Cyber Insurance:
Εργαλείο διαχείρισης κινδύνου

Παραβιάσεις ηλεκτρονικών συστημάτων και διαρροές εμπιστευτικών πληροφοριών συμβαίνουν καθημερινά και οι εταιρείες πρέπει να είναι προετοιμασμένες για την αντιμετώπισή τους

» του **Νίκου Γεωργόπουλου,**
MBA, CyRM, Cyber Risks Advisor, Cromar Lloyds Coverholder

Οι παραβιάσεις ηλεκτρονικών συστημάτων και η διαρροή εμπιστευτικών πληροφοριών αποτελούν καθημερινό φαινόμενο. **Οι επιχειρήσεις χωρίζονται σε δύο κατηγορίες: σε αυτές που έχουν υποστεί παραβίαση συστημάτων και το γνωρίζουν και σε αυτές που θα αντιμετωπίσουν το πρόβλημα στο μέλλον.**
Η ασφαλιστική αγορά, ανταποκρινόμενη στις ανάγκες των επιχειρήσεων για οικονομική προστασία από τους κινδύνους που απειλούν τα συστήματά τους με παραβίαση και διαρροή εμπιστευτικών πληροφοριών, δημιούργησε προϊόντα και υπηρεσίες cyber insurance.

Τι είναι η παραβίαση συστημάτων και η απώλεια δεδομένων;

Παραβίαση συστημάτων μπορεί να συμβεί από μη εξουσιοδοτημένη πρόσβαση σε εταιρικά συστήματα, η οποία συνοδεύεται από **απώλεια δεδομένων πελατών** –που περιλαμβάνουν οικονομικά στοιχεία, στοιχεία πιστωτικών καρτών ή τραπεζικού λογαριασμού, δεδομένα υγείας– **ή εταιρικών δεδομένων**, όπως εμπορικά μυστικά ή ζητήματα πνευματικής ιδιοκτησίας.
Η απώλεια δεδομένων μπορεί να συντελεστεί και με την κλοπή συστημάτων αποθήκευσης δεδομένων, όπως usb, δίσκους αποθήκευσης ή πιο απλά από απροσεξία όταν κάποιο στέλεχος μιας εταιρείας ξεχάσει σε ένα αεροδρόμιο ένα tablet, ένα κινητό τηλέφωνο ή ένα laptop στο οποίο δεν έχει χρησιμοποιηθεί κάποιο πρόγραμμα για την κρυπτογράφηση των δεδομένων που περιέχει.
Η παραβίαση συστημάτων μπορεί να προκαλέσει και άρνηση παροχής υπηρεσίας (ddos) του δικτύου της εταιρείας, η οποία θα οδηγήσει σε διακοπή των εργασιών της και οικονομική ζημιά.

Ποιες είναι οι επιπτώσεις της παραβίασης συστημάτων και της απώλειας εμπιστευτικών πληροφοριών

Μέχρι σήμερα, η χρηματοοικονομική επίπτωση στις ευρωπαϊκές εταιρείες ήταν λιγότερο σοβαρή, διότι δεν ισχύει επί του παρόντος η νέα πανευρωπαϊκή νομοθεσία για την προστασία των δεδομένων. Σύμφωνα με τη νέα νομοθεσία, η οποία αναμένεται να ενσωματωθεί στο ευρωπαϊκό δίκαιο, οι εταιρείες που δεν κατάφεραν να διατηρήσουν την ασφάλεια των δεδομένων τους κινδυνεύουν με διοικητικά πρόστιμα για παραβίαση των κανόνων, που φθάνουν μέχρι 100 εκατ. ευρώ ή έως και 5% του ετήσιου παγκόσμιου κύκλου εργασιών της εταιρείας.
Ωστόσο, η χρηματοοικονομική επίπτωση θα μπορούσε να είναι το λιγότερο που θα μπορούσε να συμβεί σε σχέση με την απώλεια της εμπιστοσύνης των πελατών. Οι ασφαλισμένες εταιρείες θεωρούν ότι η υπ' αριθμόν ένα ανησυχία τους είναι η βλάβη της φήμης τους. Όπως περίφημα είπε ο Warren Buffett: «Χρειάζονται 20 χρόνια για να χτιστεί η φήμη και πέντε λεπτά για να καταστραφεί».
Ενδεικτικά το κόστος ανά χαμένο record και ανά κατηγορία επιχειρηματικής δραστηριότητας, σύμφωνα με τα στοιχεία του Ponemon Institute για παραβιάσεις δεδομένων στην Αμερική, φαίνεται στον παρακάτω πίνακα:

