντριπτική πλειονότητα των οικονομικών απωλειών είναι απώλειες που θα υποστεί άμεσα η επιχείρησή σας και περιλαμβάνουν κλοπή δεδομένων ή / και ζημιά σε ψηφιακά περιουσιακά στοιχεία.

Αξιώσεις Τρίτων

Η ασφάλιση κατά κινδύνων του κυβερνοχώρου καλύπτει διάφορες οικονομικές αξιώσεις που θα εγείρουν τρίτοι σε βάρος σας, (ενδεικτικά πελάτες, συνεργάτες, προμηθευτές, ρυθμιστικές αρχές), οι οποίοι θα ισχυριστούν και θα αποδείξουν ότι με πράξεις ή παραλήψεις του οργανισμού σας ή από κακόβουλη ενέργεια τρίτων (hackers) που σχετίζεται με κινδύνους του κυβερνοχώρου προκλήθηκε σε αυτούς οικονομική ζημιά ή ηθική βλάβη, για την οποία δικαιούνται και διεκδικούν εκ του νόμου χρηματική αποζημίωση.



Διαχείριση Γεγονότων

Μια βασική παροχή που προσφέρουν αυτά τα συμβόλαια είναι ότι όχι μόνο αποζημιώνουν για την ζημιά όπως συμβαίνει με άλλα ασφαλιστήρια συμβόλαια, αλλά και συμβάλλουν ουσιαστικά στη διαχείριση του συμβάντος.

Η ασφάλιση κατά κινδύνων κυβερνοχώρου σας δίνει ταχύτατη πρόσβαση (24/7 Ανοιχτή Γραμμή Βοήθειας) σε ειδικούς για την διαχείριση περιστατικών στον κυβερνοχώρο τόσο πριν όσο και μετά την εκδήλωση ενός συμβάντος, οι οποίοι:

- ☑ θα εντοπίσουν την αιτία εφόσον είναι τεχνικά εφικτό
- ☑ θα περιορίσουν την εξάπλωση και άρα τη ζημία από την επίθεση
- ☑ θα διαχειριστούν τις επακόλουθες συνέπειες, και τέλος
- ☑ θα αποκαταστήσουν τη φυσιολογική λειτουργία της επιχείρησής σας

Έξοδα αποκατάστασης της Φήμης και της υπόληψης, διακοπής εργασιών, νομικά έξοδα και κόστη εκβίασης

Εκτός από την άμεση και επείγουσα ανταπόκριση, καθώς και το κόστος επανεγκατάστασης του software (και hardware σε κάποιες περιπτώσεις), η ασφάλιση ευθύνης κατά κινδύνων του κυβερνοχώρου καλύπτει:

- το κόστος ενημέρωσης των πελατών
- την παρακολούθηση των υποκλοπών πιστωτικών καρτών και προσωπικών δεδομένων των πελατών σας
- τη διακοπή εργασιών και τα έξοδα εναλλακτικών μέσων εργασίας
- το κόστος της έρευνας
- το κόστος της εκβίασης
- τα νομικά έξοδα και τις σχετικές αποζημιώσεις
- τη βλάβη φήμης της επιχείρησης που έχει υποστεί κυβερνοεπίθεση.

Συμπληρωματικές καλύψεις

Ορισμένες συμπληρωματικές καλύψεις που μπορεί να προσφέρει το ασφαλιστικό προϊόν είναι:

- η κάλυψη της δόλιας εντολής μεταφοράς χρημάτων (δηλαδή κάλυψη της αποστολής χρημάτων σε άγνωστο παραλήπτη μετά από λήψη παραποιημένου παραστατικού μέσω email)
- η κάλυψη της τηλεπικοινωνιακής απάτης (δηλαδή κάλυψη του κόστους τηλεπικοινωνιακών χρεώσεων λόγω παράνομης πρόσβασης & χρήσης εταιρικού τηλεφωνικού κέντρου)
- η κάλυψη για παραβίαση πνευματικής ιδιοκτησίας που προκύπτει από τη διαφήμιση των υπηρεσιών σας. Συχνά ισχύει τόσο για τη διαφήμισή σας στο διαδίκτυο, συμπεριλαμβανομένων των αναρτήσεων στα μέσα κοινωνικής δικτύωσης, όσο και για την έντυπη διαφήμιση.

