ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Περιστατικά παραβίασης δεδομένων και η σχέση τους με το ανθρώπινο λάθος

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Χατζούλα Ελένη

Επιβλέπουσα : Αναπληρώτρια Καθηγήτρια, Καρύδα Μαρία

Μέλη εξεταστικής επιτροπής: Καθηγήτρια, Μήτρου Λίλιαν
Καθηγητής, Κοκολάκης Σπύρος

Σάμος, Φεβρουάριος 2020

Πρόλογος και ευχαριστίες

Η παρούσα μεταπτυχιακή εργασία εκπονήθηκε στα πλαίσια του Μεταπτυχιακού Προγράμματος Σπουδών «Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων», του Τμήματος Μηχανικών, Πληροφοριακών και Επικοινωνιακών Συστημάτων, του Πανεπιστημίου Αιγαίου. Πριν την παρουσίαση των αποτελεσμάτων της παρούσας διπλωματικής εργασίας, αισθάνομαι την υποχρέωση να ευχαριστήσω ορισμένους από τους ανθρώπους που γνώρισα, συνεργάστηκα μαζί τους και συνέβαλαν στην πραγματοποίηση της.

Αρχικά, θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτρια μου Μαρία Καρύδα για την καθοδήγηση και την εμπιστοσύνη που μου έδειξε, μαζί με το καλό κλίμα συνεργασίας που έπαιξε σημαντικό ρόλο στην πραγματοποίηση της παρούσας διπλωματικής εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω τους συμφοιτητές μου για την ευχάριστη παρέα και τις ενδιαφέρουσες συζητήσεις που είχαμε.

Πάνω από όλα οφείλω να ευχαριστήσω τους γονείς μου, την αδερφή μου, την οικογένεια μου και τους φίλους μου για την κατανόηση, την υπομονή και την στήριξη τους σε όλο αυτό το χρονικό διάστημα.

Πίνακας περιεχομένων

Περίληψη

Η παρούσα διπλωματική εργασία ασχολείται με την συγκέντρωση περιστατικών παραβίασης δεδομένων και τη συσχέτιση τους με το ανθρώπινο λάθος. Ο στόχος της εργασίας είναι η διερεύνηση των δημοσιοποιημένων περιστατικών παραβίασης δεδομένων που έχουν καταγραφεί τα τελευταία πέντε χρόνια και η πρόληψη ή αντιμετώπιση του προβλήματος. Αρχικά, γίνεται επεξήγηση των ορολογιών που σχετίζονται με τα προσωπικά δεδομένα και την προστασία αυτών, καθώς και του σχετικού νομικού πλαισίου. Έπειτα, αναλύονται τα υπάρχοντα συστήματα διαχείρισης ασφάλειας τα οποία χρησιμοποιούνται από τους οργανισμούς, μαζί με τρόπους διαχείρισης περιστατικών ασφάλειας. Στη συνέχεια, παρουσιάζεται η έρευνα η οποία έχει διεξαχθεί για τα δημοσιοποιημένα περιστατικά παραβίασης δεδομένων, η επεξήγηση του τρόπου εξαγωγής της, καθώς και οι πίνακες και γραφήματα των περιστατικών. Ταυτόχρονα, τονίζεται η ύπαρξη του ανθρώπινου λάθους σε τέτοιες περιπτώσεις και πως ο άνθρωπος μπορεί να επηρεάσει την ασφάλεια των πληροφοριών σε ένα πληροφοριακό σύστημα ενός οργανισμού. Τα αποτελέσματα της έρευνας δείχνουν ότι στις περισσότερες περιπτώσεις που υπήρξε ανθρώπινο λάθος, υπήρχε έλλειψη επίγνωσης ασφάλειας των υπαλλήλων του οργανισμού αλλά και προβλήματα στην ασφάλεια των πληροφοριακών συστημάτων. Τέλος, δίνονται μεθοδολογίες πρόληψης και αντιμετώπισης των περιστατικών παραβίασης δεδομένων, μαζί με κάποια συμπεράσματα για τα περιστατικά παραβίασης που καταγράφηκαν.

Λέξεις κλειδιά: ανθρώπινο λάθος, αντιμετώπιση περιστατικών παραβίασης, διαχείριση κινδύνων, διαχείριση περιστατικών ασφάλειας, παραβίαση δεδομένων, συστήματα διαχείρισης ασφάλειας πληροφοριών.

Abstract

This thesis deals with the concentration of data breach incidents and their association with human error. The thesis aim is to investigate the publicly available data breach incidents recorded over the last five years and the prevention or addressing of the problem. Initially, are explained the terminology of the issues related to personal data, the protection of them and the relevant legal framework. Next, are analyzed the existing security management systems used by the agencies together with ways to manage security incidents. The investigation has subsequently been presented for publicly publicized data breach incidents, the explanation of how it is exported, and the tables and charts of the incidents. At the same time, the existence of human error in such cases is highlighted and the ways that human can influence the security of information in an information system of an organization. According to the results, in most cases of human error, there was a lack of safety awareness of the agency's employees and problems with the safety of information systems. Finally, methodologies are given to prevent and deal with data breach incidents, together with some conclusions on the cases of infringement recorded.

Keywords: data breach, human error, security incident management, information security management systems, risk management, violation incident response

1

Εισαγωγή

1.1 Αντικείμενο διπλωματικής

Το Διαδίκτυο αποτελεί αναπόσπαστο κομμάτι της καθημερινής ζωής του σύγχρονου ανθρώπου, ο οποίος το χρησιμοποιεί όλες τις ώρες της ημέρας του, αξιοποιώντας το για οποιοδήποτε ζήτημα του είναι απαραίτητο. Από μια απλή αναζήτηση σε κάποια μηχανή αναζήτησης και την πληρωμή λογαριασμών, αγορά κάποιου προϊόντος και το κλείσιμο εισιτηρίων και χώρων διαμονής. Σε αυτές και άλλες δραστηριότητες του ανθρώπου έρχονται να βοηθήσουν εκατομμύρια ιστοσελίδες, οι οποίες πολύ συχνά αποθηκεύουν προσωπικές πληροφορίες που θα παρέχει ο χρήστης στην υπηρεσία για να καλύψει τις ανάγκες του. Οι πληροφορίες αυτές, συλλέγονται, επεξεργάζονται και αποθηκεύονται από τους οργανισμούς αυτούς, προκειμένου να εξασφαλιστεί η καλύτερη λειτουργία των παροχών των χρηστών τους.

Όσο περισσότερες πληροφορίες και δεδομένα αποθηκεύονται από έναν οργανισμό, τόσο περισσότερο αυξάνεται και η ανάγκη προστασίας τους. Οι ηλεκτρονικές επιθέσεις έχουν αυξηθεί κατά πολύ τα τελευταία χρόνια, λόγω του ότι η απόκτηση των πληροφοριών αυτών, αποτελεί ένα χρήσιμο εργαλείο για τους επιτιθέμενους που προτίθενται να πουλήσουν αυτές τις πληροφορίες. Οι βάσεις δεδομένων των εταιρειών, περιλαμβάνουν ευαίσθητα προσωπικά δεδομένα, όπως ονοματεπώνυμα, διευθύνσεις, email, αριθμούς τηλεφώνων αλλά και αριθμούς πιστωτικών καρτών ή αριθμούς κοινωνικής ασφάλισης. Ένας καίριος στόχος των οργανισμών είναι τα δεδομένα να διαφυλάσσονται και να προστατεύονται για την σωστή λειτουργία των οργανισμών.

Συνεχώς, αυξάνονται οι δημοσιεύσεις σχετικά με ζητήματα ασφάλειας αλλά και τη σημασία των πληροφοριών που περιλαμβάνουν τα πληροφοριακά συστήματα ενός οργανισμού. Πολλές φορές υπήρξαν περιστατικά που οδήγησαν την διαρροή των δεδομένων, στην παραβίαση της ιδιωτικής ταυτότητας προσώπων, ακόμα και σε οικονομική απώλεια και απώλεια φήμης για τον οργανισμό (Κάτσικας, 2014). Παρόλα αυτά, παρατηρείται, κυρίως τα τελευταία πέντε χρόνια, μια μεγάλη αύξηση περιστατικών παραβίασης δεδομένων σε πολλούς τομείς, όπως στο χώρο της υγείας, σε μεγάλες εταιρείες τηλεπικοινωνιών και μεταφορικών οργανώσεων, σε πολλές ιστοσελίδες και μέσα μαζικής επικοινωνίας, ακόμα και σε πολλές κρατικές υπηρεσίες, σε πανεπιστήμια αλλά και σε χώρους εστίασης και στέγασης. Ένα περιστατικό παραβίασης δεδομένων (data breach) συνεπάγεται μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα, προστατευμένα ή εμπιστευτικά δεδομένα που οδηγούν σε συμβιβασμό εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των επηρεαζόμενων δεδομένων (Sen and Borle, 2015). Τα ευαίσθητα, προστατευμένα ή εμπιστευτικά δεδομένα ενδέχεται να περιλαμβάνουν προσωπικές πληροφορίες του πελάτη σχετικά με την υγεία, την προσωπική του ζωή, εμπορικά μυστικά ή πνευματική ιδιοκτησία ή προσωπικά οικονομικά δεδομένα. Ο αντίκτυπος των περιστατικών παραβίασης δεδομένων είναι σημαντικός τόσο για τους στοχευμένους οργανισμούς όσο και για τα επηρεαζόμενα άτομα.

Μια παραβίαση δεδομένων, μπορεί να συμβεί με διάφορους τρόπους. Ένας επιτιθέμενος αποκτάει πρόσβαση στη βάση δεδομένων ενός οργανισμού και κατ' επέκταση στις προσωπικές πληροφορίες των χρηστών. Ένα κακόβουλο λογισμικό εγκαθίσταται στο πληροφοριακό σύστημα και επηρεάζει την σωστή λειτουργία του. Ένας από τους υπαλλήλους της εταιρείας αποκτά μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες και τις χρησιμοποιεί προς όφελος του. Αυτοί και πολλοί άλλοι τρόποι μπορούν να οδηγήσουν στην παραβίαση των δεδομένων του οργανισμού.

Δημιουργείται, λοιπόν, η ανάγκη για προστασία των πληροφοριακών συστημάτων από οποιαδήποτε κακόβουλη ενέργεια που θα προκαλέσει έλλειψη ή διαρροή των προσωπικών πληροφοριών. Για την αποτελεσματικότερη προστασία των πληροφοριών ενός οργανισμού έχουν αναπτυχθεί αρκετές μέθοδοι που βοηθούν σε αυτό. Η ύπαρξη ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ), συμβάλει σημαντικά στην καλύτερη ασφάλεια των δεδομένων μιας εταιρείας (Κάτσικας, 2014). Επιπλέον, η σωστή διαχείριση των περιστατικών ασφάλειας, αποτελεί βασικό ρόλο στην αντιμετώπιση οποιουδήποτε προβλήματος. Για την ενίσχυση της προστασίας των δεδομένων, έχουν θεσπιστεί αρκετοί νόμοι που συμβάλουν στην ασφάλεια των πληροφοριών. Μαζί με την νομοθεσία, παρέχονται επίσης και αρκετές μέθοδοι πρόληψης και αντιμετώπισης περιστατικών παραβίασης δεδομένων.

Η διπλωματική αυτή εργασία, ασχολείται με περιστατικά παραβίασης δεδομένων, τα οποία έχουν δημοσιοποιηθεί κυρίως τα τελευταία χρόνια. Στόχος της εργασίας είναι η διερεύνηση των δημοσιοποιημένων παραβιάσεων και ο εντοπισμός της συσχέτισης τους με τον ανθρώπινο παράγοντα. Μέσα από την κατηγοριοποίηση των περιστατικών που συγκεντρώθηκαν, εντοπίζεται κατά πόσο ο ανθρώπινος παράγοντας και το ανθρώπινο λάθος επηρεάζουν την αποτελεσματική προστασία των

δεδομένων ενός οργανισμού, δίνοντας ταυτόχρονα κάποιες προτάσεις για την πρόληψη και αντιμετώπιση τους.

1.2 Δομή διπλωματικής

Η παρούσα διπλωματική εργασία, περιλαμβάνει πέντε κεφάλαια. Η μεθοδολογία που χρησιμοποιήθηκε, είναι η έρευνα των δημοσιοποιημένων περιστατικών παραβίασης δεδομένων που έχουν καταγραφεί τα τελευταία πέντε χρόνια, από το 2014 έως το 2019. Επιλέχθηκαν οι συγκεκριμένες χρονολογίες έτσι ώστε να περιοριστεί η ποσότητα των περιστατικών που θα συγκεντρώνονταν. Επίσης, έγινε περιορισμός ως προς το σύνολο των δεδομένων που διέρρευσαν ή κλάπηκαν, έτσι ώστε να γίνει επικέντρωση στις περιπτώσεις μεγάλης σημασίας. Γι' αυτό το λόγο συγκεντρώθηκαν περιστατικά που το σύνολο των δεδομένων τους αφορούσε σε περισσότερα από 500.000 άτομα. Στη συνέχεια, γίνεται κατηγοριοποίηση των περιστατικών με βάση την χρονολογία, την αιτία, τον τομέα και άλλες κατηγορίες που δημιουργήθηκαν για την συγκεκριμένη έρευνα. Έπειτα, αναλύονται τα συμπεράσματα των αποτελεσμάτων της έρευνας και προτείνονται τρόποι πρόληψης και αντιμετώπισης παραβιάσεων δεδομένων.

Στο πρώτο κεφάλαιο, δίνονται οι ορολογίες των προσωπικών δεδομένων (personal data) και της παραβίασης δεδομένων (data breach). Επεξηγείται η σημασία αυτών των εννοιών σε σχέση με την ασφάλεια των δεδομένων στα πληροφοριακά συστήματα, ενώ ταυτόχρονα αναλύεται η αναγκαιότητα της ιδιωτικότητας στα περιβάλλοντα αυτά. Στη συνέχεια του κεφαλαίου, παρουσιάζεται το νομοθετικό πλαίσιο που ισχύει για την προστασία των προσωπικών δεδομένων αλλά και των οργανισμών σε σχέση με τα προβλήματα ασφάλειας των πληροφοριακών συστημάτων τους, που περιλαμβάνει τόσο τις παλαιότερες νομοθεσίες των διαφόρων κρατών, μέχρι τον νέο Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).

Το επόμενο κεφάλαιο αναφέρεται στην διαχείριση ασφάλειας πληροφοριών και περιέχει τα υπάρχοντα εργαλεία για την καλύτερη προστασία των πληροφοριακών συστημάτων. Στην αρχή, αναλύεται ο τρόπος δημιουργίας ενός συστήματος διαχείρισης ασφάλειας πληροφοριών, καθώς επίσης και οι παράγοντες που επηρεάζουν την ασφάλεια τους. Κατά την δημιουργία ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών χρησιμοποιούνται πρότυπα του ISO, όπως το ISO/IEC 27001:2013. Έπειτα, δίνονται οι τρόποι διαχείρισης περιστατικών ασφάλειας, τους οποίους έχει προτείνει ο NIST.

Στη συνέχεια της διπλωματικής, εξηγείται και αναλύεται το βασικό ζήτημα του θέματος, το οποίο είναι τα δημοσιοποιημένα περιστατικά παραβίασης δεδομένων. Υπάρχει σχετική ανάλυση της μεθοδολογίας που ακολουθήθηκε κατά την διεξαγωγή της έρευνας για τον εντοπισμό των περιστατικών, μαζί με τον τρόπο εξαγωγής των αποτελεσμάτων. Επιπλέον, παρουσιάζονται τα αποτελέσματα της έρευνας με βάση τις κατηγορίες ταξινόμησης των περιστατικών παραβίασης που επιλέχθηκαν για την καλύτερη ανάλυση τους. Ταυτόχρονα, τονίζεται η σημασία του ανθρώπινου παράγοντα και πως το ανθρώπινο λάθος ήταν η αιτία που οδήγησε τις περισσότερες φορές σε διαρροή των δεδομένων ενός οργανισμού.

Στο επόμενο κεφάλαιο, τονίζεται η σημασία της επίγνωσης ασφάλειας σε έναν οργανισμό, για την αποφυγή περιστατικών αλλά και την άμεση αντιμετώπιση τους. Επίσης, δίνεται η μεθοδολογία που

ακολουθείται για την διαχείριση των κινδύνων σε περιπτώσεις παραβιάσεων και για την έγκαιρη αντιμετώπιση τους, με σκοπό την ελάττωση του προβλήματος. Παράλληλα, εξηγείται η ανάγκη της ύπαρξης μιας πολιτικής ασφάλειας για τον οργανισμό καθώς και ο τρόπος δημιουργίας αυτής έτσι ώστε να εξασφαλιστεί η προστασία των δεδομένων των πληροφοριακών συστημάτων του οργανισμού. Τέλος, με βάση τα αποτελέσματα της έρευνας, δίνονται κάποιοι προτεινόμενοι τρόποι αντιμετώπισης των αυτού του είδους των περιστατικών.