Πηγή 2015-Cost of Data Breach Study Global Analysis-Ponemon Institute Research Report

Η πρόληψη είναι αρκετή;

Παραβιάσεις ηλεκτρονικών συστημάτων και διαρροές εμπιστευτικών πληροφοριών συμβαίνουν καθημερινά και σε πολύ μεγάλη κλίμακα. Οι εταιρείες πρέπει να είναι προετοιμασμένες για την αντιμετώπιση συμβάντων παραβίασης δεδομένων. Οι μεγαλύτερες εταιρείες, αν και έχουν δημιουργήσει ειδικές ομάδες διαχείρισης κρίσης για την αντιμετώπιση αυτών των περιστατικών, μπορούν να αντιμετωπίσουν μεγάλες οικονομικές ζημίες, οι οποίες χωρίς την ύπαρξη ασφαλιστικής κάλυψης μπορούν να καταστούν καταστροφικές.

Οι μικρές και μεσαίες επιχειρήσεις πιθανόν να είναι λιγότερο προετοιμασμένες για την αντιμετώπιση περιστατικών παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών και δεν θα είναι σε θέση να απορροφήσουν το κόστος που συνδέεται με αυτά.

Πώς εξελίσσεται η ασφαλιστική αγορά;

Το μέγεθος της ασφαλιστικής αγοράς που αναπτύσσεται είναι πολύ μεγάλο, όπως αποδεικνύεται από την ανάπτυξη που παρουσιάζει η αγορά του cyber insurance στην Αμερική.

Η ανάπτυξη της αγοράς των ΗΠΑ είναι ένα ενδιαφέρον παράδειγμα του τι οδηγεί τη ζήτηση. Το πρώτο βήμα ήταν η υποχρεωτική ενημέρωση του πελάτη στην περίπτωση που έχουν χαθεί προσωπικά του δεδομένα και η γνωστοποίηση του περιστατικού στις αρμόδιες αρχές, η οποία ξεκίνησε στην Καλιφόρνια το 2003 και τώρα υπάρχει σε 48 πολιτείες. Η υποχρεωτική ενημέρωση των αρμοδίων αρχών και του πελάτη για κάθε παραβίαση δεδομένων, είτε μεγάλη είτε μικρή, ήταν αυτό που άλλαξε την αγορά.

Το εκτιμώμενο μέγεθος της ευρωπαϊκής αγοράς, σύμφωνα με τα στοιχεία της Advisen, είναι 224 εκατ. ευρώ για το 2015 και 426 εκατ. ευρώ για το 2016. Οι ευρωπαϊκές εταιρείες δεν φαίνεται να αντιλαμβάνονται τον κίνδυνο που διατρέχουν σε περίπτωση **παραβίασης ηλεκτρονικών συστημάτων και διαρροής εμπιστευτικών πληροφοριών**, ενώ οι ασφαλιστικές εταιρείες δεν έχουν μια ενιαία αντιμετώπιση απέναντι στον κίνδυνο, και οι μεσίτες ασφαλίσεων δεν έχουν τη γνώση που απαιτείται για την κατανόηση των κινδύνων και την εκπαίδευση των πελατών.

Η ευρωπαϊκή προσέγγιση της συγκεκριμένης αγοράς είναι περισσότερο συνδεδεμένη με την απώλεια κερδών μιας επιχείρησης σε περίπτωση διακοπής εργασιών λόγω στοχευμένων επιθέσεων άρνησης υπηρεσίας (ddos).

