Ασφάλιση Cloud

Τι πρέπει να γνωρίζουν εταιρίες, Cloud Integrators & Cloud providers

Οι περισσότερες επιχειρήσεις σήμερα αξιοποιούν το cloud σε μικρότερο ή μεγαλύτερο βαθμό αναγνωρίζοντας τα πλεονεκτήματα που τους προσφέρει τόσο σε επίπεδο διαχείρισης πόρων, παραγωγικότητας των εργαζομένων αλλά και κόστους ανάπτυξης και συντήρησης. Ταυτόχρονα όμως προκύπτει ένα κρίσιμο ερώτημα: Πόσο ασφαλές είναι το cloud;

Η υπηρεσία **"cloud storage",** δηλαδή η τεχνολογία διαδικτυακής αποθήκευσης οποιασδήποτε μορφής πληροφορίας σε data centers ή server farms αποτελεί πλέον την συνήθη πρακτική ειδικά για τις μεγάλες εταιρίες οι οποίες χρησιμοποιούν την συγκεκριμένη πρακτική για να αποθηκεύουν και να επεξεργάζονται δεδομένα. Δεδομένης της πολυπλοκότητας της συγκεκριμένης πρακτικής, χρησιμοποιείται το **cloud integration** το οποίο είναι ένα σύστημα εργαλείων και τεχνολογιών που συνδέει τις απαραίτητες εφαρμογές παρέχοντας ένα πακέτο υπηρεσιών όπως μετατροπή δεδομένων, σχεδιασμό διεργασιών, αρχιτεκτονική και ρύθμιση εφαρμογών, πακέτα λογιστικής, διαχείριση αποθεμάτων, email, αποθήκευση αρχείων, επιχειρηματική ευφυΐα & ηλεκτρονικό εμπόριο, εκπαίδευση προσωπικού κλπ, ώστε να μπορέσουν οι επιχειρήσεις να ενσωματώσουν τις εφαρμογές λογισμικού τους χρησιμοποιώντας το cloud.

Ειδικά όσον αφορά το cloud storage, μια κοινή ερώτηση που δεχόμαστε στον τομέα της ασφάλισης διαδικτυακών κινδύνων είναι **πώς αυτό επηρεάζει τον κίνδυνο των συμβαλλόμενων μερών** (παρόχου και πελάτη) στον κυβερνοχώρο. Σε πολλές περιπτώσεις, οι εταιρείες μπορούν πραγματικά να βελτιώσουν την ασφάλειά τους με την πρακτική του cloud computing και την συνεργασία τους με τον cloud integrator, δεδομένης της εμπειρίας και εξειδίκευσης αυτών καθώς και των οικονομιών κλίμακας. Επίσης, θα πρέπει να λαμβάνεται υπόψη και ο **cloud provider** δηλαδή η εταιρία που έχει αναλάβει την διαδικτυακή αποθήκευση των δεδομένων και η οποία **συμβάλλεται με τον cloud integrator**.

Η **πρόκληση του cloud είναι ότι αποτελεί κοινή ευθύνη** μεταξύ των τριών παραπάνω εμπλεκόμενων μερών. Και οι τρείς πλευρές πρέπει να γνωρίζουν τις ευθύνες ασφαλείας τους για την αποτροπή παραβίασης καθώς μπορεί να μην είναι πάντα σαφές ποιος ευθύνεται όταν υπάρχει αστοχία ασφαλείας και π.χ. παραβίαση δεδομένων.

Παρότι πολλά ασφαλιστήρια συμβόλαια διαδικτυακών κινδύνων, περιλαμβάνουν στον ορισμό του «συστήματος υπολογιστών» τα δίκτυα τρίτων με τα οποία η ασφαλισμένη εταιρία έχει συνάψει σύμβαση για την υποστήριξη της, **εάν συμβεί παραβίαση θα προκύψουν ερωτήματα σχετικά με τον καταμερισμό ευθυνών**.