2

Προστασία προσωπικών δεδομένων

Η συνεχής χρήση του Διαδικτύου είναι πλέον αναπόσπαστο κομμάτι της καθημερινότητας του σύγχρονου ανθρώπου. Το Διαδίκτυο συνεχίζει να επεκτείνεται και τα δεδομένα που ρέουν σε διαφορετικά δίκτυα αυξάνονται. Το 2019, το 56% του παγκόσμιου πληθυσμού χρησιμοποιεί το Διαδίκτυο - περίπου 7.676 δισεκατομμύρια χρήστες (Padwal et al, 2019). Οι δημόσιες υπηρεσίες ηλεκτρονικών επικοινωνιών, ιδίως μέσω του Διαδικτύου, ανοίγουν όχι μόνο νέες δυνατότητες για τους χρήστες, αλλά και νέους κινδύνους για τα προσωπικά τους δεδομένα και το ιδιωτικό τους απόρρητο, λόγω του ότι επιτρέπουν τη συνεχή παρακολούθηση των επικοινωνιών και των δραστηριοτήτων (Mitrou and Moulinos, 2003). Καθώς αυξάνεται το ύψος των δεδομένων που αποθηκεύονται και επεξεργάζονται από τις εταιρείες, αυξάνεται και η πολυπλοκότητα των πληροφοριακών συστημάτων που απαιτούνται για την φύλαξη τους (Acquisti et al, 2006). Η ύπαρξη τεράστιων ποσοτήτων πληροφοριών που διατίθενται στους χρήστες, έχει ως αποτέλεσμα την δημιουργία κινδύνων που συνδέονται με την λανθασμένη συμπεριφορά αλλά και με τη κλοπή δεδομένων (Padwal et al, 2019). Οι οργανισμοί βρίσκονται υπό αυξανόμενη πίεση για να αποτρέψουν αυτή την κλοπή και να προστατεύσουν τα δεδομένα τους - τόσο για τους πελάτες τους όσο και για τους υπαλλήλους τους. Ομοίως, οι κυβερνήσεις αισθάνονται την ανάγκη να ρυθμίζουν και να προστατεύουν τα συστήματα από την απάτη και την μη εξουσιοδοτημένη αποκάλυψη προσωπικών πληροφοριών.

2.1 Εννοιολογικό πλαίσιο προσωπικών δεδομένων και παραβίασης δεδομένων

Τα προσωπικά δεδομένα (personal data) είναι οποιαδήποτε πληροφορία η οποία σχετίζεται με αναγνωρίσιμο ή μη άτομο . Διαφορετικές πληροφορίες, που συλλέγονται μαζί, μπορούν να οδηγήσουν στην αναγνώριση ενός συγκεκριμένου προσώπου, αποτελούν επίσης προσωπικά δεδομένα (European Commission). Ένα περιστατικό παραβίασης δεδομένων (data breach) συνεπάγεται μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα, προστατευμένα ή εμπιστευτικά δεδομένα που οδηγούν σε συμβιβασμό εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων που επηρεάζονται (Sen and Borle, 2015). Τα ευαίσθητα, προστατευμένα ή εμπιστευτικά δεδομένα ενδέχεται να περιλαμβάνουν πληροφορίες για την υγεία, προσωπικές πληροφορίες, εμπορικά μυστικά, πνευματική ιδιοκτησία ή προσωπικά οικονομικά δεδομένα. Ο αντίκτυπος των περιστατικών παραβίασης δεδομένων είναι σημαντικός τόσο για τους στοχευόμενους οργανισμούς όσο και για τα επηρεαζόμενα άτομα.

Ένα περιστατικό παραβίασης δεδομένων καθορίζεται ως το γεγονός που συνεπάγεται την κατάχρηση των προσωπικών πληροφοριών των ατόμων (Aquisti et al, 2006). Η κατάχρηση αυτή μπορεί να συνδέεται με παράνομες πωλήσεις, παράνομη χρήση ή έλλειψη προστασίας. Μπορεί να είναι εγκληματική, εμπορική ή τελικά αβλαβής. Μπορεί να είναι σκόπιμη ή ακούσια. Μπορεί να περιλαμβάνει δεδομένα πελατών ή εργαζομένων. Ένα τέτοιο περιστατικό διεγείρει την δημιουργία συζήτησης ως προς την ιδιωτικότητα.

Οι παραβιάσεις μπορεί να είναι καταστροφικές για τους οργανισμούς. Σε περίπτωση μη προστασίας των δεδομένων ενός οργανισμού, αυξάνονται οι πιθανότητες εγκλημάτων όπως η κλοπή ταυτότητας, ιδιαίτερα όταν τα δεδομένα πελατών, συμπεριλαμβανομένων των αριθμών των πιστωτικών καρτών, αποτελούν το αντικείμενο της παραβίασης. Επίσης, αυξάνεται η πιθανότητα εταιρικής κατασκοπείας, κατά την οποία αποκτάται πρόσβαση σε πολύτιμα σχέδια ή άλλη πνευματική ιδιοκτησία από το μη εξουσιοδοτημένο συμβαλλόμενο μέρος (Sheldon, 2019).

Η ιδιωτικότητα ξεκίνησε να απασχολεί τους ανθρώπους από τον 19ο αιώνα, όταν οι Warren και Brandeis (Lengheinrich, 2001) όρισαν την ιδιωτικότητα ως «το δικαίωμα του να είναι κάποιος μόνος του». Στις μέρες μας αυτός ο ορισμός παραφράστηκε ως «το δικαίωμα του να επιλέγει κάποιος ποιες προσωπικές του πληροφορίες θα γίνονται γνωστές και σε ποια άτομα». Κυρίως από το 1960 και μετά, λόγω κάποιων σοβαρών προβλημάτων που προκλήθηκαν, η ιδιωτικότητα έγινε ακόμα πιο σημαντικό θέμα, δημιουργώντας την ανάγκη θέσπισης νόμων για την προστασία της (Lengheinrich, 2001). Με την πάροδο του χρόνου, ο κύριος στόχος της ιδιωτικότητας διαμορφώθηκε σύμφωνα με τις τεχνολογικές εξελίξεις. Έτσι, υπήρξε μια μετάβαση από την προστασία των ιδιωτικών μέσων (media privacy), στην χωρική ιδιωτικότητα (territorial privacy), έπειτα στην ιδιωτικότητα της επικοινωνίας (communication privacy), στην ατομική ιδιωτικότητα (bodily privacy), για να καταλήξει στην ιδιωτικότητα των πληροφοριών (information privacy) (Lengheinrich, 2001).

Οι δημόσιες υπηρεσίες ηλεκτρονικών επικοινωνιών, ιδίως μέσω του Διαδικτύου, ανοίγουν όχι μόνο νέες δυνατότητες για τους χρήστες, αλλά και νέους κινδύνους για τα προσωπικά τους δεδομένα και το ιδιωτικό τους απόρρητο, καθώς επιτρέπουν τη συνεχή παρακολούθηση των επικοινωνιών και των δραστηριοτήτων (Mitrou and Moulinos, 2003). Έχουν προταθεί διάφορες τεχνολογικές προσεγγίσεις για την επίλυση του προβλήματος της ιδιωτικής ζωής. Σε σχεδόν οποιοδήποτε πιθανό σενάριο - όταν κάποιος κάνει αγορές, περιηγείται στο Διαδίκτυο, απαντάει σε έρευνες ή ολοκληρώνει ιατρικές εξετάσεις - η ταυτότητα ενός ατόμου μπορεί να διαχωριστεί από τις υπόλοιπες πληροφορίες που αποκαλύφθηκαν κατά τη διάρκεια της συναλλαγής (Aquisti, 2004). Ωστόσο, οι οργανισμοί που βασίζονται σε αυτές τις τεχνολογίες έχουν αγωνιστεί να εξισορροπήσουν τις διαφορετικές ανάγκες των διαφόρων μερών στην εξίσωση της ιδιωτικής ζωής, και τελικά να μην αποκτήσουν ευρεία υιοθεσία. Παρόλο που η κύρια ανησυχία είναι για την ιδιωτικότητα και την ασφάλεια των προσωπικών δεδομένων, η κυβέρνηση παρεμβαίνει αυξάνοντας της ευθύνες των οργανισμών ως προς την συλλογή προσωπικών πληροφοριών χωρίς να ορίζονται οι υποχρεώσεις των οργανισμών απέναντι στην λανθασμένη χρήση των δεδομένων αυτών. Η ερμηνεία των προσωπικών δεδομένων ως εμπορεύσιμου αγαθού εγείρει ανησυχίες ηθικής όσον αφορά το κατά πόσο οι ζωές των ανθρώπων πρέπει να είναι ιδιοκτησία ή αν στην πραγματικότητα τα προσωπικά δεδομένα πρέπει να θεωρούνται αναφαίρετα από τα άτομα με τα οποία σχετίζονται (Spiekermann et al, 2015).

Μια παραβίαση συνήθως περνάει από τα ακόλουθα 3 στάδια:

1. Ανίχνευση: ένα μη εξουσιοδοτημένο μέρος επιδιώκει να εντοπίσει τρωτά σημεία στο σύστημα ασφαλείας ενός οργανισμού. Τέτοιες αδυναμίες δεν είναι πάντοτε βασισμένες σε συστήματα. Ο κοινός κωδικός πρόσβασης σε πολλές πλατφόρμες είναι μια κοινή μορφή ανθρώπινου λάθους που μπορεί να οδηγήσει σε παραβιάσεις.
2. Διείσδυση: στη συνέχεια, το μη εξουσιοδοτημένο μέρος εισέρχεται στο δίκτυο των οργανισμών χρησιμοποιώντας μια από τις ευπάθειες που έχει ανακαλύψει. Συχνά αυτό οφείλεται σε ανεπαρκή ασφάλεια δρομολογητών και άλλων συσκευών σύνδεσης. Υπάρχουν επίσης περιπτώσεις όπου μπορεί να εκμεταλλευτούν τα μέλη του προσωπικού και τους εργαζόμενους. Ο εκβιασμός ή ακόμα και η υπόσχεση για ένα μερίδιο εγκληματικών κερδών, μπορεί να χρησιμοποιηθεί ως μοχλός έτσι ώστε ένα μη εξουσιοδοτημένο άτομο να μπορέσει να αποκτήσει πρόσβαση σε ένα δίκτυο.
3. Εξαγωγή: μόλις οι επιτιθέμενοι βρίσκονται σε δίκτυο, το τελευταίο βήμα είναι να εξάγουν τα δεδομένα του οργανισμού. Η εξαγωγή θα μπορούσε να είναι η αντιγραφή των δεδομένων μέσω του Διαδικτύου, η τοποθέτηση τους σε μια εξωτερική συσκευή ή ακόμα και η απλή προβολή των δεδομένων και η αντιγραφή τους χειροκίνητα (Sheldon, 2019).

Πώς συμβαίνουν οι παραβιάσεις;

Οι παραβιάσεις δεδομένων μπορεί να προέρχονται από διάφορες πηγές. Παρόλο που η εγκληματικότητα στον κυβερνοχώρο και η πειρατεία είναι η κορυφαία μέθοδος διείσδυσης του δικτύου,

δεν είναι ο μόνος τρόπος που οι ανεπιθύμητοι επισκέπτες εισέρχονται στα δίκτυα (Sheldon, 2019). Σύμφωνα με μια έκθεση της Verizon, μιας από τις κορυφαίες εταιρείες παγκόσμιας ασφάλειας και συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR), οι κορυφαίες 6 μέθοδοι εισόδου σε δίκτυα είναι: Φυσικές δράσεις (Physical actions), Προβλήματα προνομίων (Privilege problems), Κοινωνική μηχανική (Social engineering), Ανθρώπινο λάθος (Human error), Κακόβουλο λογισμικό (Malware) και το Χακάρισμα (Hackers).

Σύμφωνα με το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας, οι επιθέσεις στον κυβερνοχώρο αυξάνονται σε αριθμό, ποικιλία, επίπεδο ζημιών και διαταραχές. Βασικές προκλήσεις για την ασφάλεια των δεδομένων περιλαμβάνουν την πολυπλοκότητα των συστημάτων, την επικράτηση των νέων τεχνολογιών και τις ανθρώπινες δράσεις (ή αδράνειες) (Hall and Wright, 2018). Μια πρόκληση για τη διατήρηση της ασφάλειας των δεδομένων είναι η πολυπλοκότητα των κυβερνητικών συστημάτων και των πολλών γραμμών κώδικα ή εντολών που έχουν εγγραφεί σε ένα πρόγραμμα. Μια άλλη πρόκληση είναι η δυναμική κατάσταση των κυβερνητικών συστημάτων. Οι οργανισμοί τείνουν να αναβαθμίζουν τακτικά τα λογισμικά συστήματα και η κάθε τροποποίηση συχνά έχει ως αποτέλεσμα τη δυνατότητα εκμετάλλευσης νέων τρωτών σημείων (Hall and Wright, 2018). Οι εταιρείες λογισμικού, σε μια προσπάθεια να φέρουν γρήγορα τα προϊόντα τους στην αγορά, συχνά περιορίζουν το χρόνο που ξοδεύεται για την αναζήτηση και διόρθωση των τρωτών σημείων. Η επικράτηση των νέων τεχνολογιών δημιουργεί νέες προκλήσεις ασφάλειας για τους οργανισμούς.

Ποιες είναι οι συνέπειες μιας παραβίασης των δεδομένων;

Είναι γεγονός ότι όλα τα αποτελέσματα μιας παραβίασης των δεδομένων είναι κακό για τον ενδιαφερόμενο οργανισμό. Το ICO (Γραφείο Επιτρόπου Πληροφόρησης) μπορεί να επιβάλει πρόστιμο σύμφωνα με τους κανονισμούς GDPR. Η μέγιστη ποινή είναι 20 εκατομμύρια ευρώ ή 4% του ετήσιου παγκόσμιου κύκλου εργασιών.

Το επόμενο πρόβλημα είναι η απώλεια φήμης που προκαλείται από την παραβίαση. Ακόμη και αν η διείσδυση ήταν απίστευτα πολύπλοκη, η αντίληψη του κοινού θα είναι ότι η παραβιασμένη οργάνωση υπέφερε από χαλαρή ασφάλεια και ανεπαρκή αντίμετρα (Sheldon, 2019).

Οι περισσότεροι πελάτες θα απομακρυνθούν από έναν οργανισμό ο οποίος δεν μπορεί να κρατήσει τα δεδομένα τους ασφαλή. Σε κανέναν δεν αρέσει οι εμπιστευτικές του πληροφορίες, όπως αρχεία υγείας, να δημοσιοποιούνται. Ωστόσο, αν τα τραπεζικά αρχεία και οι αριθμοί των πιστωτικών καρτών των πελατών κλαπούν, τότε αυτά τα άτομα θα πρέπει να αναλάβουν ταχεία δράση για να αποφύγουν την κλοπή ταυτότητας και αυτό είναι πιθανό να καταστρέψει οποιαδήποτε προηγούμενη σχέση με τον οργανισμό.

Οι παραβιάσεις δεδομένων επηρεάζουν τόσο τους καταναλωτές όσο και τους οργανισμούς. Η κλοπή ταυτότητας και η απάτη αποτελούν μείζονες ανησυχίες μετά την παραβίαση της ασφάλειας των δεδομένων. Ενώ οι δύο όροι χρησιμοποιούνται συχνά εναλλακτικά, υπάρχουν διαφοροποιημένες διαφορές και η απάτη ταυτότητας συμβαίνει συχνά ως αποτέλεσμα κλοπής ταυτότητας (Hall and Wright, 2018). Η

κλοπή ταυτότητας είναι ο μεγαλύτερος αντίκτυπος των παραβιάσεων δεδομένων σε ιδιώτες καθώς 12,7 εκατομμύρια θύματα απάτης υπέστησαν απώλεια αξίας 16 δισεκατομμυρίων δολαρίων το 2014.