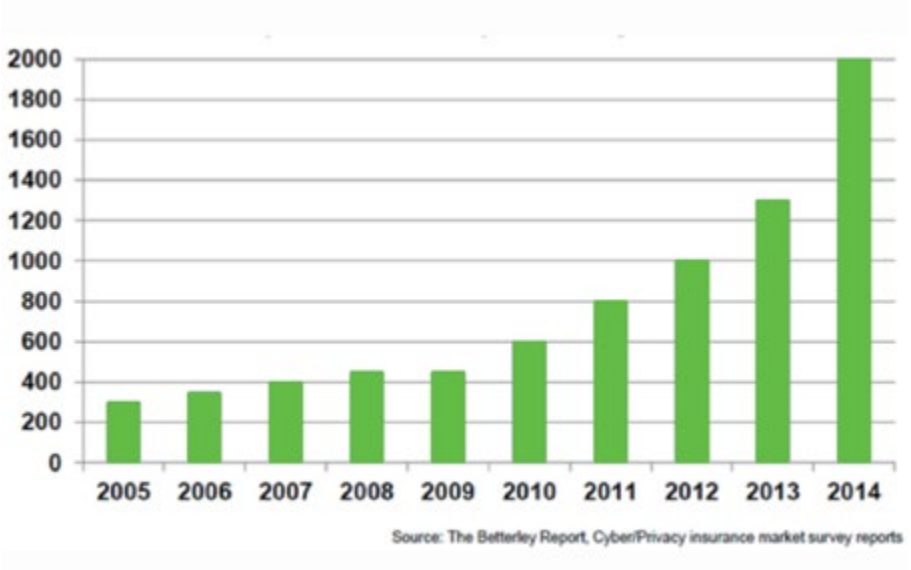
Η νέα νομοθεσία της Ευρωπαϊκής Ένωσης περί προστασίας προσωπικών δεδομένων, που πρόκειται να ενσωματωθεί στο ευρωπαϊκό δίκαιο, θα φέρει μαζί της εκτός από την αναγκαία ενημέρωση εντός 24 ωρών των Αρχών Προστασίας Προσωπικών Δεδομένων, την υποχρεωτική ενημέρωση των υποκειμένων των οποίων χάθηκαν τα προσωπικά δεδομένα, καθώς και διοικητικές κυρώσεις και πρόστιμα για τις εταιρείες που, λόγω εσφαλμένου χειρισμού τους, χάνουν δεδομένα.

Οι αλλαγές στη νομοθεσία θα μπορούσαν να αποτελέσουν καταλύτη αλλαγής της ευρωπαϊκής αγοράς του cyber insurance και να αυξήσουν σημαντικά το μέγεθός της, το οποίο μπορεί να φθάσει τα 780 εκατ. ευρώ το 2018 (Πηγή AGCS, Allianz).

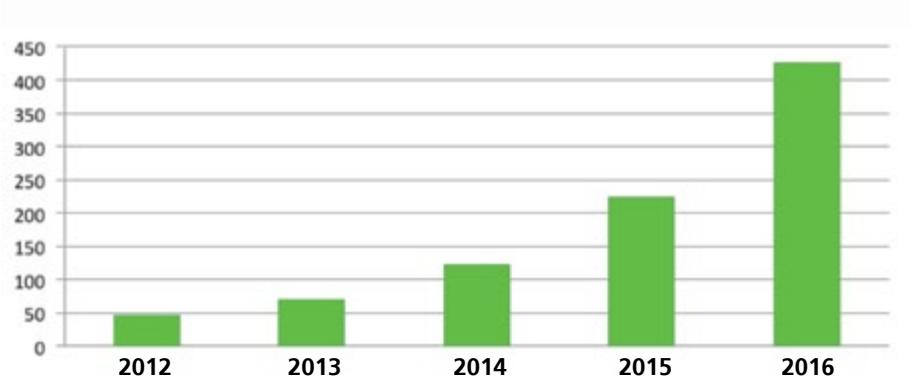
Πώς αναπτύχθηκαν τα ασφαλιστικά προϊόντα