Η συνηθέστερη παρανόηση είναι ότι με την συγκεκριμένη σύμβαση **μεταβιβάζεται πλήρως η ευθύνη για παραβίαση δεδομένων τρίτων στον cloud provider ή στον cloud integrator**, ωστόσο η σχετική νομοθεσία προβλέπει ότι η ασφαλισμένη εταιρία δεν απαλλάσσεται από την ευθύνη της έναντι των υποκειμένων των δεδομένων (τρίτων) δεδο-

Κώστας Κωσταρέλος
Τεχνικός Διευθυντής Cromar Insurance Brokers LTD.

μένου ότι αυτή αρχικά συνέλλεξε τα προσωπικά δεδομένα και έχει τον ρόλο του '' υπεύθυνου επεξεργασίας''. Με την συνεργασία cloud computing η ευθύνη απλά επεκτείνεται, δεν μεταβιβάζεται.

Επίσης, είναι σύνηθες να **περιορίζεται συμβατικά η ευθύνη των cloud providers και cloud integrators** έως του ύψους του ποσού της σύμβασης που αναλαμβάνουν. Δεδομένου ότι οι ζημίες δεν περιορίζονται μόνο στο άμεσο κόστος περιορισμού της ζημίας κλπ. αλλά και σε άλλες πτυχές της παραβίασης π.χ. κόστος της απόκρισης σε ρυθμιστικές αρχές ή η αντιμετώπιση αγωγών πελατών κλπ. τέτοιας φύσης συμβατικοί περιορισμοί ουσιαστικά ΄΄επιστρέφουν'' την ευθύνη στον αρχικό πελάτη.

Είναι όμως σύνηθες στις διαπραγματεύσεις συνεργασίας να απαιτείται από τον πελάτη ανάληψη υψηλότερου ποσοστού ευθύνης δηλαδή η ασφαλισμένη εταιρία ακόμη και εάν διατηρεί σε ισχύ ασφαλιστήριο συμβόλαιο να ζητά από τον πάροχο cloud ή και τον could integrator να διατηρεί επίσης σε ισχύ ασφαλιστήριο συμβόλαιο με ψηλά όρια ευθύνης ώστε να είναι σε θέση να συνεισφέρει σε περίπτωση κάλυψης μίας ζημίας. Μία υψηλή απαλλαγή η ανεπαρκή όρια ευθύνης στο συμβόλαιο του πελάτη, θα μπορούσαν να καλυφθούν από το ασφαλιστήριο συμβόλαιο του παρόχου cloud ή του cloud integrator, με σχετική πρόβλεψη/απαίτηση. Είναι επίσης πιθανό να ζητείται από τον πελάτη πρόβλεψη κάλυψης και για την πιθανή απώλεια κερδών λόγω επίθεσης στον κυβερνοχώρο και επακόλουθη ζημία.

Τα τελευταία χρόνια οι ασφαλιστές στον κυβερνοχώρο επεκτείνουν σταθερά την κάλυψη διακοπών λειτουργίας από τις επιχειρήσεις στον κυβερνοχώρο για να συμπεριλάβουν τις πιθανές διακοπές λειτουργίας των προμηθευτών cloud, αλλά η συγκεκριμένη κάλυψη έχει αρχίσει να παρέχεται περιορισμένα και με αυστηρότερα κριτήρια και προϋποθέσεις.

Μία από τις **σημαντικές παρανοήσεις είναι ότι ένα ασφαλιστήριο συμβόλαιο διαδικτυακών κινδύνων είναι επαρκές για έναν cloud integrator**.

Η πεποίθηση αυτή είναι λανθασμένη και δυστυχώς αυτό αποδεικνύεται σε ενδεχόμενη ζημία και επακόλουθη απαίτηση από τον πελάτη. Μια αξίωση παραβίασης δεδομένων για έναν cloud integrator είναι πιθανότερο να σχετίζεται με την επαγγελματική ευθύνη του τελευταίου για αμέλεια κατά την εκτέλεση των συμφωνημένων υπηρεσιών όχι μόνο στην περίπτωση επικαλούμενου σφάλματος (από αμέλεια) στον σχεδιασμό αλλά και σε αυτή διαδικτυακής επίθεσης και απώλειας δεδομένων (πχ αδυναμία να διατηρήσει τα δεδομένα ασφαλή).

