Ο ρόλος του διευθύνοντος συμβούλου και των ανώτατων στελεχών σε περιστατικά παραβίασης εταιρικών συστημάτων ασφαλιστικών εταιρειών

Cyber Insurance Greece Bulletin

ΤΟΥ Νίκου Γεωργόπουλου

Cyber Risks Advisor, Ιούνιος 2015

Οι παραβιάσεις συστημάτων και η κυβερνοασφάλεια είναι μία πηγή ανησυχίας κάθε ασφαλιστικής εταιρείας, δεδομένης της φύσης των πληροφοριών που διαχειρίζεται. Όπως αποδεικνύεται από αρκετές πρόσφατες παραβιάσεις συστημάτων, το πώς ένας οργανισμός χειρίζεται μια κρίση παίζει σημαντικό ρόλο στο κατά πόσο ο διευθύνων σύμβουλος και τα ανώτατα στελέχη (CIO, COO, CMO, CRO, CFO κ.λπ.) παραμένουν στη θέση τους

Η πρόσβαση στον κυβερνοχώρο έχει δημιουργήσει νέες επιχειρηματικές ευκαιρίες για τις ασφαλιστικές εταιρείες γιατί προσφέρει δυνατότητα αποτελεσματικής επικοινωνίας με τον ασφαλιστικό διαμεσολαβητή, τον τελικό πελάτη, απλοποιεί τις διαδικασίες λειτουργίας τους και δίνει τη δυνατότητα πρόσβασης σε νέα τμήματα της αγοράς με προϊόντα και υπηρεσίες χαμηλότερου κόστους.

Αυτό άλλωστε είναι και το σημαντικότερο πλεονέκτημα από τη χρήση του κυβερνοχώρου. Όμως σε αυτόν δραστηριοποιούνται και κυβερνοεγκληματίες οι οποίοι έχουν στόχο να υποκλέψουν δεδομένα και εμπιστευτικές πληροφορίες που διατηρούν οι ασφαλιστικές εταιρείες όπως: οικονομικές εκθέσεις, μισθοδοσίες υπαλλήλων, βάσεις δεδομένων πελατών, κωδικούς πρόσβασης, εμπορικά μυστικά (π.χ., συμβάσεις συνεργασίας με παρόχους υπηρεσιών υγείας), σχέδια μάρκετινγκ, σχέδια δημιουργίας νέων προϊόντων και υπηρεσιών, συμβάσεις συνεργασίας με ασφαλιστικούς διαμεσολαβητές, δεδομένα υγείας των ασφαλισμένων, δεδομένα συνταξιοδοτικών προγραμμάτων, αριθμούς των πιστωτικών καρτών και τραπεζικών λογαριασμών, περιουσιακά στοιχεία πελάτη, προσωπικά οικονομικά στοιχεία πελατών.

Επίσης μπορούν να δημιουργηθούν προβλήματα στην ομαλή λειτουργία της ασφαλιστικής εταιρείας μέσω κυβερνοεπιθέσεων που οδηγούν σε άρνηση παροχής υπηρεσίας (DDos) των συστημάτων εξυπηρέτησης πελατών και διαμεσολαβητών και αλλοίωση της ποιότητας των δεδομένων της ασφαλιστικής εταιρείας.

Η χρήση του κυβερνοχώρου δημιουργεί σημαντικό λειτουργικό κίνδυνο στις ασφαλιστικές εταιρείες ο οποίος θα μπορούσε να εκφραστεί ως ποσοστό επί των ακαθάριστων εγγεγραμμένων ασφαλίστρων. Οι κίνδυνοι που συνδέονται με τη χρήση του κυβερνοχώρου (Cyber Risks) πρέπει να αντιμετωπιστούν όπως όλοι οι κίνδυνοι και μετά την ανάλυσή τους να αποφασιστεί τι ποσοστό μπορεί να αναλάβει η ασφαλιστική εταιρεία και τι ποσοστό θα μεταφερθεί σε εξειδικευμένους ασφαλιστές ή αντασφαλιστές.