Το κόστος ενός περιστατικού ασφάλειας υπολογιστών σε έναν οργανισμό πρέπει να μετράται από την άποψη του αντίκτυπου στον οργανισμό. Επομένως τα ίδια περιστατικά σε δύο διαφορετικούς οργανισμούς του ίδιου κλάδου ή επιχειρηματικού τομέα θα μπορούσαν να έχουν διαφορετικό κόστος (Farachmand et al, 2003). Ο αντίκτυπος μπορεί να είναι οικονομικός, υπό μορφή άμεσων δαπανών και ζημιών, αλλά πολύ πιο σοβαρό είναι το κρυφό κόστος. Για παράδειγμα, ένα περιστατικό ασφάλειας υπολογιστών μπορεί να βλάψει έναν οργανισμό όσον αφορά:

- Την εικόνα της μάρκας, τη φήμη του κοινού και την καλή θέληση στην αγορά
- Την οικονομική αξία των επιχειρηματικών συναλλαγών
- Την εμπιστοσύνη των πολιτών και των πελατών στην ακρίβεια και την αντοχή στις απάτες των επιχειρηματικών συναλλαγών
- Την ικανότητα διατήρησης των εσόδων ταμειακών ροών εγκαίρως
- Την ικανότητα επίλυσης διαφορών πέρα από εύλογες αμφιβολίες
- Την ικανότητα να πληρούν τις απαιτήσεις των ρυθμιστικών αρχών

Κάθε ένα από αυτά τα περιστατικά παραβίασης δεδομένων έχει διαφορετική αιτία και μπορεί να έχει διαφορετική σειρά επιπτώσεων. Το κοινό θέμα είναι η κακή χρήση προσωπικών πληροφοριών (Aquisti et al, 2016). Ένα υποσύνολο περιστατικών μπορεί να αποδοθεί στην αποτυχία της ασφάλειας των πληροφοριών. Η αποτυχία αυτή θα μπορούσε να είναι τεχνική (άμεση επίθεση από κακόβουλους), διαχειριστική (αδυναμία εμπλοκής με γνωστή ευπάθεια), οργανωτική (ατελής προστασία) ή ανθρώπινη (δεδομένα που παραμένουν σε κλεμμένο φορητό υπολογιστή).

Τον Ιούνιο του 2014, ο Επίτροπος της Επιτροπής Κεφαλαιαγοράς (SEC) Luis Aguilar προειδοποίησε ότι τα οργανωτικά συμβούλια θα πρέπει "να προετοιμάσουν την εταιρεία για την αναπόφευκτη επιδρομή στον κυβερνοχώρο και τις επακόλουθες επιπτώσεις από μια τέτοια εκδήλωση". Το Κέντρο Στρατηγικών και Διεθνών Μελετών, McAfee, εκτιμά ότι το κόστος του εγκλήματος στον κυβερνοχώρο παγκοσμίως θα υπερβαίνει τα 400 δισεκατομμύρια δολάρια ετησίως (Hall and Wright, 2018). Σύμφωνα με την ίδια έκθεση, οι Ηνωμένες Πολιτείες έχασαν περίπου 100 δισεκατομμύρια δολάρια το 2013 όταν εξετάστηκε το άμεσο και το έμμεσο κόστος των επιθέσεων στον κυβερνοχώρο.

Επιπλέον, οι εταιρείες πρέπει επίσης να πληρώσουν για να υπερασπιστούν τους εαυτούς τους σε αγωγές που συχνά συμβαίνουν ως αποτέλεσμα παραβιάσεων δεδομένων. Αυτό καθιστά τις παραβιάσεις δεδομένων πολύ δαπανηρές για τους οργανισμούς.

2.2 Νομικό πλαίσιο

Ο κίνδυνος παραβίασης των δεδομένων είναι υψηλότερος από ποτέ και σχεδόν οι μισοί από τους οργανισμούς υποφέρουν από τουλάχιστον ένα συμβάν ασφάλειας. Για να αντιμετωπιστεί αυτό, το 48%

των οργανισμών αύξησε τις επενδύσεις σε τεχνολογίες ασφαλείας και το 73% αναγνώρισε την πιθανότητα παραβίασης με την ανάπτυξη σχεδίου απόκρισης για παραβίαση δεδομένων.

Παρά τις προληπτικές ενέργειες που λαμβάνουν οι οργανισμοί, όπως νόμοι που έχουν θεσπιστεί από διάφορες κυβερνήσεις των κρατών, απαιτήσεις κοινοποίησης παραβιάσεων δεδομένων και ο νόμος για την διαχείριση της ασφάλειας των πληροφοριών της ομοσπονδιακής κυβέρνησης, εξακολουθούν να συμβαίνουν περιστατικά παραβίασης δεδομένων (Sen and Borle, 2015).

Οι νόμοι απαιτούν οι οργανισμοί να ενημερώνουν τα άτομα όταν έχουν χαθεί ή κλαπεί τα προσωπικά τους στοιχεία. Συγκεκριμένα, οι νόμοι απαιτούν εγκαίρως κοινοποίηση εάν έχουν χαθεί ή είναι πιθανόν να αποκτηθούν προσωπικά αναγνωρίσιμα στοιχεία από μη εξουσιοδοτημένο πρόσωπο και ευλόγως θεωρείται ότι θέτουν σε κίνδυνο τις προσωπικές πληροφορίες ενός ατόμου (Romanosky et al, 2011).

Οι παραβιάσεις δεδομένων προκύπτουν όταν προσωπικά αναγνωρίσιμες πληροφορίες, όπως ονόματα, αριθμοί κοινωνικής ασφάλισης και αριθμοί πιστωτικών καρτών, χάνονται τυχαία ή λόγω κλοπής. Αυτές οι παραβιάσεις μπορούν να οδηγήσουν σε εκατοντάδες χιλιάδες αρχεία και να έχουν ως αποτέλεσμα κλοπή ταυτότητας και συναφή εγκλήματα. Στις Ηνωμένες Πολιτείες, η κλοπή ταυτότητας είχε ως αποτέλεσμα απώλειες οργανισμών αλλά και καταναλωτών. Σε μια προσπάθεια να μειωθούν αυτά τα εγκλήματα, πολλά κράτη απάντησαν υιοθετώντας νόμους περί αποκάλυψης παραβιάσεων δεδομένων, απαιτώντας από τις επιχειρήσεις να ενημερώνουν τα άτομα όταν έχουν διακυβευτεί τα προσωπικά τους στοιχεία (Romanosky et al, 2011).

Οι νόμοι σχετικά με την κοινοποίηση των παραβιάσεων συνεχίζουν να εξαπλώνονται, παρόλο που η κοινοποίηση εξακολουθεί να μην είναι υποχρεωτική στις περισσότερες χώρες. Στην Ευρώπη, ο Γενικός Κανονισμός για την Προστασία των Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR), ο οποίος άρχισε να ισχύει τον Μάιο του 2018, περιλαμβάνει ορισμένες διατάξεις περί απορρήτου, συμπεριλαμβανομένων των υποχρεωτικών κοινοποιήσεων παραβίασης. Ορισμένοι νομικοί εμπειρογνώμονες υποστηρίζουν ότι ο κανονισμός θα χρησιμεύσει ως πρότυπο για άλλες χώρες (Schwartz, 2016). Στις Ηνωμένες Πολιτείες, περίπου 47 κράτη, τρία αμερικανικά εδάφη και η Ουάσινγκτον, έχουν νόμους κοινοποίησης παραβιάσεων ποικίλης ισχύος. Παρόλα αυτά, οι προσπάθειες για την αντικατάσταση τους με ένα ενιαίο και πιο απλό ομοσπονδιακό νόμο έχουν αποτύχει. Στην Αυστραλία και στη Νέα Ζηλανδία, οι υπάλληλοι και των δύο χωρών εξετάζουν τις υποχρεωτικές προτάσεις κοινοποίησης παραβιάσεων, αλλά δεν έχουν ακόμα εκδώσει σχετικούς νόμους (Schwartz, 2016). Ταυτόχρονα, στην Ινδία, υπάρχει έλλειψη οποιουδήποτε μηχανισμού για την επιβολή νόμου κοινοποίησης παραβιάσεων δεδομένων και οι εμπειρογνώμονες λένε ότι είναι απίθανο η χώρα να εφαρμόσει οποιουσδήποτε σχετικούς νόμους στο επόμενο χρονικό διάστημα.

Σήμερα, σχεδόν 90 χώρες έχουν νόμους περί προστασίας δεδομένων - ή σχετικές δικαστικές αποφάσεις -, από την Αγκόλα και την Αργεντινή έως τη Βενεζουέλα και τη Ζιμπάμπουε, σύμφωνα με τη δικηγορική εταιρεία DLA Piper. Ωστόσο, πολλές από τις χώρες αυτές δεν απαιτούν από τους παραβιαζόμενους οργανισμούς να ενημερώνουν τις αρχές ή τα άτομα των οποίων τα προσωπικά στοιχεία

έχουν εκτεθεί σε περίπτωση παραβίασης (Schwartz, 2016). Παρακάτω, θα αναλυθούν κάποιες από τις νομοθεσίες που ισχύουν για την προστασία των προσωπικών δεδομένων αλλά και για τις παραβιάσεις τους.

Η οδηγία 97/66 / ΕΚ σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των τηλεπικοινωνιών, εφάρμοσε τις γενικές αρχές που θεσπίστηκαν με τη γενική οδηγία για την προστασία των δεδομένων (D 95/46 / ΕΚ) στον τομέα των τηλεπικοινωνιών (Mitrou and Moulinos, 2003). Αργότερα, η νέα, για τότε, οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (2002/58 ΕΚ) διευρύνει την ειδική προστασία που παρέχεται σε όλα τα κινητά, δορυφορικά και καλωδιακά δίκτυα.

Το 2013, ο Πρόεδρος Obama υπέγραψε την εκτελεστική εντολή 13.636, η οποία ασχολήθηκε με την ασφάλεια στον κυβερνοχώρο και ανέθεσε στο Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) την ευθύνη να αναπτύξει το Πλαίσιο Ασφάλειας στον κυβερνοχώρο για χρήση από παρόχους (Hayes, 2019). Το 2014, το Κογκρέσο πέρασε τρεις νόμους σχετικούς με την ασφάλεια στον κυβερνοχώρο: 1) τον νόμο για τον εκσυγχρονισμό της ομοσπονδιακής ασφάλειας πληροφοριών του 2014 (FISMA), 2) τον εθνικό νόμο για την ασφάλεια στον κυβερνοχώρο του 2014 (NCPA) και 3) την ενέργεια ενίσχυσης του κυβερνοχώρου του 2014 (CEA) . Το FISMA είναι μια ενημέρωση του νόμου για την Federal Information Security Management. Το NCPA κωδικοποιεί τις λειτουργίες του Εθνικού Κέντρου Διασφάλισης Ασφάλειας και Επικοινωνιών (NCCIC) του Υπουργείου Εσωτερικής Ασφάλειας (DHS). Το Κεφάλαιο I του CEA περιλαμβάνει κατευθυντήριες γραμμές για τις δραστηριότητες του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας σχετικά με τα πρότυπα στον κυβερνοχώρο, κωδικοποιώντας ορισμένες πτυχές του ΕΟ 13,636. Το Πλαίσιο Cybersecurity της NIST έχει μετατραπεί σε πόρο για πρότυπα στον κυβερνοχώρο εκτός από την υποδομή ζωτικής σημασίας (Hayes, 2019).

Ορισμένοι ομοσπονδιακοί νόμοι περί ασφάλειας στον κυβερνοχώρο επικεντρώνονται στην ανάγκη πληροφόρησης για την απειλή του κυβερνοχώρου μεταξύ του ιδιωτικού τομέα και της κυβέρνησης. Το 2015, ο νόμος για την ανταλλαγή πληροφοριών για την ασφάλεια στον κυβερνοχώρο (CISA) τέθηκε σε ισχύ ως μέρος του νομοσχεδίου για τις δαπάνες για το 2016 (Hayes, 2019).

Από την πλευρά της προστασίας των καταναλωτών, το Κογκρέσο αντιμετώπισε το πάγωμα των πιστωτικών ιδρυμάτων, το οποίο είναι ένα εργαλείο που διατίθεται στους καταναλωτές μετά την παραβίαση των δεδομένων τους (Hayes, 2019). Όταν ο καταναλωτής ζητά την κατάργηση της πίστωσης, το πιστωτικό γραφείο θέτει ένα μπλοκάρισμα στις νέες αιτήσεις πίστωσης από τους δανειστές. Αυτό εμποδίζει τους κλέφτες ταυτότητας να χρησιμοποιούν τις πληροφορίες του καταναλωτή για να ανοίξουν ένα νέο λογαριασμό. Όταν ο καταναλωτής θέλει ξανά να υποβάλει αίτηση για πίστωση, μπορεί να απελευθερώσει την πιστωτική έκθεσή του (Hayes, 2019). Με το νέο ομοσπονδιακό νόμο, τα τρία μεγάλα πιστωτικά γραφεία πρέπει να παρέχουν πάγωμα πίστωσης χωρίς χρέωση.

Η Ευρωπαϊκή Επιτροπή ορίζει τα PETs ως "ένα συνεκτικό σύστημα μέτρων ΤΠΕ που προστατεύει την ιδιωτική ζωή εξαλείφοντας ή μειώνοντας τα προσωπικά δεδομένα ή εμποδίζοντας την περιττή ή

ανεπιθύμητη επεξεργασία προσωπικών δεδομένων, όλα χωρίς να χάσουν τη λειτουργικότητα του συστήματος πληροφοριών" (Mitrou and Karyda, 2012). Τα PETs αποτελούνται από σύνθετες τεχνολογίες οι οποίες χρησιμοποιούν κάποια μέτρα ασφάλειας, όπως μηχανισμούς κρυπτογράφησης και ελέγχου πρόσβασης, σε συνδυασμό με άλλους μηχανισμούς για τη βελτίωση της συνολικής ιδιωτικότητας. Η εφαρμογή τους βασίζονται στις βασικές αρχές για την προστασία των προσωπικών δεδομένων. Τα PETs επιτρέπουν στα άτομα να ελέγχουν ποιες προσωπικές πληροφορίες επεξεργάζονται, πώς επεξεργάζονται και από ποιον, καθώς επίσης, δίνουν στους χρήστες την επιλογή της απόκρυψης της πραγματικής τους ταυτότητας.

Η εφαρμογή της αρχής της προστασίας δεδομένων από το σχεδιασμό σε όλα τα στάδια ανάπτυξης συστημάτων συνεπάγεται την ενσωμάτωση τεχνολογιών, συσκευών και εργαλείων για την προστασία της ιδιωτικής ζωής που μπορούν να προστατεύσουν την ιδιωτική ζωή των δεδομένων (Mitrou and Karyda, 2012). Σύμφωνα με την Ευρωπαϊκή Επιτροπή, «η χρήση των PETs μπορεί να συμβάλει στον σχεδιασμό συστημάτων και υπηρεσιών πληροφόρησης και επικοινωνιών κατά τρόπο που να ελαχιστοποιεί τη συλλογή και τη χρήση προσωπικών δεδομένων και διευκολύνει την τήρηση των κανόνων προστασίας δεδομένων. Η χρήση των PETs θα πρέπει να καταστήσει δυσχερέστερες τις παραβιάσεις ορισμένων κανόνων προστασίας δεδομένων ή να τους βοηθήσει να τις ανιχνεύσουν " (Mitrou and Karyda, 2012).

Στις 27 Απριλίου 2016, η Ευρωπαϊκή Ένωση υιοθέτησε τελικά τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR), περισσότερο από τέσσερα χρόνια μετά την πρόταση της Ευρωπαϊκής Επιτροπής. Ο κανονισμός άρχισε να ισχύει από τις 25 Μαΐου 2018. Ο νόμος για την προστασία των δεδομένων της Ευρωπαϊκής Ένωσης προστατεύει τα φυσικά πρόσωπα όσον αφορά την επεξεργασία των προσωπικών τους δεδομένων (Voss, 2017; GDPR, 2018). Το GDPR ορίζει τόσο την "επεξεργασία" όσο και την έννοια των "προσωπικών δεδομένων" σε γενικές γραμμές και σύμφωνα με την οδηγία για την προστασία των δεδομένων, παρόλο που αναδιοργανώνει και επικαιροποιεί τους ορισμούς της οδηγίας για την προστασία δεδομένων. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να περιλαμβάνει, μεταξύ άλλων, τα εξής: "συλλογή, καταγραφή, οργάνωση, διαμόρφωση, αποθήκευση, προσαρμογή ή τροποποίηση, ανάκτηση, διαβούλευση, χρήση, γνωστοποίηση μέσω μετάδοσης, διάδοση ή άλλη διάθεση, ευθυγράμμιση ή "συνδυασμός, περιορισμός, διαγραφή ή καταστροφή" (Voss, 2017; GDPR, 2018).