Για τον παραπάνω λόγο **το ορθό πλαίσιο ασφαλιστικής κάλυψης για τον cloud integrator είναι η συνδυαστική κάλυψη Επαγγελματικής Ευθύνης και διαδικτυακών κινδύνων** και δη με κοινό ασφαλιστήριο συμβόλαιο ώστε να αποφευχθεί οποιοδήποτε '' κενό '' ασφαλιστικής κάλυψης λόγω ύπαρξης δύο διαφορετικών συμβολαίων τα οποία συμπληρώνουν το ένα το άλλο.

Μία επίσης σημαντική επισήμανση αφορά την μελέτη των εκατέρωθεν συμβατικών υποχρεώσεων μίας **συμφωνίας συνεργασίας ώστε να διασφαλισθεί η ικανοποίηση των απαιτήσεων που αφορούν τις ασφαλιστικές καλύψεις του κάθε συμβαλλόμενου μέρους**. Η μελέτη από εξειδικευμένο ασφαλιστικό σύμβουλο θα πρέπει να συμπληρώνει την αντίστοιχη που πραγματοποιείται από τους νομικούς συμβούλους των εταιριών γιατί πρόκειται για δύο διαφορετικά πεδία γνώσης.

Η ερμηνεία που δίδεται από τον νομικό σύμβουλο δεν μπορεί και δεν πρέπει να αφορά και να υποκαθιστά την υλοποίηση των ασφαλιστικών υποχρεώσεων με τα κατάλληλα ασφαλιστήρια συμβόλαια, πρακτική την οποία γνωρίζει μόνο ένας έμπειρος ασφαλιστικός σύμβουλος.

Η **Cromar διατηρεί πρωταγωνιστικό ρόλο στις ασφαλίσεις διαδικτυακών κινδύνων** και διαθέτει μία πολύχρονη εμπειρία τόσο στην ερμηνεία και υλοποίηση των εκατέρωθεν ασφαλιστικών υποχρεώσεων, όσο και στην ασφάλιση των παραπάνω δραστηριοτήτων. Έχει τιμηθεί το βραβείο Lloyd's Market Innovation Award για την δημιουργία εκπαιδευτικής μηχανής σε διαγωνισμό καινοτομίας που διοργάνωσε η αγορά των Lloyd's για θέματα εκπαίδευσης, ιδιωτικότητας, διαχείρισης περιστατικών παραβίασης ασφαλείας και ασφάλισης Cyber Insurance.

Τα ασφαλιστικά προϊόντα τα οποία διαθέτουμε είναι μελετημένα ώστε να παρέχουν το απαιτούμενο πλαίσιο κάλυψης για την συγκεκριμένη δραστηριότητα, με σαφείς όρους και ανταγωνιστικό κόστος κάλυψης. Πιο συγκεκριμένα, διαθέτουμε το προϊόν **Mediatech**, το οποίο υποστηρίζεται από το συνδικά**το Beazley** των Lloyd's καθώς και το προϊόν **Tech and Media Technology** το οποίο υποστηρίζεται από την ελεύθερη αγορά του Λονδίνου, με τα δύο προϊόντα να συνδυάζουν την κάλυψη Επαγγελματικής ευθύνης με κάλυψη διαδικτυακών κινδύνων.

Επιπλέον το πρόγραμμα Tech and Media Technology παρέχει και τις καλύψεις Γενικής Αστικής Ευθύνης, Πυρός και Διακοπής Εργασιών ώστε να παρέχεται ένα ολοκληρωμένο πακέτο ασφαλιστικών καλύψεων για την εταιρία από ένα και μόνο ασφαλιστήριο συμβόλαιο. Και οι δύο ασφαλιστικές προτάσεις προσαρμόζονται ώστε να συνάδουν με τις εκάστοτε συμβατικές απαιτήσεις παρέχοντας ταυτόχρονα ένα ευρύ πλαίσιο ασφαλιστικών καλύψεων. ITSecurity