Αρχικά, τα ασφαλιστικά προϊόντα που σχεδιάστηκαν κάλυπταν τις χρηματοοικονομικές ανάγκες των εταιρειών

Εξέλιξη αμερικανικής αγοράς Cyber Insurance (2005-2014)



Εξέλιξη ευρωπαϊκής αγοράς Cyber Insurance (2012-2016)



Πηγή: Advisen

σε περίπτωση παραβίασης συστημάτων και διαρροής δεδομένων.

Στη συνέχεια, και λαμβάνοντας υπόψη τις ανάγκες των εταιρειών-πελατών, δημιουργήθηκαν νέα καινοτόμα ασφαλιστικά προϊόντα, τα οποία ενσωμάτωσαν υπηρεσίες διαχείρισης συμβάντων σε συνεργασία με εγνωσμένης αξίας παρόχους υπηρεσιών ψηφιακής εγκληματολογίας, νομικούς και επικοινωνιολόγους, με σκοπό την αποτελεσματική διαχείριση των συμβάντων και τη μείωση των συνεπειών στην εταιρική φήμη.

Η προσέγγιση αυτή αποδείχθηκε πολύτιμη για τους πελάτες, ιδιαίτερα εκείνους που δεν έχουν εξελιγμένες ομάδες διαχείρισης κινδύνου. Οι υπηρεσίες διαχείρισης συμβάντων βοηθούν την εταιρεία να καθορίσει τι έχει παραβιαστεί, να αξιολογήσει τις ευθύνες της, να ενημερώσει τους σωστούς ανθρώπους και να κάνει ό,τι είναι απαραίτητο για να σταθεί στα πόδια της και πάλι.

Ποιοι παράγοντες επηρεάζουν το κόστος ασφάλισης και τη δυνατότητα ασφάλισης

Το κόστος των προϊόντων αυτών εξαρτάται από διάφορους παράγοντες, όπως: α) η δραστηριότητα της εταιρείας, β) το μέγεθος των εσόδων, γ) ο όγκος και ο τύπος των δεδομένων, δ) η εξάπλωση της εταιρείας διεθνώς, ε) η προηγούμενη εμπειρία σε περιπτώσεις data breach, στ) ο ανταγωνισμός και κατά πόσο ή όχι οι ασφαλιστές θεωρούν ότι ο ασφαλισμένος κίνδυνος είναι καλός ή κακός.

Η δυνατότητα ασφάλισης της εταιρείας εξαρτάται από τα μέτρα προστασίας που έχει λάβει και τις διαδικασίες και πολιτικές που ακολουθεί για την αποφυγή και την αντιμετώπιση περιστατικών παραβίασης συστημάτων και διαρροής δεδομένων.

Ένας άλλος σημαντικός παράγοντας που επηρεάζει τόσο το κόστος όσο και τη δυνατότητα ασφάλισης είναι η εμπειρία της ασφαλιστικής εταιρείας στην αντιμετώπιση περιστατικών.

Ποια εταιρεία είναι κατάλληλη για ασφάλιση;

Η ύπαρξη ενός Information Security Officer είναι καθοριστικός παράγοντας στη δημιουργία πολιτικών και διαδικασιών ασφάλειας, όπως και ενός πλάνου αντιμετώπισης αυτών των περιστατικών, αλλά και στην αξιολόγηση της προς ασφάλιση εταιρείας.

Οι ασφαλιστές αναζητούν εταιρείες οι οποίες κατανοούν τον κίνδυνο, κάνουν σωστή διαχείρισή του και έχουν τις κατάλληλες πολιτικές και διαδικασίες. Η διαχείριση της κατάστασης σε περίπτωση απώλειας δεδομένων είναι αρμοδιότητα των ανώτατων στελεχών και του διοικητικού συμβουλίου.