Το εδαφικό πεδίο εφαρμογής του GDPR είναι μεγαλύτερο από αυτό της οδηγίας για την προστασία των δεδομένων. Επιπλέον, ισχύει για την "επεξεργασία δεδομένων προσωπικού χαρακτήρα των υποκειμένων των δεδομένων που βρίσκονται στην Ευρωπαϊκή Ένωση από υπεύθυνο επεξεργασίας ή μεταποιητή που δεν είναι εγκατεστημένος στην Ευρωπαϊκή Ένωση" (Voss, 2017; GDPR, 2018). Το GDPR τροποποιεί την αρχή "περιορισμού της αποθήκευσης". Οι οργανισμοί πλέον καλούνται να ασχοληθούν και επίσημα με την προστασία των πληροφοριακών τους συστημάτων και την προάσπιση των δεδομένων τους, κάνοντας τακτικά ελέγχους ασφάλειας δικτύων και υποδομών, υλοποιώντας πολιτικές ασφάλειας και διαδικασίες, αλλά και εκπαιδεύοντας τους χρήστες πληροφοριακών συστημάτων για την ορθή χρήση των πληροφοριακών συστημάτων τους (Voss, 2017; GDPR, 2018). Ο Κανονισμός επιβάλλει

μια σειρά νέων υποχρεώσεων στους υπεύθυνους επεξεργασίας, οι οποίες απορρέουν από τις βασικές αρχές και ιδίως την ενισχυμένη αρχή της διαφάνειας στον τρόπο συλλογής, επεξεργασίας και τήρησης δεδομένων και τη νέα αρχή της λογοδοσίας, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωσή του με όλες τις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων.

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος, την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή που είναι αρμόδια σύμφωνα με το άρθρο 55 του Γενικού Κανονισμού, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (GDPR, 2018).. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.

Στην σημείωση 85 του άρθρου 55 του Γενικού Κανονισμού τονίζεται ότι η παραβίαση δεδομένων προσωπικού χαρακτήρα μπορεί, εάν δεν αντιμετωπιστεί κατάλληλα και έγκαιρα, να έχει ως αποτέλεσμα σωματική, υλική ή μη υλική βλάβη για φυσικά πρόσωπα, όπως απώλεια του ελέγχου επί των δεδομένων τους προσωπικού χαρακτήρα ή ο περιορισμός των δικαιωμάτων τους, διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, παράνομη άρση της ψευδωνυμοποίησης, βλάβη της φήμης και απώλεια της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από επαγγελματικό απόρρητο ή άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα για το ενδιαφερόμενο φυσικό πρόσωπο (GDPR, 2018).

Παρατηρείται, λοιπόν, ότι παρόλο που υπήρχαν και παλαιότερα κάποιοι νόμοι για την προστασία των προσωπικών δεδομένων, ο Γενικός Κανονισμός για την Προστασία Δεδομένων, δημιούργησε ένα οργανωμένο πλαίσιο θέσπισης κανόνων. Καλύπτει όλες τις περιπτώσεις κανόνων αλλά και όλες τις δράσεις που απαιτούνται σε περίπτωση παραβίασης των προσωπικών δεδομένων.

3

Διαχείριση ασφάλειας πληροφοριών

Οι παραβιάσεις ασφάλειας προκαλούνται είτε από εξωτερικές απειλές είτε από εσωτερικές απειλές. Οι οργανισμοί πρέπει να προστατεύσουν τις υποδομές τους από οποιουδήποτε είδους παραβιάσεων, για να διασφαλίσουν τις βασικές επιχειρησιακές λειτουργίες τους. Οι υπεύθυνοι για την ασφάλεια των πληροφοριακών συστημάτων ενός οργανισμού ή αλλιώς οι διαχειριστές ασφάλειας, αναλαμβάνουν να οργανώσουν την ασφάλεια των πληροφοριών, σχεδιάζοντας και εφαρμόζοντας πολιτικές ασφάλειας και ακολουθώντας διαδικασίες πρότυπα, κατευθυντήριες γραμμές και βέλτιστες πρακτικές μέσω κάποιων πακέτων προδιαγραφών που υπάρχουν.

Υπάρχουν τρεις βασικοί παράγοντες από τους οποίους εξαρτάται το επίπεδο ασφάλειας πληροφοριών ενός οργανισμού. Ένας παράγοντας είναι τα επίπεδα κινδύνου που έχει καθορίσει ο οργανισμός. Δεύτερος παράγοντας είναι η λειτουργικότητα του πληροφοριακού συστήματος και τρίτος παράγοντας είναι το ποσό που προτίθεται να πληρώσει ο οργανισμός για την ασφάλεια του (Κάτσικας, 2014). Ο οργανισμός γνωρίζει ότι οι πληροφορίες οι οποίες συλλέγονται, επεξεργάζονται, αποθηκεύονται και μεταδίδονται είναι απαραίτητες για την λειτουργία του, γι' αυτό και πρέπει να προστατεύονται. Τα μέτρα ασφάλειας που λαμβάνει, μπορούν να ελαττώσουν τον βαθμό κινδύνου των πληροφοριών.

Με το συγκεκριμένο ζήτημα έχουν ασχοληθεί πολλοί ερευνητές οι οποίοι διερευνούν επίσης τη συμπεριφορά των εργαζόμενων ως προς την ασφάλεια αλλά και τη συμμόρφωση τους στους κανονισμούς που υπάρχουν. Είναι σημαντικό στην διαχείριση της ασφάλειας να υπολογίζεται η συμπεριφορά ασφάλειας των υπαλλήλων μαζί με τα τεχνικά αντίμετρα (Topa and Karyda, 2018). Έχει παρατηρηθεί ότι ακόμα και

όταν εφαρμόζονται οι κατάλληλοι έλεγχοι, οι υπάλληλοι των οργανισμών πολύ συχνά δεν δίνουν την απαραίτητη σημασία και δεν συμμορφώνονται με τους κανονισμούς.

Για να επιτευχθεί η ασφάλεια των πληροφοριών σε έναν οργανισμό, δημιουργείται ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ). Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System), είναι το τμήμα του συστήματος διαχείρισης του οργανισμού που αφορά την ασφάλεια πληροφοριών και περιέχει ένα πλαίσιο πολιτικών, διαδικασιών, οδηγιών και των πόρων που απαιτούνται έτσι ώστε να πετύχουν οι στόχοι που θέτει ο οργανισμός για την ασφάλεια των πληροφοριακών συστημάτων του (Κάτσικας, 2014). Η αποτελεσματικότητα αυτού του συστήματος φαίνεται στην ικανότητα του να συμβαδίζει με τις ανάγκες του οργανισμού και τον τρόπο λειτουργίας του.

3.1 Συστήματα διαχείρισης ασφάλειας πληροφοριών

Έχοντας ως στόχο την διαφύλαξη της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας πληροφοριών, το έργο των διαχειριστών ασφάλειας είναι να εφαρμόσουν πρακτικές ασφάλειας και ελέγχους από διάφορα πλαίσια ασφάλειας. Τα πλαίσια ασφάλειας που υπάρχουν αυτή τη στιγμή είναι το COBIT, τα πρότυπα του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST) και η οικογένεια ISO/IEC 27000 πρότυπα ασφαλείας.

Το COBIT είναι ένα πλαίσιο που χρησιμοποιείται για την διαχείριση και τη διοίκηση της πληροφορικής και περιλαμβάνει γενικές πρακτικές πληροφορικής και επιχειρηματικούς στόχους. Ασχολείται, επίσης, με τον μετριασμό του κινδύνου των τεχνολογιών πληροφορικής και τη διαχείριση κινδύνων και είναι σχεδιασμένο να μπορεί να είναι συμβατό με άλλα πρότυπα (Topa and Karyda, 2018). Κάτι αντίστοιχο είναι και το πλαίσιο του NIST, το οποίο αποτελείται από κάποια βήματα που πρέπει να ακολουθήσει ένας διαχειριστής ασφάλειας για τον εντοπισμό των κινδύνων, την εφαρμογή ελέγχων και την ενίσχυση της ασφάλειας.

Για την αντιμετώπιση του προβλήματος της ασφάλειας πληροφοριών στους οργανισμούς, δημιουργήθηκε ένας κατάλογος με όλα τα αποτελεσματικά μέτρα ασφάλειας που οφείλει να εφαρμόζει ένας οργανισμός. Τα πρότυπα ασφάλειας πληροφοριών ISO παρέχουν οδηγίες για τη διαχείριση της ασφάλειας πληροφοριών, τη διαχείριση κινδύνων και τα μέτρα ασφάλειας μέσα στο περιβάλλον ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (Κάτσικας, 2014; ISO27k Forum). Το 2014 υπήρχαν 23 πρότυπα της σειράς ISO27k, ενώ μέχρι σήμερα υπάρχουν τουλάχιστον 57 πρότυπα που εκδίδονται παγκοσμίως. Το βασικό πρότυπο της σειράς είναι το ISO/IEC 27001, το οποίο θέτει και τις προδιαγραφές ενός ΣΔΑΠ. Τα υπόλοιπα πρότυπα της σειράς παρέχουν υποστήριξη και οδηγίες για την υλοποίηση του συστήματος.

Το πρότυπο ISO/IEC 27001 δημοσιεύθηκε για πρώτη φορά το 1997, παρόλα αυτά η τρέχουσα έκδοση που χρησιμοποιείται είναι η ISO/IEC 27001:2013. Το πρότυπο αυτό έχει ως στόχο της θέσπιση προδιαγραφών για τον σχεδιασμό, την υλοποίηση, τη λειτουργία, την παρακολούθηση, τον έλεγχο και τη

συντήρηση ενός ΣΔΑΠ, μέσα στα πλαίσια ενός οργανισμού. Ταυτόχρονα, περιέχει προδιαγραφές για την εκτίμηση και διαχείριση των κινδύνων, οι οποίες βασίζονται στις ανάγκες του οργανισμού. Το συγκεκριμένο πρότυπο μπορεί να εφαρμοστεί σε όλους τους οργανισμούς, οποιουδήποτε τομέα. Περιλαμβάνει επτά ενότητες, οι οποίες έχουν και τις υποενότητες τους η καθεμία ξεχωριστά: Ενότητα περιβάλλον οργανισμού, Ενότητα ηγεσίας, Ενότητα σχεδιασμού, Ενότητα υποστήριξης, Ενότητα λειτουργίας, Ενότητα αξιολόγησης και Ενότητα βελτίωσης (Disterer, 2013; ISO/IEC 27001:2013).

Η πρώτη ενότητα ασχολείται με το περιβάλλον του οργανισμού και χωρίζεται σε τέσσερις υποενότητες. Μια υποενότητα είναι η αναγνώριση των στοιχείων του περιβάλλοντος του οργανισμού που επηρεάζουν τη λειτουργία του ΣΔΑΠ. Η δεύτερη υποενότητα, αναφέρεται στην αναγνώριση του οργανισμού των μερών που έχουν ενδιαφέρον για το ΣΔΑΠ και ποιες είναι οι απαιτήσεις τους από αυτό. Έπειτα η τρίτη υποενότητα ορίζει ότι ο οργανισμός θα πρέπει να καθορίσει τα όρια και την έκταση εφαρμογής του συστήματος. Η τέταρτη υποενότητα δίνει στον οργανισμό την απαίτηση να θεσπίσει, να υλοποιήσει, να συντηρεί και να βελτιώνει συνεχώς το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Κάτσικας, 2014; ISO/IEC 27001:2013; Disterer, 2013).

Η δεύτερη ενότητα αναφέρεται στην ηγεσία και περιλαμβάνει τρεις υποενότητες. Το ανώτερο επίπεδο διοίκησης του οργανισμού, στην πρώτη υποενότητα, πρέπει να ηγηθεί όλη τη διαδικασία και να αναλάβει δεσμεύσεις για την αποτελεσματική λειτουργία του ΣΔΑΠ. Θα πρέπει δηλαδή να θεσπίσει μια πολιτική ασφάλειας πληροφοριών, να φροντίσει για την εμπέδωση των προδιαγραφών του συστήματος, να διαθέσει όσους πόρους χρειάζεται το ΣΔΑΠ για να εκτελεστεί και να διασφαλίσει ότι θα υπάρχουν τα επιθυμητά αποτελέσματα του συστήματος διαχείρισης. Ταυτόχρονα, το ανώτερο επίπεδο διοίκησης, οφείλει να γνωστοποιήσει το πόσο σημαντικό είναι το ΣΔΑΠ για τον οργανισμό, να καθοδηγήσει τους υπαλλήλους και να βοηθά στην συνεχή βελτίωση τους (Κάτσικας, 2014; ISO/IEC 27001:2013).

Η δεύτερη υποενότητα της δεύτερης ενότητας του ISO/IEC 27001, θέτει στο ανώτερο επίπεδο διοίκησης την θέσπιση μιας πολιτικής ασφάλειας πληροφοριών, η οποία θα είναι κατάλληλη για τους σκοπούς του οργανισμού, θα περιλαμβάνει τους στόχους ασφάλειας και θα δεσμεύεται ότι θα ικανοποιηθούν οι απαιτήσεις του συστήματος. Η τελευταία υποενότητα αναφέρεται επίσης στο ανώτερο επίπεδο διοίκησης και το ορίζει να αναθέσει αρμοδιότητες στους υπαλλήλους με βάσει το ΣΔΑΠ (Κάτσικας, 2014; ISO/IEC 27001:2013).

Η επόμενη ενότητα ασχολείται με τον σχεδιασμό και αποτελείται από δύο υποενότητες. Στην πρώτη υποενότητα, επισημαίνονται οι ενέργειες που είναι απαραίτητες να γίνουν για τον εντοπισμό των κινδύνων και των ευκαιριών, ενώ η δεύτερη περιέχει τις ενέργειες που χρειάζονται για τον καθορισμό των στόχων ασφάλειας και τον σχεδιασμό επίτευξης τους. Στην ενότητα του σχεδιασμού δηλαδή, θα πρέπει να γίνουν οι κατάλληλες ενέργειες τόσο για τον εντοπισμό των κινδύνων όσο και για την λήψη κατάλληλων μέτρων ασφάλειας, καθώς και τη διαμόρφωση ενός σχεδίου διαχείρισης κινδύνων (Κάτσικας, 2014; ISO/IEC 27001:2013).

Η ενότητα για την υποστήριξη περιλαμβάνει πέντε υποενότητες. Στην πρώτη, ο οργανισμός θα πρέπει να ορίσει και να δώσει τους πόρους που χρειάζεται το ΣΔΑΠ για την υλοποίηση, βελτίωση και συντήρηση του. Η δεύτερη υποενότητα θέτει στον οργανισμό την αναγνώριση των ικανοτήτων των υπαλλήλων του που σχετίζονται με την ασφάλεια των πληροφοριών, καθώς θα πρέπει να έχουν τις απαραίτητες γνώσεις για να ανταπεξέλθουν. Με βάση την τρίτη υποενότητα, οι υπάλληλοι του οργανισμού θα πρέπει να έχουν επίγνωση της πολιτικής ασφάλειας του ΣΔΑΠ, μαζί με τον ρόλο που έχει ο καθένας στην αποτελεσματικότητα του. Η τέταρτη υποενότητα αναφέρεται στην ανάγκη για καθορισμό των επικοινωνιακών αναγκών που είναι σχετικές με το ΣΔΑΠ, ενώ η πέμπτη υποενότητα, τονίζει την ανάγκη τεκμηρίωσης του συστήματος διαχείρισης από τον οργανισμό (Κάτσικας, 2014; ISO/IEC 27001:2013).

Στη συνέχεια, υπάρχει η ενότητα για την λειτουργία. Αυτή αποτελείται από τρεις υποενότητες. Μια υποενότητα είναι ο λειτουργικός σχεδιασμός και ο έλεγχος όπου ο οργανισμός οφείλει να σχεδιάσει, να υλοποιήσει και να ελέγχει. Επίσης, είναι σημαντική η τεκμηρίωση των διεργασιών, ο έλεγχος των αλλαγών και η εξέταση των συνεπειών. Στην επόμενη υποενότητα, αναφέρεται η εκτίμηση των κινδύνων και η εκπόνηση μελέτης εκτίμησης κινδύνων σε τακτά χρονικά διαστήματα. Η τρίτη υποενότητα, τονίζει την διαχείριση των κινδύνων, καθώς ο οργανισμός θα πρέπει να υλοποιεί το σχέδιο διαχείρισης κινδύνων και να τεκμηριώνει τα αποτελέσματα (Κάτσικας, 2014; ISO/IEC 27001:2013).