Πιθανές εξαιρέσεις από την ασφάλιση κατά κινδύνων του κυβερνοχώρου

Όπως σε κάθε ασφαλιστήριο συμβόλαιο, είναι σημαντικό να αξιολογήσετε όχι μόνο τι καλύπτεται από το ασφαλιστήριο σας αλλά και τι εξαιρείται.

Οι εξαιρέσεις από την κάλυψη, όπως και το πλαίσιο κάλυψης που προσφέρει ένα ασφαλιστήριο, μπορεί να διαφέρει μεταξύ ασφαλιστών.

Θα πρέπει επομένως να μελετήσετε καλά τις εξαιρέσεις, καθώς και τους ορισμούς και τις προϋποθέσεις παροχής της κάλυψης κατά την αξιολόγηση του συμβολαίου σας.

Πολλές εξαιρέσεις στην ασφάλιση στον κυβερνοχώρο είναι οι ίδιες με αυτές σε άλλα ασφαλιστήρια συμβόλαια, αλλά υπάρχουν επίσης ορισμένες που αφορούν ειδικά στην ασφάλιση αυτή, όπως:

1. εξαίρεση κάλυψης ζημίας που οφείλεται σε Σωματικές Βλάβες και Υλικές Ζημιές
2. εξαίρεση κάλυψης ζημίας που οφείλεται σε παραβίαση Πνευματικής Ιδιοκτησίας
3. εξαίρεση κάλυψης ζημίας που οφείλεται σε παράλειψη αποκατάστασης γνωστών αδυναμιών των συστημάτων της εταιρίας
4. εξαίρεση κάλυψης των απωλειών που προκύπτουν από κυβερνοπόλεμο και κυβερνοεπιθέσεις που μπορεί να συνδέονται με τις ενέργειες μιας συγκεκριμένης χώρας ή κυβέρνησης.

Αγορά ασφάλισης κατά κινδύνων του κυβερνοχώρου

Στην αγορά διατίθενται **ασφαλιστήρια** για **επιχειρήσεις μεγάλου μεγέθους**, με υψηλά ανώτατα ποσά αποζημιώσεων και ανάλογο κόστος, και **ασφαλιστήρια για όλα τα μεγέθη επιχειρήσεων**, με μικρότερα όρια αποζημίωσης και με ιδιαίτερα προσιτό κόστος.

Κατά τη διάρκεια της διαδικασίας συμπλήρωσης της αίτησης ασφάλισης θα σας ζητηθεί να απαντήσετε σε ποικίλες ερωτήσεις σχετικά με την επιχείρησή σας και τις πρακτικές ασφάλειας στον κυβερνοχώρο που ακολουθεί ο οργανισμός σας. Αυτές περιλαμβάνουν ερωτήσεις που είναι κοινές για όλους τους τύπους ασφάλισης, όπως πληροφορίες σχετικά με την επιχείρησή σας, τον κύκλο εργασιών, τους πελάτες, το ιστορικό ασφαλιστικών απαιτήσεων κ.α..

Ορισμένες ερωτήσεις που ενδέχεται να σας κάνουν οι ασφαλιστές κατά το στάδιο της αίτησης ασφάλισης αφορούν ειδικά στην ασφάλεια στον κυβερνοχώρο και μπορεί να περιλαμβάνουν:

1 Πολιτικές και διαδικασίες ασφάλειας στον κυβερνοχώρο

- Έχετε διορισμένο Υπεύθυνο Προστασίας Προσωπικών Δεδομένων ή Ασφάλειας Πληροφοριών;
- Χρησιμοποιείτε κρυπτογράφηση;
- Χρησιμοποιείτε και εφαρμόζετε έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA);
- Έχετε ασφαλή απομακρυσμένη πρόσβαση (διαδικασίες ελέγχου πρόσβασης για την αποτροπή μη εξουσιοδοτημένης πρόσβασης) στα συστήματα και το δίκτυό σας;
- Διαθέτετε λογισμικό προστασίας από ιούς και τείχος προστασίας (anti-virus & firewall software);
- Εφαρμόζετε τακτικά ενημερώσεις κώδικα σε κρίσιμα συστήματα και σε λογισμικό προστασίας από ιούς/τείχος προστασίας;