Οι μηχανισμοί προστασίας των δεδομένων που εφαρμόζαμε μέχρι σήμερα μπορούν εύκολα να παρακαμφθούν ακόμη και από μια απροσεξία ενός εργαζόμενου που μπήκε σε μια μολυσμένη ιστοσελίδα ή απάντησε σε ένα e-mail phishing.

Τα αποτελέσματα μιας μελέτης που διεξήχθη το 2014 από την εταιρεία Corporate Board Member & FTI Consulting, Inc και έλαβαν μέρος σχεδόν 500 διευθυντές εταιρειών και μέλη διοικητικών συμβουλίων έδειξαν ότι οι κίνδυνοι του κυβερνοχώρου και η διαχείρισή τους αποτελεί μια από τις κορυφαίες ανησυχίες.

Τα μέλη του διοικητικού συμβουλίου και τα ανώτερα στελέχη πρέπει να δίνουν ύψιστη προτεραιότητα στην ασφάλεια στον κυβερνοχώρο και στην προστασία των δεδομένων της επιχείρησης.

Ο λόγος γι' αυτή την ανησυχία είναι ότι υπάρχουν πολλές επιχειρηματικές άμεσες και έμμεσες ζημιές που σχετίζονται με το έγκλημα στον κυβερνοχώρο και την απώλεια δεδομένων.

Άμεσες ζημιές οι οποίες περιλαμβάνουν επαγγελματικές αμοιβές εξειδικευμένων συμβούλων διαχείρισης περιστατικών παραβάσης συστημάτων, πρόστιμα και έξοδα όπως:

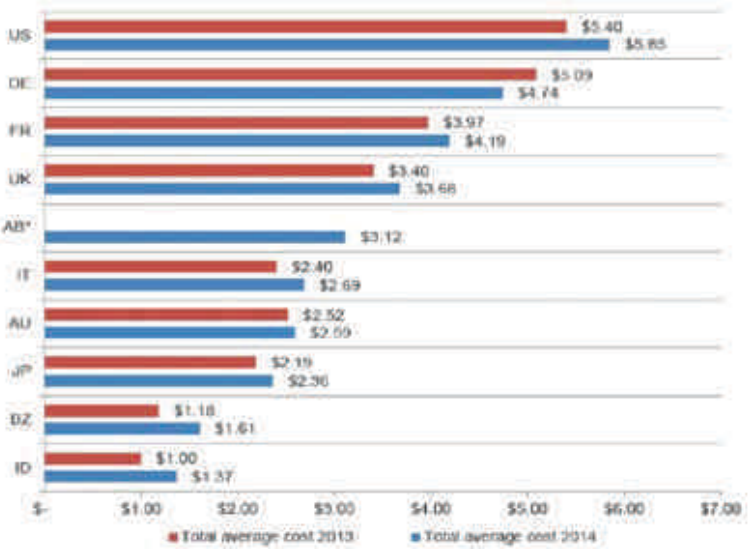
- αμοιβές εξειδικευμένου δικηγόρου
- υπηρεσίες ειδικών ψηφιακής εγκληματολογίας (forensics)
- υπηρεσίες δημοσίων σχέσεων και επικοινωνίας
- υπηρεσίες τηλεφωνικού κέντρου
- υπηρεσίες ελεγκτών
- Credit Monitoring – Υπηρεσία Παρακολούθησης χρήσης δεδομένων που έχουν κλαπεί για την πραγματοποίηση παράνομων χρηματοοικονομικών συναλλαγών
- έξοδα αντικατάστασης στοιχείων ενεργητικού
- αντικατάσταση της πιστωτικής κάρτας του πελάτη
- αντικατάσταση υλικού hardware ή software κ.λπ.
- έκτακτα έξοδα οπως:
- αναγκαία έξοδα ταξιδίου και διαμονής για ομάδες ειδικών διαχείρισης περιστατικών,
- τα έξοδα αποστολής, ενημερωτικών επιστολών σε πελάτες, κ.λπ.,
- Πρόστιμα για μη τήρηση της νομοθεσίας περί προσωπικών δεδομένων
- έξοδα για την επίτευξη επιχειρησιακής συνέχειας
- έξοδα εγκατάστασης νέων συστημάτων ασφάλειας