Η έκτη ενότητα ασχολείται με την αξιολόγηση της επίδοσης και περιέχει τρεις υποενότητες. Η πρώτη υποενότητα σχετίζεται με την παρακολούθηση, την μέτρηση, την ανάλυση και την αξιολόγηση. Ο οργανισμός πρέπει να ορίζει τι θα παρακολουθείται και θα μετράται, ποιες μεθόδους θα χρησιμοποιούνται, πότε θα γίνεται η παρακολούθηση, ποιος θα την κάνει, πότε θα αναλύονται τα αποτελέσματα και ποιος θα τα αξιολογεί. Η δεύτερη υποενότητα της αξιολόγησης επίδοσης, περιλαμβάνει τον εσωτερικό έλεγχο τον οποίο πρέπει να κάνει ο οργανισμός για να εξασφαλίζεται η σωστή λειτουργία του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Απαιτείται η σχεδίαση, θέσπιση, υλοποίηση και συντήρηση προγραμμάτων ελέγχου. Επίσης, είναι απαραίτητη η ύπαρξη κριτηρίων ελέγχου, η επιλογή ελεγκτών, η εξασφάλιση αποτελεσματικότητας και η διατήρηση της τεκμηρίωσης από τον οργανισμό. Η τελευταία υποενότητα, τονίζει την επανεξέταση του ΣΔΑΠ ώστε να διασφαλιστούν η καταλληλότητα, η επάρκεια και η αποτελεσματικότητα του. Για να θεωρείται σωστή η λειτουργία του συστήματος, θα πρέπει να πραγματοποιούνται οι ενέργειες του και να υπάρχουν αποτελέσματα από την εκτίμηση κινδύνων (Κάτσικας, 2014; ISO/IEC 27001:2013).

Η έβδομη και τελευταία ενότητα της δομής των απαιτήσεων του πρότυπου ISO/IEC 27001:2013, είναι η ενότητα της βελτίωσης, η οποία και αυτή με τη σειρά της αποτελείται από δύο υποενότητες. Η πρώτη σχετίζεται με την περίπτωση μη συμμόρφωσης και τις διορθωτικές ενέργειες, ορίζοντας ότι σε περίπτωση προβλήματος, ο οργανισμός θα πρέπει να αντιμετωπίσει το ζήτημα και να αξιολογήσει την κατάσταση προκειμένου να εντοπίσει τις αιτίες του προβλήματος. Η δεύτερη υποενότητα ορίζει ότι ο οργανισμός πρέπει συνεχώς να βελτιώνει την λειτουργία του Συστήματος Διαχείρισης Ασφάλειας

Πληροφοριών για την αποφυγή προβλημάτων και την καλύτερη ασφάλεια του (Κάτσικας, 2014; ISO/IEC 27001:2013).

Το ISO/IEC 27002:2013 δίνει κατευθυντήριες γραμμές για οργανωσιακά πρότυπα ασφάλειας πληροφοριών, για πρακτικές διαχείρισης της ασφάλειας και για την επιλογή, υλοποίηση και διαχείριση μέτρων ασφάλειας. Με βάση το πρότυπο, πρέπει να τηρούνται οι απαιτήσεις του συστήματος από τους ελέγχους ασφάλειας, να αντιμετωπίζονται διαφορετικές πτυχές του περιβάλλοντος και να διασφαλίζονται οι επιχειρηματικοί στόχοι του οργανισμού. Το συγκεκριμένο πρότυπο περιέχει 35 κύριες κατηγορίες ασφάλειας, με 114 ελέγχους ασφάλειας, οι οποίοι περιλαμβάνουν κυρίως τεχνικά μέτρα (Topa and Karyda, 2018). Παράλληλα, δίνονται οδηγίες για την ασφάλεια των ανθρώπινων πόρων, συμπεριλαμβανομένης και της εκπαίδευσης ασφάλειας. Η εκπαίδευση ασφάλειας είναι σημαντική καθώς ενημερώνει τους υπαλλήλους του οργανισμού για την λογοδοσία τους και τις συνέπειες που θα υπάρξουν σε περίπτωση παραβίασης της ασφάλειας. Επίσης, ορίζονται και κάποιες κυρώσεις που γίνονται σε περίπτωση παραβίασης, μαζί με μηχανισμούς παρακολούθησης των συμβάντων (Disterer, 2013; Topa and Karyda, 2018).

Στη συνέχεια υπάρχει το ISO/IEC 27003:2010, το οποίο εστιάζει στις κρίσιμες πτυχές του επιτυχούς σχεδιασμού και υλοποίησης ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Περιγράφει τη διεργασία προδιαγραφής και σχεδιασμού του ΣΔΑΠ από την αρχή μέχρι τη διαμόρφωση των σχεδίων υλοποίησης. Επιπλέον, περιγράφει την διεργασία λήψης έγκρισης από την διοίκηση για την υλοποίηση του συστήματος, ορίζει ένα έργο υλοποίησης και παρέχει οδηγίες για το πώς σχεδιάζεται το έργο ΣΔΑΠ ώστε να αποτελέσει σχέδιο υλοποίησης (Κάτσικας, 2014; Topa and Karyda, 2018).

Το ISO/IEC 27005: 2011, αναφέρεται στην διαδικασία διαχείρισης των κινδύνων, χωρίς όμως να καθορίζει ποια είναι η κατάλληλη προσέγγιση διαχείρισης κινδύνου που πρέπει να ακολουθηθεί. Ορίζει τις απαιτήσεις που είναι απαραίτητες για την υποστήριξη του ΣΔΑΠ . Υποστηρίζει τις γενικές αρχές του προτύπου ISO/IEC 27001 και εφαρμόζεται σε όλους τους οργανισμούς. Παρέχει γενικές οδηγίες σχετικά με τα κριτήρια που πρέπει να έχουν οι διαχειριστές ασφάλειας στην διαδικασία διαχείρισης κινδύνου (Κάτσικας, 2014; Topa and Karyda, 2018).

3.2 Διαχείριση περιστατικών ασφάλειας

Ο οργανισμός λοιπόν, έχει φροντίσει να υπάρχει ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών, έχει προβεί στις κατάλληλες ενέργειες και βρίσκεται σε διαρκεί επαγρύπνηση και ετοιμότητα για να αντιμετωπίσει οποιαδήποτε κατάσταση. Μέχρι την στιγμή που γίνεται κάποιο περιστατικό παραβίασης της ασφάλειας των πληροφοριών και εκεί πρέπει να δράσει αποτελεσματικά για την αντιμετώπιση του. Η διαχείριση και αντιμετώπιση περιστατικών ασφάλειας είναι το σύνολο των ενεργειών όπου θα εκτελεστούν σε περίπτωση μη αναμενόμενων επιθέσεων, απωλειών, κλοπών ή ατυχημάτων τα οποία εκδηλώνονται λόγω της έλλειψης ή της αστοχίας των μέτρων ασφάλειας (Κάτσικας, 2014).

Ο βασικός στόχος της διαχείρισης των περιστατικών είναι να εντοπίσει άμεσα τα περιστατικά ασφάλειας έτσι ώστε να περιοριστούν οι επιπτώσεις που θα έχουν στο σύστημα και κατ' επέκταση και στον οργανισμό. Οι απειλές μπορεί να είναι είτε τεχνικής φύσης, όπως για παράδειγμα, επιθέσεις με τη χρήση κακόβουλου λογισμικού, επιθέσεις άρνησης υπηρεσίας (Denial of Service, DoS), είτε μπορεί να είναι αποτέλεσμα κάποιων λαθών στο σύστημα, όπως ατύχημα ή αστοχία του ή διακοπή της λειτουργίας του (Κάτσικας, 2014). Ο ανθρώπινος παράγοντας επίσης παίζει σημαντικό ρόλο, καθώς μπορεί να κλαπούν υλικά, όπως για παράδειγμα ένα λάπτοπ ή αντίγραφα ασφαλείας ή ακόμα και να γίνει κάποιο ατύχημα που θα επηρεάσει την λειτουργία του συστήματος. Επιπλέον, στις απειλές συμπεριλαμβάνονται και οι περιπτώσεις φυσικών καταστροφών, όπως μια πυρκαγιά, πλημμύρα ή σεισμός. Η διαχείριση περιστατικών στοχεύει στον άμεσο εντοπισμό του περιστατικού, στη σωστή διαχείριση του, καθώς και στον περιορισμό και την μείωση του προβλήματος και στην αποκατάσταση των ζημιών, βελτίωσης του ΣΔΑΠ και ενημέρωσης για το περιστατικό. Στη συνέχεια, θα δοθούν κάποιες περιπτώσεις περιστατικών που είναι πολύ συχνές και ποιες είναι οι αιτίες που τις προκαλούν.

Περιστατικά άρνησης υπηρεσίας (Denial of Service)

Ένα περιστατικό άρνησης υπηρεσίας, μπορεί να προκαλέσει την διακοπή της λειτουργίας του συστήματος ή να εμποδίσει την πρόσβαση στους εξουσιοδοτημένους χρήστες. Το συγκεκριμένο περιστατικό χωρίζεται σε περιπτώσεις αφαίρεσης πόρων και σε περιπτώσεις εξάντλησης τους. Ο επιτιθέμενος το πετυχαίνει αυτό με την αποστολή μηνυμάτων βολιδοσκόπησης (pinging), με την αποστολή δεδομένων με μορφοποίηση η οποία δεν είναι αναγνωρίσιμη από το σύστημα και προκαλεί κόλλημα στη λειτουργία του (crash) και με την επίθεση στο σύστημα μέσω ανοίγματος πολλών συνόδων επικοινωνίας, το οποίο προκαλεί συμφόρηση στο σύστημα. Παρόλα αυτά, κάποια από τα περιστατικά άρνησης υπηρεσίας μπορεί να προκύψουν τυχαία στο σύστημα, χωρίς την παρέμβαση κάποιου επιτιθέμενου. Συνήθως, τα περιστατικά άρνησης υπηρεσίας τα οποία δεν οφείλονται σε κάποια επίθεση, μπορεί να προκληθούν από κάποια παραβίαση των μέτρων φυσικής απώλειας του οργανισμού, από τυχαία ζημιά στο υλικό, από ακατάλληλες περιβαλλοντικές συνθήκες ή από δυσλειτουργία του συστήματος (Κάτσικας, 2014; Cichoski et al, 2012).

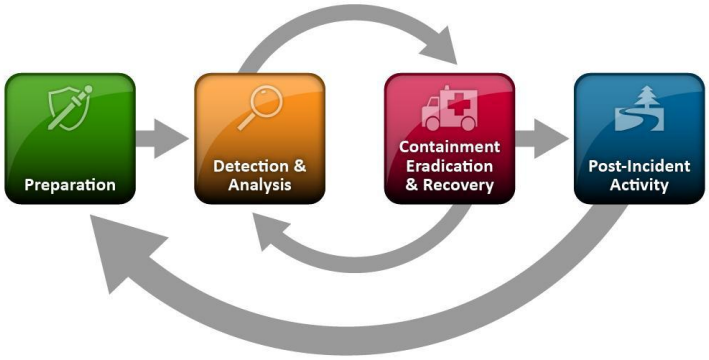
Περιστατικά συλλογής πληροφοριών

Τα περιστατικά συλλογής πληροφοριών σχετίζονται με περιπτώσεις όπου ο επιτιθέμενος συλλέγει πληροφορίες για το σύστημα στο οποίο στοχεύει να εισέλθει, έτσι ώστε να μπορεί να γνωρίζει τις ευπάθειες του, τις υπηρεσίες που εκτελούνται, καθώς και τον τύπο της επίθεσης που θα επιλέξει για το συγκεκριμένο σύστημα. Ένα περιστατικό συλλογής πληροφοριών πολλές φορές εξελίσσεται και σε περιστατικό μη εξουσιοδοτημένης πρόσβασης. Κάποια είδη επιθέσεων σε αυτή την κατηγορία είναι η αποθήκευση αρχείων Domain Name System (DNS), η διερεύνηση διαδικτυακών διευθύνσεων, η σάρωση διαθέσιμων δικτύων του συστήματος και η αναζήτηση υπηρεσιών με ευπάθειες (Cichoski et al, 2012). Ταυτόχρονα, αν ένα περιστατικό συλλογής πληροφοριών προκληθεί λόγω κακής διαμόρφωσης του λειτουργικού συστήματος, μπορεί να έχει ως αποτέλεσμα της διαρροή πληροφοριών.

Περιστατικά μη εξουσιοδοτημένης πρόσβασης

Ίσως από τις πιο συνηθισμένες περιπτώσεις περιστατικών, η μη εξουσιοδοτημένη πρόσβαση μπορεί να προκύψει μέσω απόπειρας ανάκτησης αρχείων συνθηματικών, επίθεσης που προκαλεί υπερχείλιση στο σύστημα, μέσω κάποιας ευπάθειας που έχει το πρωτόκολλο δικτύων ή και μέσω προσπάθειας απόκτησης δικαιωμάτων πρόσβασης σε πληροφορίες οι οποίες δεν είναι διαθέσιμες στο συγκεκριμένο άτομο. Όλα αυτά, συμπεριλαμβανομένου και της περίπτωσης να υπάρχει κάποια δυσλειτουργία στο λογισμικό που θα οδηγήσει στην κακή χρήση της πληροφορίας, έχουν ως αποτέλεσμα την μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες.

Η αντιμετώπιση των περιστατικών ασφάλειας, με βάση τον NIST (2012), περιέχει έξι φάσεις: την Προετοιμασία, την Ανίχνευση, την Αναχαίτιση, την Εξάλειψη, την Ανάκαμψη και την Ανασκόπηση. Παρατηρείται ότι ο κύκλος ζωής αυτής της διαδικασίας ξεκινάει πριν τον εντοπισμό του περιστατικού.



Εικόνα 1, Κύκλος ζωής αντιμετώπισης περιστατικών

Στην φάση της Προετοιμασίας, τα ανώτερα διοικητικά στελέχη ενός οργανισμού, συγκεντρώνονται για την οργάνωση του τρόπου αντιμετώπισης περιστατικών ασφάλειας, αναπτύσσοντας μέτρα πρόληψης και ανίχνευσης περιστατικών και διαμορφώνοντας σχέδια για την αντιμετώπιση τους. Συγκεκριμένα σε αυτή τη φάση:

- Καθορίζονται οι προσεγγίσεις που θα χρησιμοποιηθούν για την διαχείριση των περιστατικών
- Καθιερώνεται η πολιτική και προστίθενται προειδοποιήσεις στα πληροφοριακά συστήματα
- Διαμορφώνεται το σχέδιο επικοινωνίας με τους υπεύθυνους του οργανισμού
- Θεσπίζονται κριτήρια για την λήψη αποφάσεων για το περιστατικό
- Διαμορφώνεται μια ομάδα αντιμετώπισης των περιστατικών
- Καθορίζεται μια ασφαλή τοποθεσία ως τόπος εφαρμογής του σχεδίου αντιμετώπισης
- Διασφαλίζεται η διαθεσιμότητα του απαραίτητου εξοπλισμού

Αφού έχει προηγηθεί η φάση της προετοιμασίας και προκύψει αργότερα κάποιο περιστατικό, ενεργοποιείται η φάση της Ανίχνευσης. Σε αυτή τη φάση θα πρέπει να οριστεί το αν όντως έχει συμβεί κάποιο περιστατικό ασφάλειας. Πολλές φορές ένας οργανισμός ενημερώνεται για πιθανή παραβίαση από

πληροφοριακά συστήματα, από χρήστες ή από άλλους οργανισμούς. Παρόλα αυτά, θα πρέπει να ελεγχθεί η εγκυρότητα της αναφοράς, καθώς μπορεί να πρόκειται για κάποιον λάθος συναγερμό (Κάτσικας, 2014). Γι' αυτό και σε αυτό το σημείο, η ανίχνευση του περιστατικού, η αξιολόγηση της κατάστασης, ο εντοπισμός των αιτιών και ο γρήγορος εντοπισμός λύσεων είναι πολύ σημαντικά για την αποφυγή σοβαρού προβλήματος στον οργανισμό, σε περίπτωση που η αναφορά για περιστατικό είναι αληθείς. Ο εντοπισμός περιστατικού ασφάλειας μπορεί να γίνει μέσω λογισμικού αυτόματης ανάλυσης αρχείων καταγραφής, μέσω αναχωμάτων ασφαλείας, μέσω συστημάτων ανίχνευσης ή μέσω λογισμικού προστασίας του συστήματος από ιούς (antivirus). Είναι επίσης σημαντικό, οι υπάλληλοι του οργανισμού να γνωρίζουν το σχέδιο αντιμετώπισης και να μπορούν να ανταπεξέλθουν κατάλληλα την ώρα του συμβάντος. Σε αυτή τη φάση λοιπόν γίνονται τα εξής βήματα:

