PROFESSIONAL
itsecurity
www.itsecuritypro.gr
Μάρτιος - Απρίλιος 2015 • Τεύχος 40 • Τιμή 5€

SMARTPRESS, ΜΑΓΕΡ 11, 104 38 ΑΘΗΝΑ
ΠΛΗΡΩΜΕΝΟ ΤΕΛΟΣ
Ταχ. Γραφείο ΚΕΜΠ.ΚΡ.
Αριθμός Άδειας 116
PRESS POST (X+7) PRESS POST
ΕΛΤΑ Hellenic Post
ΕΝΤΥΠΟ ΚΛΕΙΣΤΟ ΑΡ. ΑΔΕΙΑΣ 22/2008 ΚΕΜΠ.Α.ΚΡ.

GRC
Η αποτελεσματική υλοποίηση της διεργασίας

- Cyber Insurance ως εργαλείο Διαχείρισης Κινδύνου
- Internet of Everything for Defense

OTE
OTE Information Security
Ολοκληρωμένες υπηρεσίες ασφάλειας πληροφοριών στη διάθεση της INTERAMERICAN

Issue

Cyber Insurance ως εργαλείο Διαχείρισης Κινδύνου

Οι παραβιάσεις ηλεκτρονικών συστημάτων και η διαρροή εμπιστευτικών πληροφοριών είναι καθημερινό φαινόμενο το οποίο εκδηλώνεται στις μέρες μας με πολλούς τρόπους. Η συχνότητα του φαινομένου και οι επιπτώσεις του οδηγεί στη ζήτηση και την ανάπτυξη αντίστοιχων ασφαλιστικών προϊόντων.

Οι επιχειρήσεις χωρίζονται σε δύο κατηγορίες σε αυτές που εχουν υποστεί παραβίαση συστημάτων και το γνωρίζουν και σε αυτές που δεν το γνωρίζουν. Η παραβίαση συστημάτων και η κλοπή προσωπικών δεδομένων είναι ένα φαινόμενο που κάθε εταιρία που κατέχει δεδομένα πελατών ενδέχεται να βιώσει 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 μπορούμε να έχουμε 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 εταιρίας 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.

Σε πολλούς τομείς όπως το λιανικό εμπόριο, την υγειονομική περίθαλψη, τις τράπεζες και τη φιλοξενία, που κατέχουν σημαντικές ποσότητες προσωπικών δεδομένων, οι προσπά-

Νίκος Γεωργόπουλος
MBA, CyRM, Cyber Risks Advisor
Cromar Lloyds Coverholder

θειες παραβίασης των δεδομένων είναι ένας διαρκής κίνδυνος για την επιχειρηματική δραστηριότητα.

Τι ζημιά μπορεί να δημιουργήσει η παραβίαση συστημάτων και η απώλεια δεδομένων;

Μέχρι σήμερα, η χρηματοοικονομική επίπτωση στις ευρωπαϊκές Εταιρείες ήταν λιγότερο σοβαρή, διότι δεν ισχύει επί του παρόντος η πανευρωπαϊκή νομοθεσία για την προστασία των δεδομένων. Η νομοθεσία αυτή που παρουσιάστηκε τον Ιανουάριο του 2013 από την Επίτροπο Δικαιοσύνης της ΕΕ, κα Viviane Reding, προβλέπει την αναθεώρηση των νόμων περί προστασίας δεδομένων της ΕΕ και αναμένεται να ενσωματωθεί στο ευρωπαϊκό δίκαιο. Σύμφωνα με τη νέα νομοθεσία, οι εταιρίες που δεν κατάφεραν να διατηρήσουν την ασφάλεια των δεδομένων τους κινδυνεύουν με διοικητικά πρόστιμα για παραβίαση των κανόνων που φθάνουν μέχρι 100 εκ. € ή έως 5 % του ετήσιου παγκόσμιου κύκλου εργασιών της εταιρείας, όποιο από τα δύο είναι μεγαλύτερο. Ωστόσο, η Χρηματοοικονομική επίπτωση θα μπορούσε να είναι το λιγότερο από τις ανησυχίες μιας εταιρείας σε σχέση με την απώλεια της εμπιστοσύνης των πελατών. **Οι ασφαλισμένες εταιρίες θεωρούν ότι η υπ 'αριθμόν μία ανησυχία τους είναι βλάβη της φήμης τους.** 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 1**.

Πίνακας 1

Όπως περίφημα είπε ο Warren Buffett: «Χρειάζονται 20 χρόνια για να χτιστεί η φήμη και πέντε λεπτά για να καταστραφεί».

Σε μια μελέτη που πραγματοποιήθηκε από την Economist Intelligence Unit του περασμένου έτους, **το ένα τέταρτο των ερωτηθέντων ανέφερε ότι είχε πέσει θύμα της παραβίασης των δεδομένων κατά τα τελευταία δύο χρόνια**. Οι πελάτες /συνεργάτες των εταιριών αυτών δήλωσαν οτι δεν θα συνεργάζονταν ξανά με αυτες τις επιχειρήσεις που έχουν υποστεί παραβίαση συστημάτων και διαρροή προσωπικών δεδομένων.