Οι Έμμεσες απώλειες μπορεί να είναι ακόμα πιο σημαντικές, συμπεριλαμβανομένων:

- μείωσης της φήμης της εταιρείας
- πτώσης των εσόδων
- χαμένων επιχειρηματικών ευκαιριών
- απώλεια πελατών
- απώλεια συνεργατών
- καθυστερήσεις έργων και λανσαρίσματος νέων προϊόντων
- αύξηση των αμοιβών των υπηρεσιών τρίτων παρόχων
- κόστη εκπαίδευσης και ευαισθητοποίησης σε θέματα ασφάλειας πληροφοριών του ανθρώπινου δυναμικού της εταιρείας
- επαναλαμβανόμενα έξοδα για τακτικούς ελέγχους ασφάλειας.

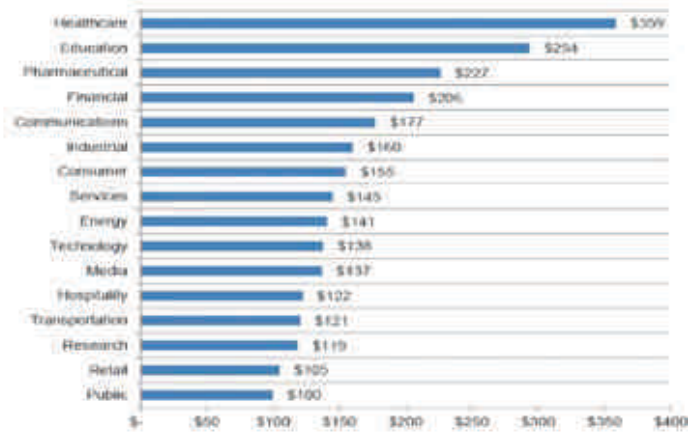
Δυστυχώς, πολλές από αυτές τις άμεσες και έμμεσες δαπάνες είναι απρογραμμάτιστες και δεν υπάρχουν προβλέψεις στον προϋπολογισμό. Τα περιστατικά παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών μπορεί να έχουν αρνητική επίπτωση στην ρευστότητα και τις ταμειακές ροές της ασφαλιστικής εταιρείας.

Το Ponemon Institute στο Report "2014 – Cost of Data Breach Study Global" αναφέρει ότι το μέσο κόστος της παραβίασης συστημάτων και απώλειας δεδομένων στην Αμερική ήταν 5,85 εκατ. δολάρια.



US: Ηνωμένες Πολιτείες, DE: Γερμανία, FR: Γαλλία, UK: Ηνωμένο Βασίλειο, AB: Αραβικά Εμιράτα, IT: Ιταλία, AU: Αυστραλία, JP: Ιαπωνία, BZ: Βραζιλία, ID: Ινδία.

Ο Νίκος Γεωργόπουλος είναι κάτοχος Master in Business Administration (ALBA) και πτυχίου Φυσικής του Πανεπιστημίου Πάτρας. Είναι μέλος του International Association of Privacy Professionals και εξειδικευμένος σύμβουλος στην παροχή ασφαλιστικών λύσεων Cyber / Privacy Liability & Data Breach Management και Πιστοποιημένος Cyber Insurance Risk Manager. Είναι δημιουργός του "Cyber Risks Advisors" Linkedin Group, του www.privacyrisksadvisors.com και του www.cyberinsurancegreece.com
Νίκος Γεωργόπουλος, MBA, CyRM.
Cyber Risk Advisor
CROMAR Coverholder at LLOYD´S
Email: nikos.georgopoulos@cromar.gr



Το κόστος απώλειας δεδομένων ανά record και ανά κατηγορία επιχειρηματικής δραστηριότητας σύμφωνα με τα στοιχεία της έρευνας του Ponemon institute στην Αμερική φαίνονται στο διάγραμμα που ακολουθεί.