- Ανάθεση της ευθύνης χειρισμού του περιστατικού
- Επιβεβαίωση αναφοράς ύπαρξης περιστατικού
- Καθορισμός ατόμων που θα συλλέξουν τα δεδομένα του περιστατικού, τα οποία μπορεί να αποτελέσουν αποδεικτικά στοιχεία
- Καθορισμός σοβαρότητας του περιστατικού

Μετά τον εντοπισμό ενός περιστατικού και αφού επιβεβαιωθεί ότι είναι αληθές, ακολουθεί η φάση της αναχαίτισης. Η ομάδα διαχείρισης των περιστατικών θα αναλάβει δράση για να περιορίσει την έκθεση του οργανισμού και των ζημιών. Ανάλογα με το είδος της παραβίασης θα εκτελέσει τις κατάλληλες ενέργειες. Αν το περιστατικό σχετίζεται με κακόβουλο λογισμικό, θα αποσυνδεθούν τα επηρεαζόμενα μέρη του συστήματος. Αν πρόκειται για κάποιον εισβολέα στο δίκτυο, θα περιοριστεί ένα τμήμα του δικτύου και θα απενεργοποιηθούν προσωρινά οι ευάλωτοι λογαριασμοί. Αν υπάρχει επίθεση άρνησης υπηρεσίας, θα εντοπιστούν οι πηγές της επίθεσης και θα απαγορευτεί η πρόσβαση στο δίκτυο. Τέλος, αν έχει παραβιαστεί η ασφάλεια κάποιοι εξυπηρετητή, θα απενεργοποιηθεί η επικοινωνία με άλλους εξυπηρετητές. Γενικά σε αυτή τη φάση:

- Ενεργοποιείται η ομάδα διαχείρισης και αντιμετώπισης περιστατικών
- Ειδοποιούνται οι ανώτεροι του οργανισμού για το περιστατικό
- Εγκρίνονται δράσεις που θα επιτρέψουν την άμεση αντιμετώπιση
- Υλοποιούνται οι δράσεις αναχαίτισης
- Συλλέγονται και φυλάσσονται στοιχεία σχετικά με το περιστατικό
- Τεκμηριώνεται κάθε ενέργεια και λαμβάνονται αντίγραφα ασφαλείας

Η τέταρτη φάση της αντιμετώπισης περιστατικών ασφάλειας είναι η φάση της Εξάλειψης η οποία θεωρείται η πιο απλούστερη. Μετά την ολοκλήρωση της φάσης αναχαίτισης, είναι απαραίτητος ο εντοπισμός των αιτιών που προκάλεσαν το περιστατικό. Οι αιτίες μπορεί να εξαλειφθούν με την αποκατάσταση των συστημάτων μέσω αντιγράφων ασφαλείας, μέσω της απομάκρυνσης τους, μέσω της

βελτίωσης της άμυνας ή μέσω της διεξαγωγής ανάλυσης των ευπαθειών του συστήματος. Συνοπτικά, στην φάση της εξάλειψης:

- Καθορίζονται οι ενδείξεις και τα αίτια του περιστατικού
- Εντοπίζονται τα αντίγραφα ασφαλείας
- Απομακρύνονται τα αίτια του περιστατικού
- Βελτιώνεται η άμυνα με την υλοποίηση μέτρων προστασίας
- Διεξάγονται αναλύσεις ευπαθειών

Αμέσως μετά ακολουθεί η φάση της Ανάκαμψης, στην οποία πρέπει ο οργανισμός να επανέλθει στα φυσιολογικά του πλαίσια και στην κανονική του λειτουργία, όπως ορίζει το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών του. Συγκεκριμένα σε αυτή τη φάση:

- Επαναφέρονται όλες οι λειτουργίες στην κανονική τους κατάσταση
- Επικυρώνεται η επιτυχία των ενεργειών αποκατάστασης
- Ελέγχεται η σωστή λειτουργία των συστημάτων
- Εξασφαλίζεται η κατάσταση κανονικής λειτουργίας των συστημάτων

Η τελευταία φάση είναι αυτή της Ανασκόπησης, η οποία είναι αρκετά σημαντική καθώς χρειάζεται να γίνει μια συνολική εκτίμηση του περιστατικού. Δημιουργείται μια έκθεση μέσω της οποίας η ομάδα αντιμετώπισης του περιστατικού ενημερώνει τον οργανισμό για το περιστατικό, τι ακριβώς συνέβη, ποια μέτρα πάρθηκαν και ποια ήταν τα αποτελέσματα. Γενικά λοιπόν, σε αυτή τη φάση γίνονται τα εξής βήματα:

- Συντάσσεται μια έκθεση για το περιστατικό
- Υπολογίζεται το κόστος του περιστατικού
- Αναλύονται τα θέματα που προέκυψαν κατά την αντιμετώπιση του
- Προτείνονται βελτιώσεις για την καλύτερη προστασία
- Δημοσιοποιείται η έκθεση στους μετόχους του οργανισμού

Ένα περιστατικό παραβίασης ασφάλειας είναι μεγάλο πρόβλημα για έναν οργανισμό. Γι’ αυτό και οφείλει να λάβει τα απαραίτητα μέτρα για την προστασία των συστημάτων του. Σε αυτό βοηθάει η δημιουργία ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Ταυτόχρονα, σε περίπτωση περιστατικού ασφάλειας, ο οργανισμός θα πρέπει να είναι σε θέση να ανταπεξέλθει άμεσα για να αντιμετωπίσει το ζήτημα, έτσι ώστε να μην υπάρξει σημαντικό πρόβλημα ως προς την λειτουργία του συστήματος του αλλά και ως προς τις πληροφορίες του. Τα κατάλληλα μέτρα και οι τρόποι αντιμετώπισης που παρέχονται, βοηθούν αποτελεσματικά στην διαχείριση και αντιμετώπιση περιστατικών ασφάλειας.

4

Μέθοδος της έρευνας και περιστατικά παραβίασης δεδομένων

Σε αυτό το κεφάλαιο θα αναλυθεί η μέθοδος της έρευνας, η οποία έγινε για την συγκέντρωση των περιστατικών που έχουν δημοσιευθεί και σχετίζονται με την παραβίαση των προσωπικών δεδομένων σε μεγάλες εταιρείες και υπηρεσίες. Στη συνέχεια, υπάρχει εξήγηση των περιπτώσεων και κατηγοριοποίηση τους. Τέλος, διευκρινίζεται πως ο ανθρώπινος παράγοντας επηρέασε αυτά τα περιστατικά και γενικά πως το ανθρώπινο λάθος μπορεί να οδηγήσει σε παραβίαση των προσωπικών δεδομένων των χρηστών.

4.1 Μέθοδος έρευνας

Ο σκοπός αυτής της εργασίας είναι η συγκέντρωση των μεγαλύτερων περιστατικών παραβίασης δεδομένων που έχουν καταγραφεί και ο εντοπισμός του ανθρώπινου λάθους στην κάθε περίπτωση. Η έρευνα λοιπόν, αρχικά ξεκίνησε με την συγκέντρωση πληροφοριών σχετικά με τα περιστατικά παραβίασης δεδομένων. Έγινε αναζήτηση των όρων «data breach», «published data breaches», «security incidents», «data breaches and human error» και διάφορων παρόμοιων για τον εντοπισμό της βιβλιογραφίας.

Καθώς τα αποτελέσματα της αναζήτησης ήταν χιλιάδες, έπρεπε να γίνει κάποιος περιορισμός ως προς το εύρος της βιβλιογραφίας που θα χρησιμοποιηθεί. Ένας πρώτος περιορισμός που επιλέχθηκε να γίνει ήταν με βάση την χρονολογία των περιπτώσεων. Περιστατικά παραβίασης δεδομένων μπορούν να βρεθούν ακόμα και δέκα χρόνια πριν, παρόλα αυτά δεν είναι χρήσιμα για την παρούσα έρευνα. Γι’ αυτό τον λόγο

επιλέχθηκαν όσα περιστατικά συνέβησαν την τελευταία πενταετία, από το 2014 έως το 2019. Για να μειωθεί ακόμη περισσότερο ο όγκος των αποτελεσμάτων, χρειάστηκε να περιοριστούν οι περιπτώσεις και ως προς το σύνολο των δεδομένων, το οποία είτε κλάπηκαν είτε τέθηκαν σε κίνδυνο. Για τους σκοπούς της έρευνας, δεν θα ήταν απαραίτητα περιστατικά στα οποία υπήρξε σχετικά μικρή απώλεια δεδομένων, επομένως, επιλέχθηκαν περιπτώσεις όπου ο αριθμός των δεδομένων που διακυβεύτηκαν ήταν από 500.000 και πάνω, για να μπορέσουν να επιλεχθούν τα πιο σημαντικά περιστατικά.

Μετά τον περιορισμό της βιβλιογραφίας, βρέθηκε ότι υπήρξαν πάρα πολλές παραβιάσεις δεδομένων την τελευταία πενταετία και σε πάρα πολλούς τομείς. Κατόπιν αναζήτησης στο Google scholar, παρατηρήθηκε ότι δεν έχουν γραφτεί πολλά επιστημονικά κείμενα σχετικά με τα data breaches, ενώ όσα υπάρχουν, αναφέρονται κυρίως στην αντιμετώπιση και αποφυγή τέτοιων καταστάσεων, καθώς επίσης αρκετά από αυτά τα κείμενα σχετίζονται με την νεφοϋπολογιστική (cloud computing). Με αυτό τον τρόπο, η έρευνα περιορίστηκε στην αναζήτηση ιστότοπων που αναφέρουν τι έγινε σε κάθε περιστατικό.

Για να θεωρηθούν αξιόπιστες οι πηγές, επειδή προέρχονται από διαδικτυακούς ιστότοπους, έπρεπε να προέρχονται από γνωστές και μεγάλες ιστοσελίδες. Προτιμήθηκαν κυρίως ιστοσελίδες μεγάλων εφημερίδων του εξωτερικού, όπως οι New York Times, The Washington Post, US Today και The Guardians, αλλά και άλλες γνωστές ιστοσελίδες ενημέρωσης όπως το BBC, το CNN, το Forbes, το CNBC κ.α. Σε κάποιες περιπτώσεις επιλέχθηκαν, με επιφύλαξη, ιστότοποι που σχετίζονται με θέματα τεχνολογίας όπως το techcrunch.com ή το cnet.com.

Παρατηρήθηκε το γεγονός ότι στα περισσότερα περιστατικά, δεν έχει δημοσιευθεί λεπτομερώς ο τρόπος με τον οποίο έγινε η παραβίαση των δεδομένων, καθώς στις ιστοσελίδες αναφέρεται κυρίως ότι υπήρξε υποκλοπή από επιτιθέμενο (hacker), χωρίς όμως να εξηγούν το πώς κατάφερε να αποκτήσει πρόσβαση στα δεδομένα. Η έλλειψη τέτοιων λεπτομερειών είναι κατανοητή λόγω του ότι το άρθρο απευθύνεται σε άτομα τα οποία δεν γνωρίζουν τεχνικούς όρους της πληροφορικής και της τεχνολογίας, παρόλα αυτά σε επίπεδο έρευνας, αποτελεί κάποιο πρόβλημα, καθώς περιορίζει τις πληροφορίες που μπορούν να συλλεχθούν για το κάθε περιστατικό.

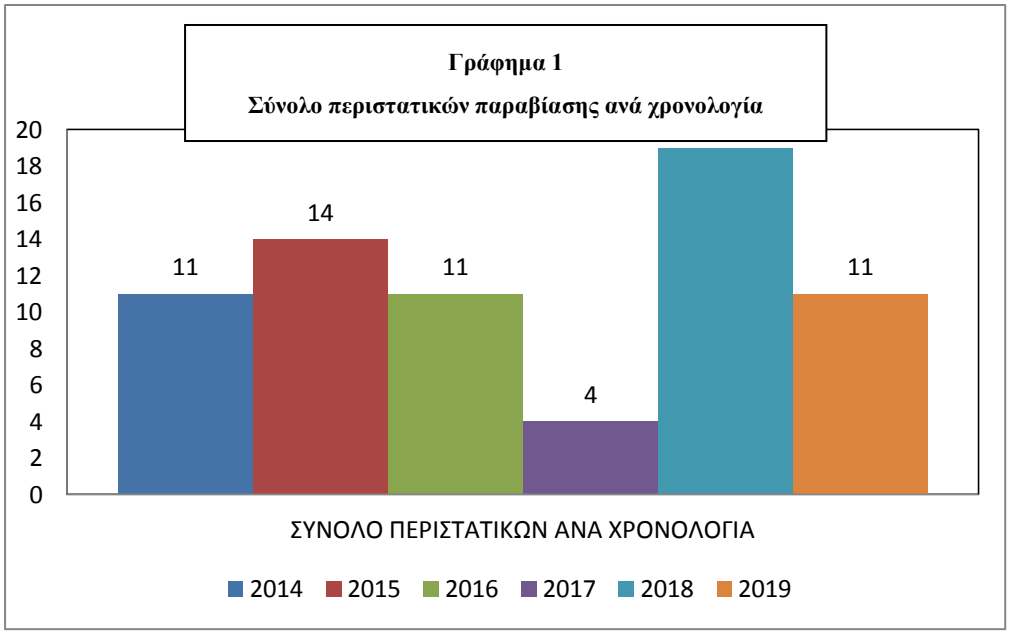
Με την ολοκλήρωση της συλλογής της βιβλιογραφίας, έγινε καταγραφή των περιστατικών που συγκεντρώθηκαν και κατηγοριοποίηση τους. Τοποθετήθηκαν σε πίνακα όπου περιείχε την χρονολογία αλλά και την ακριβή ημερομηνία του γεγονότος, τα αίτια που οδήγησαν στην παραβίαση, ο τρόπος με τον οποίο έγινε, το πώς αντιμετωπίστηκε, καθώς και το κόστος που είχε για την κάθε εταιρεία είτε αυτό ήταν οικονομικό είτε υλικό. Στη συνέχεια, τα περιστατικά, κατηγοριοποιήθηκαν με βάση τον τομέα στον οποίο βρίσκεται η κάθε περίπτωση, για παράδειγμα αν πρόκειται για μια ιστοσελίδα, ομαδοποιήθηκε στην κατηγορία web, ενώ αν πρόκειται για κάποιο νοσοκομείο, στην κατηγορία healthcare. Αναλυτικά, θα αναφερθούν παρακάτω οι κατηγορίες και ο τρόπος ταξινόμησης.

Τέλος, μετά την ταξινόμηση των περιστατικών, δημιουργήθηκαν κάποιοι πίνακες και γραφήματα, τα οποία θα βοηθήσουν στην καλύτερη εικόνα των περιστατικών και θα αναλυθούν στη συνέχεια.

4.2 Δημοσιοποιημένα περιστατικά παραβίασης δεδομένων

Με την ολοκλήρωση της συγκέντρωσης της βιβλιογραφίας των περιστατικών, επιλέχθηκαν 70 περιπτώσεις οι οποίες θα χρησιμοποιηθούν τελικά στην έρευνα. Υπάρχουν πολλές περισσότερες, παρόλα αυτά, περιορίστηκαν σε έναν ικανοποιητικό αριθμό που μπορεί να αξιοποιηθεί τόσο για ποσοτική όσο και για ποιοτική έρευνα.

Οι περιπτώσεις μελετήθηκαν και κατηγοριοποιήθηκαν ανάλογα με το περιεχόμενο τους. Για μια πρώτη οργάνωση, δημιουργήθηκε ο πίνακας 1, στον οποίο τοποθετήθηκαν τα περιστατικά με βάση την χρονολογία στην οποία συνέβησαν. Παρατηρείται, όπως φαίνεται και στο γράφημα 1, ότι από τις 70 περιπτώσεις, οι περισσότερες συνέβησαν το 2015 και το 2018 ενώ το 2017 υπήρξαν τα λιγότερα περιστατικά. Παρόλα αυτά, είναι σημαντικό να αναφερθεί ότι και το 2019 έγιναν πολλές παραβιάσεις δεδομένων, κάτι που αποδεικνύει ότι ακόμα και σήμερα δεν έχουν λυθεί πολλά από τα ζητήματα ασφαλείας που υπάρχουν ως προς την προστασία των προσωπικών δεδομένων. Επίσης, υπάρχουν περιπτώσεις, όπως αυτή του Facebook, όπου αντιμετώπισαν πρόβλημα τουλάχιστον δύο φορές και μάλιστα μέσα σε σύντομο χρονικό διάστημα.



