Η ασφάλεια των πληροφοριών αποτελεί ευθύνη του διευθύνοντος συμβούλου και των ανώτατων στελεχών

Το κόστος των κυβερνοεπιθέσεων που θα δεχθούν επιχειρήσεις και οργανισμοί την επόμενη δεκαετία (2015-2025) ανέρχεται σε 1.06 δισ. δολ. του εκτιμώμενου ΑΕΠ της Ελλάδας.

από τον
Νίκο Γεωργόπουλο
MBA, CyRM, Cyber Risk Advisor-Cromar Coverholder at Lloyd's

Οι παραβιάσεις συστημάτων και η κυβερνοασφάλεια αποτελούν πηγή ανησυχίας για κάθε εταιρεία, δεδομένης της φύσης των πληροφοριών που διαχειρίζεται. Όπως αποδεικνύεται από 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 εταιρείες, γιατί προσφέρει τη δυνατότητα της αποτελεσματικής επικοινωνίας με τα δίκτυα διανομής και τον τελικό πελάτη, απλοποιεί τις διαδικασίες λειτουργίας τους και προσφέρει τη δυνατότητα της 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 εταιρείες, όπως οικονομικές εκθέσεις, μισθοδοσίες υπαλλήλων, βάσεις δεδομένων πελατών, κωδικούς πρόσβασης, εμπορικά μυστικά, σχέδια του μάρκετινγκ, σχέδια δημιουργίας νέων προϊόντων και υπηρεσιών, συμβάσεις συνεργασίας με τα δίκτυα διανομής, δεδομένα υγείας, αριθμούς πιστωτικών καρτών και τραπεζικών λογαριασμών, περιουσιακά και προσωπικά οικονομικά στοιχεία πελατών.

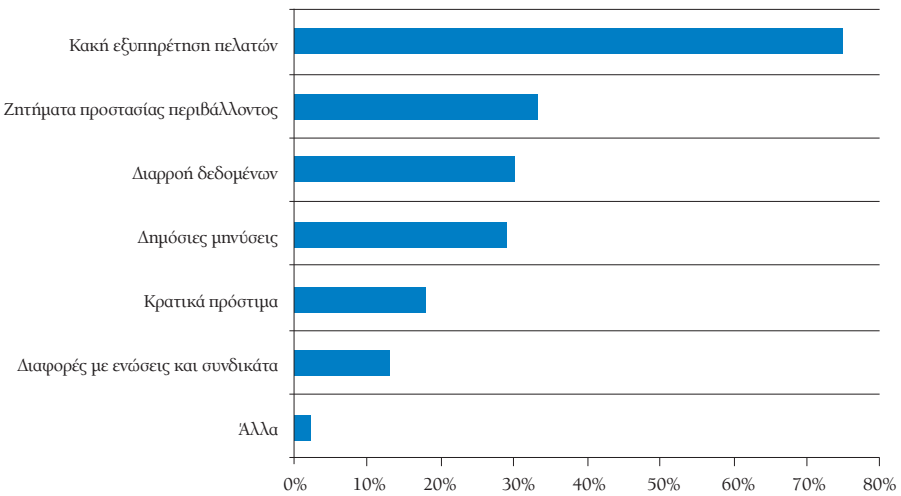
Επίσης, μπορεί να δημιουργηθούν προβλήματα στην ομαλή λειτουργία και διαθεσιμότητα των συστημάτων της ασφαλιστικής εταιρείας μέσω των κυβερνοεπιθέσεων που οδηγούν σε άρνηση παροχής υπηρεσίας (DDoS) των συστημάτων εξυπηρέτησης και αλλοίωση της ποιότητας των δεδομένων της εταιρείας.

Η χρήση του κυβερνοχώρου δημιουργεί έναν σημαντικό λειτουργικό κίνδυνο στις εταιρείες, για τη διαχείριση του οποίου, εκτός από τις λύσεις που προσφέρει η τεχνολογία, οι πολιτικές ασφαλείας και οι διαδικασίες που ακολουθεί κάθε εταιρεία, απαραίτητο εργαλείο είναι η ασφάλιση.

Με την εφαρμογή της νέας ευρωπαϊκής νομοθεσίας για την προστασία των προσωπικών δεδομένων, οι εταιρείες που δεν θα καταφέρουν να διατηρήσουν την ασφάλεια των δεδομένων τους κινδυνεύουν με διοικητικά πρόστιμα για παραβίαση των κανόνων, που φθάνουν έως το 2% του ετήσιου παγκόσμιου κύκλου εργασιών της εταιρείας.

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

ΠΑΡΑΓΟΝΤΕΣ ΠΟΥ ΕΠΗΡΕΑΖΟΥΝ ΤΗΝ ΕΤΑΙΡΙΚΗ ΦΗΜΗ

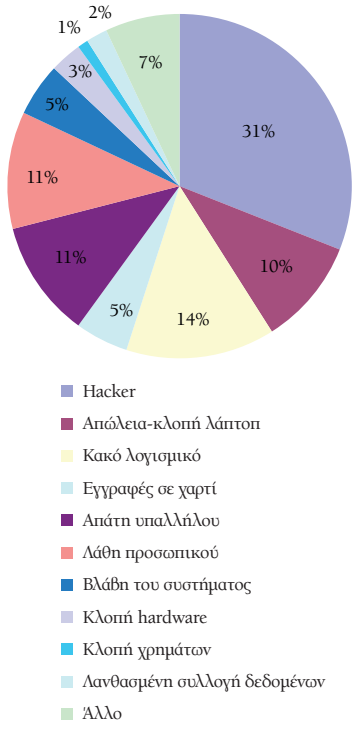


Πηγή: The Aftermath of a data breach Consumer Sentiment. Ponemon Institute Report.