Έχετε ένα Σχέδιο Επιχειρηματικής Συνέχειας ή Αντιμετώπισης Καταστροφών που περιλαμβάνει επιθέσεις στον κυβερνοχώρο (π.χ. παραβιάσεις δεδομένων, παραβιάσεις ασφάλειας, άρνηση παροχής υπηρεσιών, ransomware); Έχει δοκιμαστεί το Σχέδιο τους τελευταίους 12 μήνες;

Διαθέτετε πιστοποιήσεις για την ασφάλεια στον κυβερνοχώρο, όπως το ISO 27001;

Έχετε βιώσει προηγούμενα περιστατικά στον κυβερνοχώρο;

Λαμβάνετε πρόσθετα μέτρα για τον εντοπισμό και την πρόληψη επιθέσεων ransomware;

Χρήση και αποθήκευση δεδομένων

2

Ποιος είναι ο συνολικός αριθμός εγγραφών προσωπικών δεδομένων που είναι αποθηκευμένος στις υποδομές σας;

Πραγματοποιείτε κρυπτογράφηση των ευαίσθητων/εμπιστευτικών πληροφοριών κατά την μετάδοση και την αποθήκευση;

Πόσες οικονομικές συναλλαγές μέσω καρτών επεξεργάζεστε ετησιώς;

Διατηρείτε αντίγραφα ασφαλείας των κρίσιμων δεδομένων τουλάχιστον σε εβδομαδιαία βάση;

Αντίγραφα ασφαλείας (Back Ups)

3

Είναι τα αντίγραφα ασφαλείας σας κρυπτογραφημένα;

Κρατάτε αντίγραφα ασφαλείας εκτός των υποδομών σας π.χ. εκτός δικτύου ή σε κάποια υπηρεσία cloud;

Συγχρονίζετε τα αντίγραφα ασφαλείας σας με κάποια υπηρεσία cloud (Dropbox, OneDrive, SharePoint, Google, κλπ);

Δοκιμάζετε την ακεραιότητα των αντιγράφων ασφαλείας πριν την επαναφορά δεδομένων για να πιστοποιήσετε πως δεν έχουν προσβληθεί από κάποιο κακόβουλο λογισμικό;

Πόσος χρόνος θα χρειαστεί για να επαναφέρετε πλήρως τα συστήματά σας από τα αντίγραφα ασφαλείας σας;

Χρήση Ιστοσελίδας

4

Έχετε ιστοσελίδα;

Ποια είναι η διεύθυνση URL του ιστότοπού σας;

Πόσα έσοδα έχετε από online δραστηριότητα;

Πληρωμές με κάρτα

5

Χρησιμοποιείτε πληρωμές με πιστωτικές κάρτα;

Αποθηκεύετε δεδομένα καρτών πληρωμών στα συστήματά σας;

Συμμορφώνεστε με το πιο πρόσφατο Πρότυπο Ασφάλειας Δεδομένων του κλάδου των καρτών πληρωμής;

Εξωτερική ανάθεση σε Τρίτους

6

Ποιες υπηρεσίες πληροφορικής/δεδομένων ανατίθενται σε τρίτους;

Τι έλεγχο δέουσας επιμέλειας κάνετε για αυτό;

Παρέχετε προσωπικά αναγνωρίσιμες, ευαίσθητες ή εμπιστευτικές πληροφορίες σε τρίτους;

Χρήσιμες συμβουλές για το πώς μπορείτε να ενισχύσετε την ανθεκτικότητα της επιχείρησής σας κατά κινδύνων του κυβερνοχώρου

Η ασφάλιση είναι μόνο ένα μέρος των προληπτικών μέτρων που πρέπει να λάβει ένας οργανισμός για να προστατευθεί.