Πίνακας 1

Περιστατικά παραβίασης δεδομένων με βάση την χρονολογία

2014	2015	2016	2017	2018	2019
Domino's Pizza (France)	SLACK	Nival Networks	Bell Canada	Google Plus	Health sciences authority
Neiman Marcus	Internal revenue service	Verizon communications	Timehop	Orbitz	Desjardins
AOL	Carefirst bluecross blue shield	21st Century Oncologe	Taringa!	T-Mobile	STOCKX
Michaels	PATREON	SNAPCHAT	EQUIFAX	Earl Enterprises	Quest diagnostics
Community health systems	Medical informatics engineering	TAOBAO		Cathay pacific airways	JUSTIDIAL
GMAIL	SCOTTRADE	MySpace		CAREEM	Mobile Telesystems (MTS)
Korea Credit Bureau	Ucla Medical Center	Weebly		TYCKETFLY	CAPITAL ONE
HOME DEPOT	VTECH	Philippines commission on elections		HAUTELOOK	TRUECALLER
JP Morgan Chase	Excellus Bluecross Blueshield	UBER		PANERA	Facebook
eBay	Primera	Friend Finder Networks		Facebook	First American Corporation
Yahoo	Experian T-Mobile US	EYEWIRE		United States Postal Service	
	US Office of Personnel Management			MYHERITAGE	
	Ashley Madison			Quora	
	Anthem INC			Under Armour	
				Twitter	
				Marriot International	
				SingHealth	
				REDDIT	
				TYPEFORM	

Αξίζει να αναφερθεί ότι στα περισσότερα από τα παραπάνω περιστατικά παραβίασης δεδομένων, υπάρχει μια μεγάλη διαφορά ως προς τις ημερομηνίες στις οποίες συνέβη το περιστατικό και τις ημερομηνίες στις οποίες η κάθε εταιρεία εντόπισε ότι υπάρχει πρόβλημα. Οι εταιρείες χρησιμοποιούν κάποιους μηχανισμούς ασφαλείας για την προστασία των δεδομένων τους. Παρόλα αυτά όμως, ελάχιστες μπόρεσαν να εντοπίσουν εγκαίρως την παραβίαση που τους συνέβη. Αυτό αποτελεί σημαντικό πρόβλημα σχετικά με την ασφάλεια των συστημάτων και των πληροφοριών και είναι κάτι το οποίο πρέπει να διερευνηθεί και να επιλυθεί για την αποφυγή παρόμοιων ή χειρότερων περιστατικών. Ενδεικτικό παράδειγμα είναι η περίπτωση της Scottrade (Frank, 2015; Pagliery, 2015; Weise, 2015). Η Scottrade είναι μια χρηματιστηριακή εταιρεία, όπου οι επιτιθέμενοι είχαν αποκτήσει πρόσβαση στην ενιαία βάση δεδομένων της από τα τέλη του 2013 και συνέχισαν να έχουν πρόσβαση μέχρι τον Οκτώβριο του 2015 όταν ανακαλύφθηκε η παραβίαση.

Άλλη μια περίπτωση είναι η εταιρεία Orbitz (Brook, 2018; Cluley, 2018; Locklear, 2018). Η Orbitz είναι ένας ιστότοπος που προσφέρει ταξιδιωτικές υπηρεσίες. Τον Οκτώβριο του 2017, οι επιτιθέμενοι απέκτησαν πρόσβαση στις πληροφορίες των χρηστών της εταιρείας και υπέκλεψαν στοιχεία από το 2016. Το πρόβλημα εντοπίστηκε τον Μάρτιο του 2018. Ένα ακόμα παράδειγμα αποτελεί η παραβίαση της Carefirst Bluecross Blue Shield- Maryland (Goldman, 2015; Krebs, 2015; Vintom, 2015), η οποία είναι ένας ασφαλιστικός φορέας παροχής υγειονομικής περίθαλψης. Στις 21 Απριλίου του 2015 ανακαλύφθηκε ότι υπήρχε παραβίαση των δεδομένων από τον Ιούνιο του 2014 και τον Μάιο του 2015 δόθηκε στην δημοσιότητα το γεγονός.

Ένα περιστατικό το οποίο δεν συνέβη στο Διαδίκτυο, είναι αυτό της Earl Enterpises (Abel, 2019; Cain, 2019; Liptak, 2019), η οποία είναι μια εταιρεία εστιατορίων. Στο συγκεκριμένο συμβάν, οι επιτιθέμενοι εγκατέστησαν malware σε σημείο πώλησης κάποιου εστιατορίου και απέκτησαν έτσι πρόσβαση σε δεδομένα, όπως για παράδειγμα αριθμούς πιστωτικών καρτών. Η υποκλοπή γινόταν από τον Μάιο του 2018 και παρόλο που εντοπίστηκε τον Φεβρουάριο του 2019, συνεχίστηκε μέχρι τον Μάιο του 2019.

Επίσης χαρακτηριστικό παράδειγμα αποτελεί και η παραβίαση της Excellus Bluecross Blue Shield (Blake, 2015; McCann, 2015; Warwick, 2015), στην οποία οι επιτιθέμενοι είχαν πρόσβαση στη βάση δεδομένων για δύο χρόνια, καθώς η επίθεση ξεκίνησε τον Δεκέμβριο του 2013 και εντοπίστηκε τον Αύγουστο του 2015. Τα δεδομένα περιπτώσεων όπως αυτής της παραβίασης που σχετίζονται με ιατρικά θέματα, είναι εύκολος στόχος των επιτιθέμενων, διότι μπορούν να τα πουλήσουν σε διάφορες διαφημιστικές εταιρείες.

Από την άλλη πλευρά υπάρχουν και περιπτώσεις στις οποίες δεν γίνεται κάποια επίθεση από κακόβουλο αλλά κάποιος εσωτερικός υπάλληλος της εταιρείας κινείται απειλητικά έναντι της εταιρείας. Στην περίπτωση της Korea Credit Bureau (Osbome, 2014; Yans and Kwan, 2014), μιας υπηρεσίας συλλογής δεδομένων, ένας από τους εργαζόμενους της, αντέγραψε την βάση δεδομένων και την πούλησε

σε διαφημιστικές εταιρείες. Η παραβίαση διήρκησε μεγάλο χρονικό διάστημα, από τον Μάιο του 2012 έως τον Δεκέμβριο του 2013, ενώ το πρόβλημα εντοπίστηκε μόλις τον Ιανουάριο του 2014.

Το Timehop (Burgess, 2018; Chin, 2018; TimeHop, 2018) είναι μια εφαρμογή για κινητά όπου συλλέγει δεδομένα, κυρίως φωτογραφίες, από άλλα μέσα κοινωνικής δικτύωσης. Από τον Δεκέμβριο του 2017 μέχρι τον Ιούλιο του 2018, όπου και ανακαλύφθηκε το πρόβλημα, ένας επιτιθέμενος κατάφερε να αποκτήσει τα στοιχειά σύνδεσης ενός υπαλλήλου και στη συνεχεία αντιγράφοντας τα API, απέκτησε πρόσβαση στα δεδομένα της εφαρμογής.

Κάτι παρόμοιο συνέβη και στο Facebook (O'Flaherty, 2018; Perez and Whittake, 2018; Wong, 2018), καθώς ο επιτιθέμενος κατάφερε μέσω ευπαθειών του συστήματος να αποκτήσει πρόσβαση στα δεδομένα με την βοήθεια των APIs. Το περιστατικό έγινε τον Ιούλιο του 2017, ενώ η εταιρεία το αντιλήφθηκε τον Σεπτέμβριο του 2018. Αλλά και στην περίπτωση του 2019 (Utermohlen, 2019; Whittaker, 2019; Winder, 2019), τα δεδομένα βρέθηκαν εκτεθειμένα για τέσσερις μήνες και μπορούσε ο οποιοσδήποτε να έχει πρόσβαση σε αυτά.

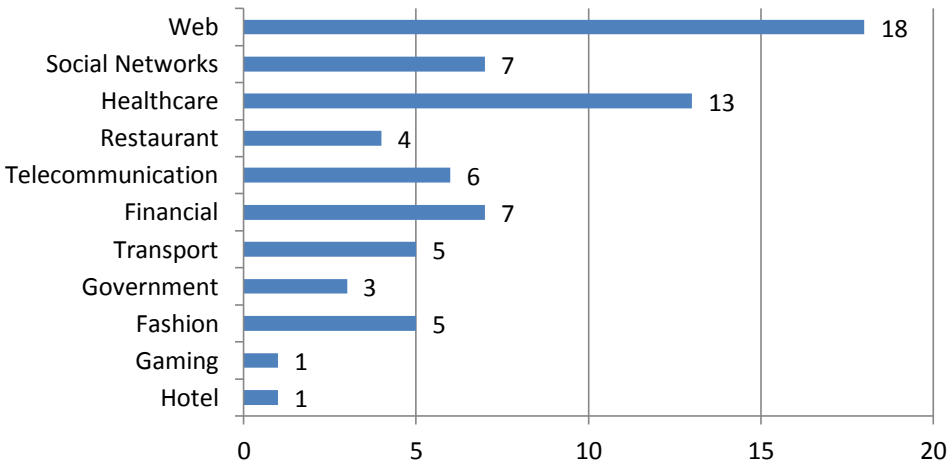
Αυτά είναι μόνο κάποια από τα παραδείγματα των παραβιάσεων που δείχνουν την έλλειψη ασφάλειας σε πολλές εταιρείες και κυρίως το πρόβλημα που υπάρχει ως προς τον εντοπισμό των απειλών και των επιθέσεων που μπορεί να δέχονται. Τα διαστήματα που μεσολάβησαν από την αρχή των επιθέσεων μέχρι τον εντοπισμό τους είναι αρκετά μεγάλα για να δημιουργήσουν τεράστια προβλήματα στην λειτουργία, την αξιοπιστία και την ασφάλεια μιας εταιρείας. Επίσης, το γεγονός ότι τα περιστατικά αυτά είναι πρόσφατα χρονολογικά, υποδεικνύει ότι υπάρχει μεγάλη έλλειψη σωστής ενημέρωσης και ασφαλών μέτρων των εταιρειών για την διασφάλιση των δεδομένων τους.

Σε όλες αυτές τις περιπτώσεις, τα δεδομένα τα οποία είτε βρίσκονται σε κίνδυνο είτε έχουν κλαπεί, είναι σχεδόν κάθε φορά συγκεκριμένα. Από τα πιο εύκολα δεδομένα για να διαρρεύσουν είναι τα ονοματεπώνυμα των χρηστών, τα usernames, τα emails και οι κωδικοί πρόσβασης, με ή χωρίς προστασία τους. Σε πολλές περιπτώσεις επίσης, ειδικά όταν πρόκειται για ιστοσελίδες ή φυσικά καταστήματα στα οποία πραγματοποιούνται χρηματικές συναλλαγές, τα δεδομένα που διακυβεύονται είναι οι αριθμοί πιστωτικών και χρεωστικών καρτών. Εξίσου σημαντικά για να κινδυνεύσουν θεωρούνται και οι διευθύνσεις κατοικίας, οι αριθμοί τηλεφώνων, οι ημερομηνίες γέννησης και οι αριθμοί κοινωνικής ασφάλισης. Αυτά και παρόμοια δεδομένα είναι οι στόχοι των επιτιθέμενων καθώς μπορούν να τα εκμεταλλευτούν προς όφελος τους. Επίσης, χρειάζονται προστασία γιατί είναι πολύ εύκολο να χαθούν από τα πληροφοριακά συστήματα και να δημιουργήσουν πρόβλημα στην λειτουργία του οργανισμού.

Στην συνέχεια της έρευνας, έγινε ταξινόμηση των περιστατικών με βάση τον τομέα με τον οποίο σχετίζεται η κάθε εταιρεία. Βασικός σκοπός είναι η ομαδοποίηση των περιστατικών σε γενικές κατηγορίες, κυρίως για την αποφυγή πολλών μικρών υποκατηγοριών που θα περιέχουν από ένα περιστατικό. Οι κατηγορίες που δημιουργήθηκαν είναι: Ιστοσελίδες (Web), στις οποίες περιλήφθηκαν περιστατικά που έγιναν μέσω Διαδικτυακών ιστότοπων, Μέσα Κοινωνικής Δικτύωσης (Social Networks), τα οποία περιλαμβάνουν όσες εφαρμογές, είτε στο Διαδίκτυο είτε σε συσκευές, αποτελούν μέσο κοινωνικής

δικτύωσης, Τομείς υγείας (Healthcare), που περιλαμβάνουν όσα περιστατικά σχετίζονται με υπηρεσίες υγείας, Εστίαση (Restaurant), τηλεπικοινωνίες (Telecommunications), Οικονομικά (Financial), στα οποία περιέχονται όσες περιπτώσεις έχουν σχέση με οικονομικές εταιρείες ή υπηρεσίες, Μεταφορές (Transport), κυρίως για αεροπορικές εταιρείες, Κυβερνητικές υπηρεσίες (Government), για οτιδήποτε σχετίζεται με εταιρείες ή οργανισμούς που μπορεί να έχουν σχέση με την κυβέρνηση, Μόδα (Fashion), για τις εταιρείες ρούχων και Gaming και Ξενοδοχεία (Hotel), για δύο μεμονωμένα περιστατικά.

Γράφημα 2
Σύνολο περιστατικών παραβίασης ανά κατηγορία



Στην κατηγορία Web, συμπεριλήφθηκαν και περιστατικά που έχουν σχέση με εταιρείες online αγορών καθώς και διάφορες εταιρείες παραγωγής προϊόντων. Όπως παρατηρείται και στο γράφημα 2, τα περισσότερα περιστατικά συνέβησαν σε ιστοσελίδες (18 παραβιάσεις), σε υπηρεσίες υγείας (13 παραβιάσεις), σε μέσα κοινωνικής δικτύωσης και σε εταιρείες που σχετίζονται με οικονομικά θέματα (7 παραβιάσεις αντίστοιχα).

Στην περίπτωση των ξενοδοχειακών επιχειρήσεων Marriot International (Marriot International, 2018; Sweney, 2019; Volodzko, 2018), η εταιρεία ενημερώθηκε για μη εξουσιοδοτημένη πρόσβαση στη βάση δεδομένων της, στην οποία διατηρούσε στοιχεία για χρήστες που συνδέονταν ως guest λογαριασμοί για τις κρατήσεις τους. Εντοπίστηκε όμως ότι το πρόβλημα ίσως είχε ξεκινήσει πριν από 4 χρόνια. Η κίνηση της εταιρείας για την επίλυση του θέματος ήταν η δημιουργία μιας ιστοσελίδας μέσω της οποίας ενημέρωσαν τους χρήστες για την παραβίαση των δεδομένων.

Παράλληλα, στην κατηγορία gaming, η Nival Networks (Cyber Insurance, 2016; Franceshi-Bichierai, 2016) αντιμετώπισε σοβαρότερο πρόβλημα. Τα άτομα που βρίσκονταν πίσω από την επίθεση

ισχυρίζονται ότι η συγκεκριμένη παραβίαση έγινε ως διαμαρτυρία ενάντια στην εξωτερική πολιτική της Ρωσίας ως προς την Ουκρανία, σε κάποια γεγονότα που συνέβαιναν το 2016.

Στην κατηγορία των κυβερνητικών υπηρεσιών υπάρχουν τρία περιστατικά τα οποία αξίζει να αναφερθούν. Το πρώτο περιστατικό είναι η περίπτωση της US Office of Personnel Management (Fruhlinge, 2018; Koerner, 2016; Krebs, 2016) μιας ανεξάρτητης υπηρεσίας που διαχειρίζεται το εργατικό δυναμικό της κυβέρνησης. Αρχικά οι επιτιθέμενοι κατάφεραν να πάρουν πληροφορίες για την αρχιτεκτονική του συστήματος. Στη συνέχεια εγκατέστησαν malware και σταδιακά αποκτούσαν πρόσβαση σε πολλά δεδομένα. Η παραβίαση αυτή είχε ως αποτέλεσμα να παραιτηθούν κάποια από τα κορυφαία στελέχη της υπηρεσίας και το θέμα διερευνήθηκε από το Κογκρέσο.