Αντιμέτωπες με διοικητικά πρόστιμα για παραβίαση των κανόνων, που φθάνουν έως το 2% του ετήσιου παγκόσμιου κύκλου εργασιών τους, βρίσκονται οι εταιρείες.

Επίσης, στη μελέτη της NetDiligence, "Cyber Claims Study 2015", μπορούμε να δούμε από περιστατικά παραβίασης συστημάτων ασφαλισμένων αμερικανικών εταιρειών την κατανομή των αιτίων που οδήγησαν σε παραβίαση των συστημάτων και απώλεια εμπιστευτικών πληροφοριών.

Πιο αναλυτικά, το 31% οφείλεται σε hacking, το 10% σε απώλεια εταιρικών συσκευών που περιέχουν εταιρικά δεδομένα (tablets, κινητά τηλέφωνα), το 14% σε malware/virus, το 11% σε περιστατικά κακόβουλων εργαζομένων, το 11% σε λάθη εργαζομένων, το 5% σε προβλήματα συστημάτων, το 3% σε κλοπή hardware (δίσκοι backup, usb), το 1% σε κλοπή χρημάτων και το 7% σε διάφορους παράγοντες.



Πηγή: NetDiligence "Cyber Claims Study 2015"

Ειδικότερα για την Ελλάδα, σύμφωνα με μελέτη που εκπόνησε η αγορά των Lloyd's, σε συνεργασία με το Κέντρο Μελετών Κινδύνων του Πανεπιστημίου του Κέιμπριτζ, το κόστος των κυβερνοεπιθέσεων που θα δεχθούν επιχειρήσεις και οργανισμοί την επόμενη δεκαετία (2015-2025) ανέρχεται στο 1.06 δισ. δολ. του εκτιμώμενου ΑΕΠ της Ελλάδας, το οποίο υπολείπεται ελάχιστα του 1.07 δισ. δολ. του εκτιμώμενου ΑΕΠ που βρίσκεται σε κίνδυνο λόγω σεισμού.

Για την αντιμετώπιση των επιπτώσεων ενός περιστατικού παραβίασης (data breach) αποτελεσματικό εργαλείο διαχείρισης αποτελεί η ασφάλιση Cyber Insurance, η οποία, εκτός από τις χρηματικές αποζημιώσεις, προσφέρει πρόσβαση σε ομάδα ειδικών (δικηγόρους, επικοινωνιολόγους, forensic investigators κ.λπ.) οι οποίοι έχουν αντιμετωπίσει πλήθος περιστατικών και μπορούν, σε συνεργασία με την Ομάδα Διαχείρισης Περιστατικών Παραβίασης Συστημάτων της εταιρείας, να διαχειριστούν αποτελεσματικά τα περιστατικά παραβίασης, να περιορίσουν τις χρηματοοικονομικές επιπτώσεις τους και να προστατεύσουν την εταιρική φήμη.

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 να έχει πλήρη εικόνα για τις πληροφορίες που συλλέγει και επεξεργάζεται η εταιρεία του, για τις ευθύνες που έχει στην περίπτωση ενός περιστατικού παραβίασης συστημάτων, για τα συστήματα και τις υποδομές της εταιρείας. Επίσης, πρέπει να έχει στη διάθεσή του και μια Εκπαιδευμένη Ομάδα Αντιμετώπισης & Διαχείρισης Περιστατικών Παραβίασης Συστημάτων, η οποία, συνεργαζόμενη με την ασφαλιστική εταιρεία που προσφέρει την ασφάλιση Cyber Insurance, να μπορεί να διαχειριστεί αποτελεσματικά τα περιστατικά παραβίασης, περιορίζοντας τις χρηματοοικονομικές επιπτώσεις και προστατεύοντας τη φήμη της εταιρείας του.

Λαμβάνοντας υπόψη τις ανάγκες των επιχειρήσεων, η Beazley δημιούργησε το Beazley Global Breach Solution, το οποίο αποτελεί μια συνολική λύση αποτελεσματικής διαχείρισης των κινδύνων παραβίασης συστημάτων και απώλειας δεδομένων, που επιτρέπει στις επιχειρήσεις να διαχειριστούν περιστατικά παραβίασης συστημάτων και να μετριάσουν τον κίνδυνο να θιγεί η εταιρική τους φήμη. Προσφέρεται στην Ελλάδα από την Cromar.

Το Beazley Global Breach Solution προσφέρει, εκτός από την κάλυψη των χρηματοοικονομικών επιπτώσεων της εταιρείας, και πρόσβαση στην Ομάδα Διαχείρισης Περιστατικών, η οποία βραβεύθηκε από την Advisen ως η καλύτερη ομάδα για το 2015, και έχει αντιμετωπίσει πάνω από 2.000 περιστατικά παγκοσμίως.