Σήμερα, δεν έχει τόση σημασία πόσο πολλά firewalls έχει μια εταιρεία ή πόσο καλά είναι τα συστήματά της, καθώς κανένα σύνολο ελέγχων δεν μπορεί να εγγυηθεί ότι δεν θα έχουν μια παραβίαση συστημάτων και απώλεια δεδομένων.

Τι μπορεί να κάνει η ασφαλιστική βιομηχανία για να βοηθήσει τις εταιρείες;

Η ασφαλιστική αγορά για την αποτελεσματική διαχείριση των οικονομικών συνεπειών των περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων προσφέρει την **κάλυψη των εξόδων διαχείρισης της κρίσης που προκαλεί ένα τέτοιο περιστατικό**, όπως: α) έξοδα για την πρόσληψη εξειδικευμένων ερευνητών ασφαλείας, β) έξοδα για την ενημέρωση των πελατών, γ) έξοδα δημοσίων σχέσεων και διαχείρισης κρίσης, δ) νομικά έξοδα για τη διαχείριση των κανονιστικών απαιτήσεων, ε) έξοδα νομικών συμβουλών για την αξιολόγηση των συνεπειών του περιστατικού, στ) έξοδα πρόσληψης ειδικών διαπραγματευτών σε περίπτωση εκβιασμού.

Επίσης **ασφαλίζει για την ευθύνη του ασφαλισμένου έναντι τρίτων**, οι οποίοι θα μπορούσαν να ασκήσουν αγωγή κατά του ασφαλισμένου για ζημία που μπορούν να υποστούν λόγω περιστατικών παραβίασης ηλεκτρο-

νικών συστημάτων και διαρροής προσωπικών τους δεδομένων **και την απώλεια κερδών σε περίπτωση άρνησης παροχής υπηρεσίας (ddos) λόγω κυβερνοεπιθέσεων.**

Η καινοτομία των νέων ασφαλιστικών προϊόντων προέρχεται από την παροχή υπηρεσιών διαχείρισης συμβάντων σε συνεργασία με εγνωσμένης αξίας παρόχους υπηρεσιών ψηφιακής εγκληματολογίας, νομικούς, επικοινωνιολόγους, με σκοπό την αποτελεσματική διαχείριση των συμβάντων και τη μείωση των συνεπειών στην εταιρική φήμη.

Παράγοντες που λαμβάνονται υπόψη στον σχεδιασμό ενός προγράμματος

Η ασφάλιση των οικονομικών συνεπειών μια εταιρείας σε περίπτωση παραβίασης συστημάτων και απώλειας δεδομένων δεν είναι μια συνηθισμένη κάλυψη. Η μη γνώση των κινδύνων, οι υπηρεσίες που παρέχονται και η διαχείριση τέτοιων συμβάντων απαιτεί εξειδικευμένους ασφαλιστικούς διαμεσολαβητές. Η σωστή αξιολόγηση των κινδύνων, η κατανόηση των ιδιαιτεροτήτων κάθε επιχείρησης σε μια περίπτωση παραβίασης συστημάτων και απώλειας δεδομένων, οι διαδικασίες που ακολουθεί και το ύψος της κάλυψης είναι ζωτικής σημασίας.

Για να σχεδιαστεί ένα πρόγραμμα που θα καλύπτει τις ανάγκες μιας εταιρείας θα πρέπει να σκεφτούμε τα ακόλουθα θέματα: α) ποιοι είναι οι κίνδυνοι, β) ποιες είναι οι υφιστάμενες ασφαλιστικές καλύψεις, γ) ποια είναι τα σωστά όρια και υποόρια του προγράμματος, δ) ποιες είναι οι εξαιρέσεις, ε) πώς καλύπτονται οι εταιρείες σε περίπτωση χρήσης εξωτερικών παρόχων, ζ) ποιες είναι οι διαδικασίες που ακολουθούν οι εταιρείες, στ) αν τα δεδομένα είναι κρυπτογραφημένα.