Καθώς οι απειλές στον κυβερνοχώρο συνεχίζουν να εξελίσσονται είναι ζωτικής σημασίας η επιχείρησή σας να λάβει επιπλέον μέτρα για να ενισχύσει την ανθεκτικότητα και την ασφάλεια της κατά των κινδύνων του κυβερνοχώρου.

Υπάρχουν διάφορα βήματα που μπορεί να κάνει μία επιχείρηση για να βελτιώσει την ασφάλεια της στον κυβερνοχώρο. Πιο συγκεκριμένα:

1. Επενδύστε στην εκπαίδευση των εργαζομένων σας, η οποία πρέπει να «φρεσκάρεται» και να εμπλουτίζεται τακτικά.
   Μάθετε για τις απάτες phishing! Αποφύγετε το άνοιγμα ύποπτων email.

2. Χρησιμοποιήστε anti-virus και anti-malware λογισμικά.

3. Δημιουργήστε αντίγραφα ασφαλείας των σημαντικών δεδομένων σας. Είναι πολύ σημαντικό τα αντίγραφα ασφαλείας να είναι κρυπτογραφημένα.

4. Περιορίστε την πρόσβαση των υπαλλήλων σε δεδομένα και πληροφορίες και αποτρέψτε τη δυνατότητα εγκατάστασης λογισμικού.

5. Ενεργοποιήστε την ταυτοποίηση πολλαπλών παραγόντων (2FA/MFA) για τους λογαριασμούς cloud και απομακρυσμένης πρόσβασης. Η εφαρμογή της προβλέπει ότι ο χρήστης θα πρέπει να "ξεκλειδώσει" δύο ή περισσότερα πεδία ελέγχου και ταυτοποίησης - π.χ. βιομετρικό αποτύπωμα, κωδικός μιας χρήσης κ.τ.λ. - μοναδικές δηλαδή παραμέτρους ασφαλείας, προκειμένου να έχει πρόσβαση στον εταιρικό λογαριασμό του.

6. Διαχειριστείτε σωστά τις Ενημερώσεις Κώδικα (Good Patch Management). Η διαδικασία αυτή είναι ιδιαιτέρως χρήσιμη για τις ενημερώσεις κρίσιμης σημασίας ή τις τακτικές ενημερώσεις κώδικα, για την προγραμματισμένη χαρτογράφηση ευρετηρίου των λειτουργικών συστημάτων, για την καταγραφή των ελέγχων ασφαλείας (firewalls, antivirus software, τεχνολογίες EDR, κ.ο.κ.), για την κατηγοριοποίηση των κινδύνων, για την ιεράρχηση σημαντικών δεδομένων και για τον έλεγχο κι εφαρμογή ενημερώσεων σε τακτά χρονικά διαστήματα.

7. Δημιουργήστε ένα πλάνο επιχειρησιακής συνέχειας που να περιλαμβάνει την ανάκτηση των συστημάτων σε περίπτωση μιας καταστροφής.

Για περισσότερες πληροφορίες για την ασφάλιση κατά των κινδύνων του κυβερνοχώρου μπορείτε να απευθύνεστε στην ασφαλιστική εταιρία σας ή στον ασφαλιστικό διαμεσολαβητή σας.

Θα θέλαμε να σημειώσετε ότι όλες οι πληροφορίες που περιέχονται στον παρόντα Οδηγό είναι γενικής ενημερωτικής φύσεως και δεν τροποποιούν ή επηρεάζουν τους όρους, προϋποθέσεις & εξαιρέσεις οποιουδήποτε ασφαλιστηρίου συμβολαίου. Οι ασφαλιστικές καλύψεις διέπονται πάντα από τους όρους και τις συμφωνίες της εκάστοτε συναπτόμενης μεταξύ ασφαλιστή και ασφαλισμένου ασφαλιστικής σύμβασης.

ΕΝΩΣΗ
ΑΣΦΑΛΙΣΤΙΚΩΝ
ΕΤΑΙΡΙΩΝ
ΕΛΛΑΔΟΣ

CYBER INSURANCE

Ασφάλιση κατά των Κινδύνων Κυβερνοχώρου

www.eaee.gr