Πηγή 2014 – Cost of Data Breach Study Global – Ponemon Institute Research Report

Για την αντιμετώπιση των χρηματοικονομικών επιπτώσεων, αποτελεσματικό εργαλείο διαχείρισης των περιστατικών παραβίασης αποτελεί η ασφάλιση Cyber Insurance, δίνοντας -εκτός από τις χρηματικές αποζημιώσεις- και πρόσβαση σε ομάδες ειδικών οι οποίες έχουν αντιμετωπίσει πλήθος περιστατικών.

Ενώ η ασφάλιση δεν μπορεί να αποτρέψει ένα περιστατικό παραβίασης, όπως αυτή της Sony που συνέβη πρόσφατα, μπορεί να βοηθήσει ελαχιστοποιώντας την οικονομική καταστροφή και τη βλάβη της φήμης που μπορεί να συντελεστεί σε σύντομο χρονικό διάστημα.

Πρέπει να τονιστεί ότι, με την εφαρμογή της προτεινόμενης ευρωπαϊκής νομοθεσίας για την προστασία των προσωπικών δεδομένων, θα έχουμε αύξηση των χρηματοοικονομικών επιπτώσεων. Η νομοθεσία αυτή που παρουσιάστηκε τον Ιανουάριο του 2013 από την Επίτροπο Δικαιοσύνης της Ε.Ε., κα Viviane Reding, προβλέπει την αναθεώρηση των νόμων περί προστασίας δεδομένων της Ε.Ε. και αναμένεται να ενσωματωθεί στο ευρωπαϊκό δίκαιο. Πριν από μερικές ημέρες οριστικοποιήθηκε και αναμένεται η τελική έγκρισή της εντός του 2015.

Σύμφωνα με τη νέα νομοθεσία, οι εταιρείες που δεν θα καταφέρουν να διατηρήσουν την ασφάλεια των δεδομένων τους κινδυνεύουν με διοικητικά πρόστιμα για παραβίαση των κανόνων που φθάνουν μέχρι 100 εκατ. ευρώ ή έως 2 % του ετήσιου παγκόσμιου κύκλου εργασιών της εταιρείας, όποιο από τα δύο είναι μεγαλύτερο.

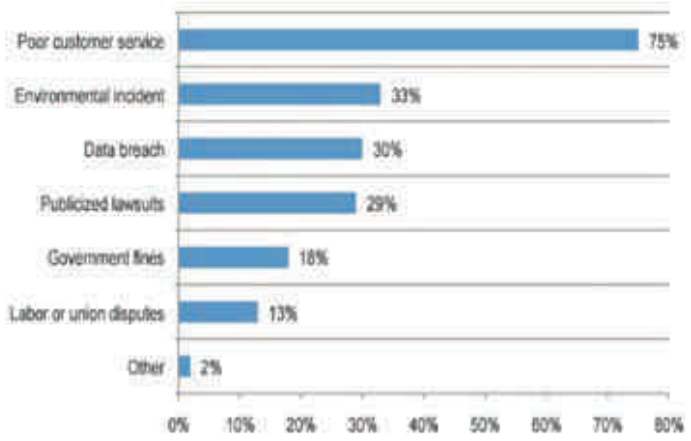
Ένα ακόμη μεγάλο πρόβλημα που έχει να αντιμετωπίσει ένας διευθύνων σύμβουλος είναι η βλάβη που μπορεί να υποστεί η φήμη της εταιρείας του.

Όπως είπε περίφημα ο Warren Buffett:

"Χρειάζονται 20 χρόνια για να χτιστεί η φήμη μιας εταιρείας και μόνο πέντε λεπτά για να καταστραφεί."