Η Πρόληψη είναι αρκετή;

Παραβιάσεις ηλεκτρονικών συστημάτων και διαρροή 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 πιθανό να είναι λιγότερο προετοιμασμένες για την αντιμετώπιση περιστατικών παραβίασης συστημάτων και απωλειας εμπιστευτικών πληροφοριών και δεν θα είναι σε θέση να απορροφήσουν το κόστος που συνδέεται με αυτά.

Πώς ανταποκρίνεται η ασφαλιστική αγορά;

Η ανάπτυξη της αγοράς των ΗΠΑ είναι ένα ενδιαφέρον παράδειγμα του τι οδηγεί τη ζήτηση. Το πρώτο βήμα ήταν η υποχρεωτική ενημέρωση του πελάτη σε 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.**

Με την αποκάλυψη του συμβάντος κάθε εταιρία εκτέθηκε νομικά, και άρχισε να γίνεται εμφανές ότι η αντιμετώπιση παραβιάσεων δεδομένων ήταν τόσο πολύπλοκη όσο και δαπανηρή. Όλο αυτό έχει οδηγήσει τόσο τη ζήτηση όσο και την ανάπτυξη των ασφαλιστικών προϊόντων. Όταν οι κανόνες της ΕΕ αλλάξουν και η υποχρεωτική κοινοποίηση όλων των παραβιάσεων δεδομένων και τα διοικητικά πρόστιμα για εσφαλμένη διαχείριση των δεδομένων των πελατών γίνουν νόμος, αυτό θα αναγκάσει τις επιχειρήσεις να λάβουν σοβαρά υπόψη τους κινδύνους αυτούς. Επίσης, θα αυξήσει τη ζήτηση για αυτά τα προγράμματα και θα επηρεάσει την τιμή τους, τις παροχές και τους όρους προσφέρουν.

Πως αναπτύχθηκαν τα ασφαλιστικά προϊόντα

Αρχικά τα ασφαλιστικά προϊόντα που σχεδιάστηκαν κάλυπταν τις χρηματοοικονομικές ανάγκες των εταιριών σε περίπτωση παραβίασης συστημάτων και διαρροής δεδομένων.

Στην συνέχεια και λαμβάνοντας υπόψη τις ανάγκες των εταιριών πελατών δημιουργήθηκαν νέα ασφαλιστικά καινοτόμα προϊόντα τα οποία ενσωμάτωσαν υπηρεσίες διαχείρισης

Issue

συμβάντων σε συνεργασία με εγνωσμένης αξίας παρόχους υπηρεσιών ψηφιακής εγκληματολογίας, νομικούς, επικοινωνιολόγους με σκοπό την αποτελεσματική διαχείριση των συμβάντων και την 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 βοηθάνε την εταιρία να καθορίσει τι έχει παραβιαστεί, να αξιολογήσει τις ευθύνες της, να ενημερώσει τους σωστούς ανθρώπους και να γίνει ό, τι είναι απαραίτητο για να σταθεί η επιχείρηση και πάλι στα πόδια της και πάλι.

Ποιοι παράγοντες επηρεάζουν το κόστος ασφάλισης και την δυνατότητα ασφάλισης

Το κόστος των προϊόντων αυτών εξαρτάται από διάφορους παράγοντες όπως: α) η δραστηριότητα της εταιρίας β) το μέγεθος των εσόδων γ) ο όγκος και ο τύπος των δεδομένων δ) η εξάπλωση της εταιρίας 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 ασφάλιση της εταιρίας εξαρτάται απο τα μέτρα προστασίας που έχει λάβει και τις διαδικασίες και πολιτικές που ακολουθεί για την αποφυγή και 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 εταιρίας στην αντιμετώπιση περιστατικών.

Ποια εταιρία είναι κατάλληλη για ασφάλιση;

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

Οι ασφαλιστές αναζητούν εταιρίες οι οποίες κατανοούν τον κίνδυνο, κάνουν σωστή διαχείρισή του και έχουν εχουν τις κατάλληλες πολιτικές και διαδικασίες. **Η διαχείριση της κατάστασης σε περίπτωση απώλειας δεδομένων είναι αρμοδιότητα των ανωτάτων στελεχών και του διοικητικού συμβουλίου**. Σήμερα δεν έχει σημασία πόσο πολλά firewalls έχει μια εταιρεία, ή το πόσο καλά είναι τα συστήματά της, καθώς κανένα σύνολο ελέγχων δε μπορεί να εγγυηθεί ότι δεν θα έχουν μια παραβίαση συστημάτων και απώλεια δεδομένων.

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

Η ασφαλιστική αγορά για την αποτελεσματική διαχείριση των οικονομικών συνεπειών 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 πελατών γ) έξοδα δημοσίων σχέσεων και διαχείρισης κρίσης, δ) νομικά έξοδα για την διαχείριση των κανονιστικών απαιτήσεων ε) έξοδα νομικών συμβουλών για την αξιολόγηση των συνεπειών του περιστατικού στ) έξοδα πρόσληψης ειδικών διαπραγματευτών σε περίπτωση εκβιασμού και του κόστους απώλειας κερδών λόγω μη λειτουργίας των συστημάτων λόγω ddos.