Τι προσφέρουμε στην ελληνική αγορά σαν λύση αντιμετώπισης περιστατικών παραβίασης συστημάτων και διαρροής δεδομένων

Η Cromar Insurance Brokers (www.cromar.gr), εξουσιοδοτημένος ανταποκριτής των Lloyds (Lloyds Coverholder), προσφέρει στην ελληνικη αγορά, σε συνεργασία με την Beazley, εταιρεία με μεγάλη εμπειρία στη διαχείριση περιστατικών data breach, η οποία έχει διαχειριστεί πάνω από 2.000 περιστατικά, με υψηλή αξιολόγηση (A Excellent, AM Best), το Beazley Global Breach Solution. Το Beazley Global Breach Solution, το οποίο αποτελεί μια συνολική λύση αποτελεσματικής διαχείρισης των κινδύνων παραβίασης συστημάτων και απώλειας δεδομένων και επιτρέπει στις επιχειρήσεις να διαχειριστούν την αυξανόμενη ευθύνη τους λόγω της διαχείρισης μεγάλου όγκου προσωπικών δεδομένων των πελατών τους, καθώς και να μετριάσουν τον κίνδυνο να θιγεί η εταιρική φήμη από μια πιθανή παραβίαση συστημάτων και απώλεια των δεδομένων αυτών.

Πώς μπορεί κάποιος να εμπλουτίσει τις γνώσεις του σε θέματα ασφάλισης και διαχείρισης περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων

Δημιουργήσαμε την πρώτη ελληνική κοινότητα συζήτησης περιστατικών data breach, στην οποία προσφέρουμε καθημερινή ενημέρωση μέσω του Cyber Risks Advisors Linkedin Group, το οποίο είναι group στο Linkedin. Η αποδοχή του συγκεκριμένου group είναι μεγάλη. Σε αυτό συμμετέχουν μέλη από όλο τον κόσμο και πολλοί Έλληνες που διαπρέπουν στο εξωτερικό σε τομείς που σχετίζονται με τη διαχείριση περιστατικών data breach. Άλλη μια καινοτομία μας είναι η δημιουργία του πρώτου ελληνικού website www.cyberinsurancegreece.com, το οποίο αποτελεί ένα εργαλείο ενημέρωσης και γνώσης για την αντιμετώπιση περιστατικών παραβίασης της ιδιωτικότητας.

Ποιες είναι οι πιο συχνές απαντήσεις μη ασφάλισης μιας εταιρείας

- Είμαστε ήδη ασφαλισμένοι για απώλεια δεδομένων από το συμβόλαιο γενικής αστικής ευθύνης
- Οι εργαζόμενοι της εταιρείας γνωρίζουν πώς πρέπει να προστατεύσουν τα δεδομένα και την εταιρεία
- Έχουμε το καλύτερο τμήμα μηχανογράφησης
- Το κόστος ανταπόκρισης σε ένα περιστατικό είναι πολύ μικρό
- Τα περισσότερα περιστατικά συμβαίνουν σε μεγάλες εταιρείες.

Νίκος Γεωργόπουλος
Cyber Risks Advisor CyRM, Cromar Insurance Brokers

Ο Νίκος Γεωργόπουλος είναι κάτοχος MBA από το ALBA Graduate Business School και πτυχίου Φυσικής του Πανεπιστημίου Πάτρας. Διαθέτει εργασιακή εμπειρία 22 ετών στον χρηματοοικονομικό τομέα (Xiosbank, Alpha Trust, Generali Hellas) στους τομείς Marketing, Πωλήσεων και Εναλλακτικών Δικτύων, είναι μέλος του International Association of Privacy Professionals και Πιστοποιημένος Cyber Insurance Risk Manager (CyRM). Είναι επίσης δημιουργός του "Cyber Risks Advisors" Linkedin Group, του www.privacyrisksadvisors.com και του www.cyberinsurancegreece.com