Σε μελέτη του Ponemon Institute το 2014 διαπιστώθηκε ότι οι παραβιάσεις συστημάτων και η διαρροή εμπιστευτικών πληροφοριών είναι από τα τρία κορυφαία περιστατικά που μπορούν να επηρεάσουν τη φήμη της εταιρείας και σε συνδυασμό με την κακή εξυπηρέτηση πελάτων και την πολιτική προστασίας του περιβάλλοντος που ακολουθεί να οδηγήσουν σε απώλεια πελατών.

Παράγοντες που επηρεάζουν την εταιρική φήμη



Πηγή: The Aftermath of a data breach Consumer Sentiment. Ponemon Institute Report

Δυστυχώς, υπάρχουν αρκετά παραδείγματα παραβιάσεων συστημάτων επιχειρήσεων που δεν ήταν επαρκώς προετοιμασμένες και δεν κατάφεραν να διαχειριστούν αποτελεσματικά τα εκδηλωθέντα περιστατικά.

Το μεγαλύτερο λάθος που κάνουν οι εταιρείες στην αντιμετώπιση αυτών των περιστατικών είναι ότι δεν έχουν προετοιμάσει την επικοινωνιακή στρατηγική τους. Θεωρούν δεδομένο ότι μπορούν να αντιμετωπίσουν μια κρίση που μπορεί να προέλθει από περιστατικά παραβίασης συστημάτων γιατί έχουν την καλύτερη ομάδα IT. Ακόμα χειρότερα γιατί θεωρούν οτι μπορούν να χειριστούν την κρίση την στιγμή που συμβαίνει χωρίς προηγούμενη προετοιμασία.

Οι ασφαλιστικές εταιρείες θα πρέπει να είναι προετοιμασμένες για κάθε πιθανή κατάσταση. Δεν έχει σημασία πόσο μακρινό φαίνεται αυτό το ενδεχόμενο. Ο σχεδιασμός της αντιμετώπισης της κρίσης μετά την εκδήλωσή της και χωρίς καμία αρχική πρετοιμασία οδηγεί σε σφάλματα που οφείλονται σε ανακριβείς πληροφορίες, πανικό, και μη σωστό καθορισμό προτεραιοτήτων.

Αυτό που παρατηρείται επίσης είναι ότι οι εταιρείες είτε ανταποκρίνονται πολύ γρήγορα σε μια κρίση, ή πολύ αργά. Ο συγχρονισμός είναι ζωτικής σημασίας για την αντιμετώπιση της κρίσης.

Αν για το περιστατικό παραβίασης βγει κάποια ανακοίνωση πολύ γρήγορα, ίσως να μη γνωρίζουμε την πλήρη έκταση της ζημίας, κατι που σε δεύτερο χρόνο θα μας αναγκάσει πιθανόν να την αναθεωρήσουμε. Αν αυτό γίνει πάρα πολύ αργά, θα φαίνεται ότι προσπαθούμε να αποφύγουμε την ευθύνη και λόγω αυτής της καθυστέρησης και οι πελάτες της εταιρείας μπορούν να επηρεαστούν περισσότερο από το περιστατικό.

Οι δημόσιες σχέσεις μπορούν να μετριάσουν σημαντικά τη ζημιά σε μια κατάσταση κρίσης. Η μη άμεση ανταπόκριση μπορεί να ενισχύσει την κατάσταση και να προκαλέσει πρόσθετη ζημία σε μια εταιρεία σε μια κατάσταση κρίσης. Πάντοτε πρέπει να έχουμε ένα σχέδιο αντιμετώπισης τέτοιων περιστατικών.