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 παραβιάσεις ηλεκτρονικών συστημάτων και διαρροής προσωπικών τους δεδομένων **και την Απώλεια Κερδών σε περίπτωση άρνησης παροχής υπηρεσίας (ddos) λόγω κυβερνοεπιθεσεων**.

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 την μείωση των συνεπειών στην εταιρική φήμη.

Παράγοντες που λαμβάνονται υπόψη στον σχεδιασμό ενός προγράμματος

Η ασφάλιση των οικονομικών συνεπειών μια εταιρίας 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 διαμε-

σολαβητές. Οι εταιρίες πελάτες δεν έχουν την γνώση να διαχειριστούν μόνοι τους τα περιστατικά παραβίασης.
Η σωστή αξιολόγηση των κινδύνων, η κατανόηση των ιδιαιτεροτήτων κάθε επιχείρησης σε περίπτωση παραβίασης συστημάτων και απώλειας δεδομένων, οι διαδικασίες που ακολουθεί και το ύψος της κάλυψης είναι ζωτικής σημασίας. Η δημιουργία μιας ομάδας που αποτελείται από τον ασφαλιστή, τον μεσίτη και τεχνικούς εμπειρογνώμονες θα εξασφαλίσει ότι το πρόγραμμα που θα δημιουργηθεί θα καλύψει αποτελεσματικά τις ανάγκες της εταιρίας. Για να σχεδιαστεί ένα πρόγραμμα που θα καλύπτει τις ανάγκες μιας εταιρίας 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)πως καλύπτονται οι εταιρίες σε περίπτωση χρήσης εξωτερικών παρόχων ζ)ποιες οι διαδικασίες που ακολουθούν οι εταιρίες 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) , ανταποκριτής των Lloyds (Lloyds Coverholder), με 15 έτη συνεχούς παρουσίας στην ελληνική αγορά και δυνατότητα τοποθέτησης κινδύνων στην διεθνή αγορά προσφέρει σε συνεργασία με τους **Beazley, εταιρία με μεγάλη εμπειρία στην διαχείριση περιστατικών data breach, η οποία έχει διαχειριστεί άνω των 2.000 περιστατικών και υψηλή αξιολόγηση** προσφέρει στην ελληνικη αγορά 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 πιθανή παραβίαση συστημάτων και απώλειας των δεδομένων αυτών.

Πως μπορεί κάποιος να εμπλουτίσει τις γνώσεις του για 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 και συμμετέχουν μέλη από όλο τον κόσμο και πολλοί Ελληνες που διαπρέπουν στο εξωτερικό σε τομείς που σχετίζονται με την διαχείριση περιστατικών data breach.
Άλλη μια καινοτομία που κάναμε είναι η δημιουργία του www.privacyrisksadvisors.com το οποίο αποτελεί ένα εργαλείο ενημέρωσης και γνώσης αντιμετώπισης περιστατικών παραβίασης ιδιωτικότητας και αντιμετώπισής τους. Με την βοήθεια του **"The Data Breach Toolkit"** μπορείτε να υπολογίσετε το κόστος των οικονομικών συνεπειών σε περίπτωση παραβίασης συστημάτων και διαρροής δεδομένων, να βρείτε αναλύσεις για το κόστος των περιστατικών αυτών, το νομικό πλαίσιο που ισχύει σε όλο τον κόσμο και οδηγούς αντιμετώπισης αυτών των περιστατικών.
"Cyber Risks Academy" είναι μια ψηφιακή ακαδημία με παρουσιάσεις από ειδικούς για θέματα αντιμετώπισης περιστατικών παραβίασης συστημάτων και τρόπους ασφαλιστικής αντιμετώπισής τους.

Ποιες είναι οι ποιο συχνές απαντήσεις μη ασφάλισης μιας εταιρίας.

- Οι Οικονομικές συνέπειες παραβίασης συστημάτων και απώλειας δεδομένων καλύπτονται από το συμβόλαιο Γενικής Αστικής Ευθύνης.
- Οι εργαζόμενοι της εταιρίας γνωρίζουν πως 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 συμβαινουν σε μεγάλες εταιρίες iTSecurity

Νικος Γεωργόπουλος, Cyber Risks Advisor CyRM, Cromar Insurance Brokers

Ο Νίκος Γεωργόπουλος είναι κάτοχος Master in Business Administration (ALBA) και πτυχίου Φυσικής του Πανεπιστημίου Πάτρας. Διαθέτει 21 έτη εργασιακή εμπειρία στο χρηματοοικονομικό τομέα (XIOSBANK, Alpha Trust, Generali Hellas) στους τομείς Marketing, Πωλήσεων και Εναλλακτικών Δικτύων, είναι μέλος του International Association of Privacy Professionals και ειδικευμένος σύμβουλος στην παροχή ασφαλιστικών λύσεων Cyber /Privacy Liability & Data Breach Management. Είναι δημιουργός του "Cyber Risks Advisors" Linkedin Group και του www.privacyrisksadvisors.com.