Για το λόγο αυτό θα πρέπει σε κάθε εταιρεία να έχει δημιουργηθεί μια Ομάδα Διαχείρισης Περιστατικών Παραβίασης Συστημάτων η οποία αποτελείται από ανώτατα στελέχη της εταιρείας από τα τμήματα:

- Information Security
- IT
- Νομικής υπηρεσίας
- Κανονιστικής Συμμόρφωσης
- Δημοσίων Σχέσεων & Επικοινωνίας
- Εξυπηρέτησης Πελατών
- Οικονομικής Διεύθυνσης
- Business Continuity
- Risk Management
- HR
- Marketing

και εξειδικευμένους εξωτερικούς συμβούλους όπως: δικηγόρους, επικοινωνιολόγους, ερευνητές ψηφιακής εγκληματολογίας.

Η ομάδα πρέπει να συνεδριάζει σε τακτικά χρονικά διαστήματα και να εκπονεί ασκήσεις προσομοίωσης διάφορων σεναρίων ώστε τα μέλη της να είναι σε ετοιμότητα για την αντιμετώπιση περιστατικών.

Η ομάδα αυτή πρέπει να συντονίζεται από τον Cyber Breach Coach ο οποίος θα φροντίζει για τη συνεχή ετοιμότητά της και θα δίνει την κατάλληλη πληροφόρηση στον διευθύνοντα σύμβουλο κατά την εξέλιξη ενός περιστατικού παραβίασης. Όταν συμβεί παραβίαση συστημάτων και διαρροή δεδομένων, θα πρέπει να παρθούν γρήγορα αποφάσεις και πολλές φορές ακόμα και χωρίς δυνατότητα αναίρεσης. Σε πολλές περιπτώσεις οι αποφάσεις αυτές πρέπει να παρθούν χωρίς τα στελέχη της εταιρείας να έχουν στη διάθεσή τους όλη τη σχετική πληροφόρηση.

Περιστατικά παραβίασης συστημάτων και απώλειας δεδομένων καταγράφονται καθημερινά σε ασφαλιστικές εταιρείες όπως η Anthem από την οποία χάθηκαν 80 εκατ. records και οι μέχρι σήμερα εκτιμήσεις ορίζουν το κόστος αντιμετώπισης του περιστατικού αυτού σε 100 εκατ. δολάρια. Η εταιρεία είχε ασφαλιστήριο συμβόλαιο και ένα τμήμα του κόστους θα αντιμετωπιστεί, το υπόλοιπο θα επιβαρύνει τον ισολογισμό της εταιρείας.

Ασφαλιστικές εταιρείες που εχουν υποστεί data breach

Η ασφάλιση Cyber Insurance δίνει, εκτός από τις χρηματικές αποζημιώσεις, πρόσβαση σε ομάδες ειδικών (δικηγόροι, επικοινωνιολόγοι, forensics investigators κ.λπ.) οι οποίες έχουν αντιμετωπίσει πλήθος περιστατικών και μπορούν, σε συνεργασία με την Ομάδα Διαχείρισης Περιστατικών Παραβίασης της εταιρείας, να διαχειριστούν αποτελεσματικά τα περιστατικά παραβίασης, να περιορίσουν τις χρηματοοινομικές επιπτώσεις τους και να προστατεύσουν την εταιρική φήμη. Η ασφάλιση Cyber Insurance αποτελεί ένα αποτελεσματικό εργαλείο αντιστάθμισης κινδύνου.

Σε κάθε περίπτωση, ο διευθύνων σύμβουλος, για την αντιμετώπιση αυτών των περιστατικών, θα πρέπει να έχει στη διάθεσή του τη μέγιστη δυνατή και ακριβή πληροφόρηση για το περιστατικό. Είναι αναγκαίο ο διευθύνων σύμβουλος να έχει πλήρη εικόνα: για τις πληροφορίες που συλλέγει και επεξεργάζεται η εταιρεία του, για τις ευθύνες που έχει σε περίπτωση περιστατικού παραβίασης συστημάτων, για τα συστήματα και τις υποδομές της και μια Εκπαιδευμένη Ομάδα Αντιμετώπισης & Διαχείρισης Περιστατικών Παραβίασης Συστημάτων στη διάθεσή του.