Το επόμενο κυβερνητικό περιστατικό αφορά τις Philippines Commission on Elections (Chi, 2016; Hern, 2016; Temperton, 2016), την παραβίαση δηλαδή που πραγματοποιήθηκε στις εκλογές των Φιλιππίνων. Στις 27 Μαΐου 2016, οι επιτιθέμενοι κατάφεραν να αποκτήσουν πρόσβαση σε πέντε πεδία της βάσης δεδομένων των ψηφοφόρων και απείλησαν μέσω Facebook για δημοσιοποίηση των δεδομένων.

Το τρίτο περιστατικό παραβίασης δεδομένων, αφορά το US Postal Services (Gorey, 2018; Khondelwal, 2018; Krebs, 2018), όπου τον Νοέμβριο του 2018, μια αδυναμία που υπήρχε στο σύστημα, έδωσε την δυνατότητα σε όποιον είχε λογαριασμό να μπορεί να δει τις πληροφορίες των υπόλοιπων χρηστών. Η υπηρεσία προσπάθησε να λύσει το πρόβλημα, παρόλα αυτά, τα δεδομένα βρέθηκαν εκτεθειμένα.

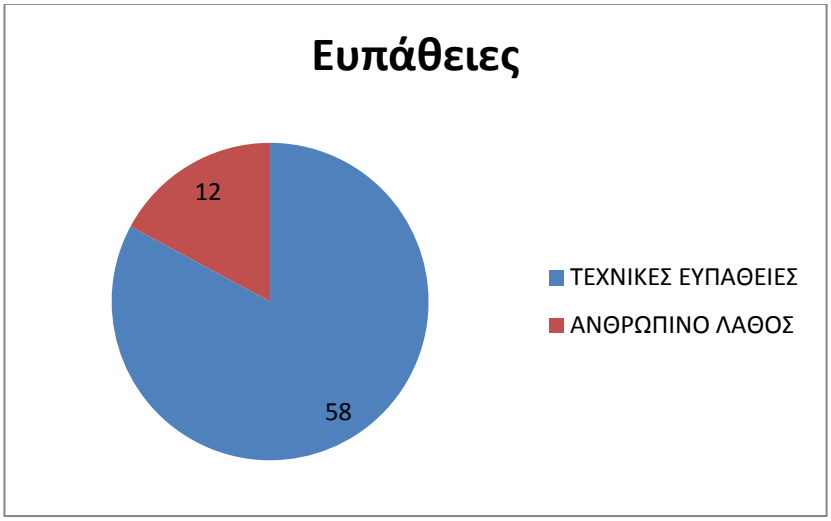
Παρατηρείται το φαινόμενο, πολλές εταιρείες να έχουν προβλήματα και κενά ασφάλειας στα συστήματα τους, χωρίς όμως να το γνωρίζουν ότι υπάρχει κάποιο θέμα. Αυτό δίνει την δυνατότητα στους επιτιθέμενους να εκμεταλλευτούν την οποιαδήποτε ευπάθεια εντοπίσουν στο σύστημα και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε βάσεις δεδομένων και προσωπικές πληροφορίες.

Μια ακόμα κατηγοριοποίηση των δεδομένων έγινε ως προς τις ευπάθειες που επηρέασαν και κατ' επέκταση οδήγησαν σε παραβίαση. Οι ευπάθειες χωρίστηκαν με βάση την προέλευση τους, σε τεχνικές ευπάθειες και στον παράγοντα του ανθρώπινου λάθους. Οι τεχνικές ευπάθειες περιλαμβάνουν όλες τις περιπτώσεις στις οποίες υπήρχε κάποιο πρόβλημα στο πληροφοριακό σύστημα, κυρίως εξαιτίας της έλλειψης ασφάλειας του. Στο γράφημα 3, παρατηρείται ότι τα περισσότερα περιστατικά οφείλονται σε τεχνικές ευπάθειες, γεγονός που αποδεικνύει ότι οι εταιρείες έχουν σημαντική έλλειψη ασφάλειας ως προς τα συστήματα τους. Αυτό που αποτελεί βασικό ενδιαφέρον στην έρευνα είναι οι περιπτώσεις στις οποίες ο ανθρώπινος παράγοντας ήταν αυτός που οδήγησε στην παραβίαση των δεδομένων. Όπως φαίνεται και στο γράφημα, από τις 70 περιπτώσεις που συγκεντρώθηκαν, μόνο οι 12 προέρχονται από ανθρώπινο λάθος και αυτό οφείλεται στο γεγονός ότι οι περισσότερες παραβιάσεις έγιναν μέσω κακόβουλης επίθεσης (χακάρισμα), το οποίο προκύπτει από την έλλειψη ασφάλειας των συστημάτων και από τις ευπάθειες τους.

Από το σύνολο των περιστατικών που μελετήθηκαν, τα 56 προήλθαν από χακάρισμα του συστήματος. Στις περισσότερες περιπτώσεις, οι επιτιθέμενοι μπόρεσαν να εκμεταλλευτούν όποιες ευπάθειες είχε το εκάστοτε σύστημα και να αποκτήσουν πρόσβαση στη βάση δεδομένων της εταιρείας.

Υπήρξαν επίσης περιπτώσεις, στις οποίες οι επιτιθέμενοι είχαν προσχεδιάσει την επίθεση τους, ενώ σε άλλες περιπτώσεις εκμεταλλεύτηκαν την χρήση τερματικών μηχανημάτων σε φυσικά καταστήματα για να υποκλέψουν τις πληροφορίες.

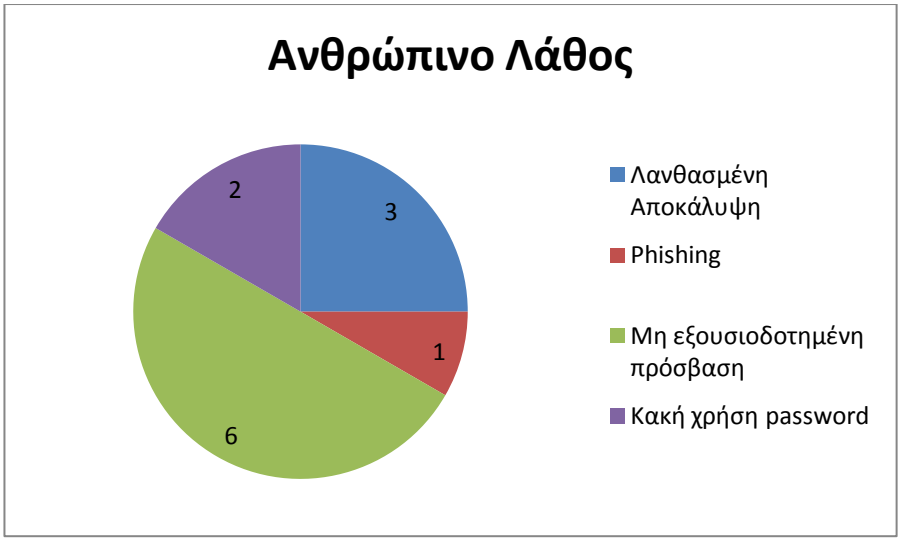
Γράφημα 3, Ευπάθειες περιστατικών παραβίασης



Παράλληλα, αρκετοί επιτιθέμενοι απείλησαν μεγάλες εταιρείες για δημοσίευση των δεδομένων, ζητώντας τους λύτρα μεγάλου μεγέθους. Οι κακόβουλες επιθέσεις, χακάρισμα, είναι οι πιο συχνές επιθέσεις σε πληροφοριακά συστήματα. Επιπλέον, υπάρχουν και οι περιπτώσεις όπου οι ευπάθειες του συστήματος οδηγούν σε διαρροή των δεδομένων. Πολλές φορές έχει γίνει διαρροή των δεδομένων του συστήματος της εταιρείας και η ίδια η εταιρεία δεν γνώριζε πως υπήρχε πρόβλημα. Αυτό όμως έχει ως αποτέλεσμα, τα δεδομένα να βρίσκονται εκτεθειμένα σε κίνδυνο, γεγονός που επηρεάζει την αξιοπιστία της εταιρείας λόγω έλλειψης ασφάλειας.

Όπως αναφέρθηκε, το βασικό ζήτημα της έρευνας, είναι η συσχέτιση του ανθρώπινου λάθους στις περιπτώσεις παραβίασης των δεδομένων. Παρακάτω, παρουσιάζεται ένα γράφημα με τους τρόπους όπου ο ανθρώπινος παράγοντας υπήρξε καθοριστικός.

Γράφημα 4, Ανθρώπινο λάθος στα περιστατικά παραβίασης



Παρόλο που στην συγκεκριμένη έρευνα εντοπίστηκε μικρό ποσοστό περιπτώσεων παραβίασης δεδομένων οι οποίες να οφείλονται στον ανθρώπινο παράγοντα, υπήρξε αρκετή ποικιλία ως προς το είδος του ανθρώπινου λάθους. Από τα 12 περιστατικά που συγκεντρώθηκαν, τα έξι προέρχονται από μη εξουσιοδοτημένη πρόσβαση. Χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση της εταιρείας Desjardins (Connoly, 2019; Tomesco, 2019), όπου τον Δεκέμβριο του 2018, ένας από τους υπαλλήλους της απέκτησε πρόσβαση στη βάση δεδομένων έχοντας κακόβουλο σκοπό. Η εταιρεία για να αντιμετωπίσει την παραβίαση, απέλυσε τον υπάλληλο και πρόσθεσε επιπλέον μέτρα ασφάλειας στο σύστημα της.

Παρόμοια περίπτωση είναι και η εταιρεία Korea Credit Bureau (BBC Technology News, 2014), στην οποία κακόβουλος υπάλληλος, έχοντας μη εξουσιοδοτημένη πρόσβαση στη βάση δεδομένων, αντέγραψε τις πληροφορίες του συστήματος και πούλησε τα δεδομένα σε εταιρείες μάρκετινγκ. Η παραβίαση εξελίσσονταν από τον Μάιο του 2012 έως τον Δεκέμβριο του 2013, ενώ η εταιρεία ανακάλυψε το γεγονός τον Ιανουάριο του 2014. Ως αποτέλεσμα της παραβίασης υπήρξε η σύλληψη του υπαλλήλου της εταιρείας αλλά και των διευθυντών των εταιρειών μάρκετινγκ που αγόρασαν τα δεδομένα.

Παρατηρείται ότι πολύ συχνά, παρόλο που εταιρείες δίνουν βάση στην προστασία των πληροφοριακών συστημάτων τους, αμελούν την προστασία τους από τον ανθρώπινο παράγοντα. Θα πρέπει να λαμβάνονται μέτρα για τις περιπτώσεις μη εξουσιοδοτημένης πρόσβασης έτσι ώστε να ελαττωθούν οι παρόμοιες ενέργειες.

Ένας άλλος παράγοντας ανθρώπινου λάθους είναι η λανθασμένη αποκάλυψη των δεδομένων. Στο γράφημα παρουσιάζονται τρεις παραβιάσεις σε αυτή την περίπτωση, στις οποίες οι αιτίες είναι διαφορετικές, όλες όμως οφείλονται σε λανθασμένη αποκάλυψη. Η πρώτη περίπτωση, είναι η εταιρεία Health Sciences Authority (Choo and Kurohi, 2019; Davis, 2019; Siew, 2019), στην οποία υπήρξε δημοσίευση λόγω έλλειψης επίγνωσης ασφάλειας του υπαλλήλου. Χρειάστηκε να περάσουν δύο μήνες για να εντοπίσει η εταιρεία ότι ένας από τους πωλητές δημοσίευσε την βάση δεδομένων στο Διαδίκτυο, χωρίς

να εξασφαλίσει την προστασία της από μη εξουσιοδοτημένη πρόσβαση. Στις 13 Μαρτίου του 2019, η εταιρεία ενημερώθηκε για το θέμα και απαίτησε από τον πωλητή να διαγράψει την βάση δεδομένων.

Εκτός από τους απλούς υπαλλήλους όμως, υπάρχουν και περιπτώσεις όπως αυτή του Facebook (Winder, 2019; Utermohlen, 2019), όπου οι προγραμματιστές της εταιρείας άφησαν απροστάτευτα τα δεδομένα στο cloud και μέσω αυτού ο οποιοσδήποτε μπορούσε να έχει πρόσβαση στις πληροφορίες των χρηστών. Η έκθεση των δεδομένων στο cloud διήρκησε περίπου τέσσερις μήνες, χωρίς η εταιρεία να γνωρίζει την ύπαρξη διαρροής.

Το τρίτο παράδειγμα που αξίζει να αναφερθεί είναι η περίπτωση κλοπής υλικού. Η εταιρεία Eyewire (Silversmith, 2016) έχει δημιουργήσει ένα παιχνίδι που χαρτογραφεί τον εγκέφαλο του χρήστη για επιστημονικούς σκοπούς. Το 2016, ένας υπάλληλος της εταιρείας βρισκόταν σε ένα συνέδριο και είχε μαζί του το λάπτοπ του, μέσα στο οποίο υπήρχε αντίγραφο της βάσης δεδομένων της εταιρείας. Το λαπτοπ κλάπηκε και ο επιτιθέμενος μπόρεσε να αποκτήσει πρόσβαση στα δεδομένα, χωρίς ιδιαίτερη δυσκολία. Η εταιρεία για να αντιμετωπίσει το θέμα ενημέρωσε τους χρήστες να αλλάξουν τους κωδικούς πρόσβασης τους και διέγραψε από τα δεδομένα της όσους κωδικούς είχαν επηρεαστεί.

Στους δύο επόμενους παράγοντες ανθρώπινου λάθους, υπάρχουν συγκεκριμένα περιστατικά. Στην περίπτωση της κακής χρήσης κωδικών πρόσβασης (password), έχουν εντοπιστεί δύο περιπτώσεις στις οποίες οι επιτιθέμενοι κατάφεραν να αποκτήσουν πρόσβαση στα δεδομένα εξαιτίας κάποιων υπαλλήλων που χρησιμοποιούσαν είτε πολύ απλούς κωδικούς πρόσβασης, είτε είχαν τον ίδιο κωδικό σε πολλές εφαρμογές, κάτι που διευκόλυνε αρκετά τους επιτιθέμενους για να τους παραβιάσουν. Στην περίπτωση της εταιρείας eBay (Gordon, 2014; Wakerfield, 2014), η επίθεση διήρκησε περίπου δύο μήνες και όταν εντοπίστηκε το πρόβλημα, προσλήφθηκαν ειδικοί για την αντιμετώπιση του. Στην περίπτωση του TimeHop (Lomas, 2018; TimeHop, 2018), η εταιρεία όταν ενημερώθηκε για την παραβίαση, απενεργοποίησε προληπτικά κάποια από τα δεδομένα για να περιοριστεί ο κίνδυνος.

Στην περίπτωση του μέσου κοινωνικής δικτύωσης Snapchat (Hern, 2016; King, 2016; Russell, 2016), ένας υπάλληλος έπεσε θύμα phishing, καθώς του ζητήθηκε να παραδώσει πληροφορίες μισθοδοσίας σχετικά με υπαλλήλους της εταιρείας. Η εταιρεία έδρασε αμέσως και μέσα σε τέσσερις ώρες την υπόθεση είχε αναλάβει το FBI. Παρόλο που κανένα από τα δεδομένα των χρηστών δεν επηρεάστηκε από την συγκεκριμένη περίπτωση, πολλές οικονομικές πληροφορίες των υπαλλήλων της εταιρείας βρέθηκαν σε κίνδυνο, λόγω αφέλειας του ενός.

Στην συνέχεια, στον πίνακα 2, παρουσιάζονται αναλυτικά οι επιπτώσεις που υπήρξαν από την κάθε παραβίαση δεδομένων, ως προς τον αριθμό των δεδομένων που βρέθηκαν σε κίνδυνο. Όπως αναφέρθηκε και στη μεθοδολογία, για την συγκεκριμένη έρευνα, επιλέχθηκαν οι περιπτώσεις που είχαν μεγάλο όγκο δεδομένων. Ξεκινώντας από την περίπτωση του Slack (Gorvis, 2019; Goldman, 2015; Greenberg, 2015), όπου κινδύνευσαν τουλάχιστον 500.000 δεδομένα χρηστών, η λίστα ανεβαίνει σε περιπτώσεις με μεγέθη μεγαλύτερα από ένα εκατομμύριο δεδομένα.

Πίνακας 2

Επιπτώσεις από την παραβίαση δεδομένων ανά εταιρεία

ΑΑ	ΠΕΡΙΠΤΩΣΗ	ΕΠΙΠΤΩΣΕΙΣ	ΑΑ	ΠΕΡΙΠΤΩΣΗ	ΕΠΙΠΤΩΣΕΙΣ
1	SLACK	500.000	36	US OFFICE OF PERSONNEL MANAGEMENT	21.500.000
2	GOOGLE PLUS	500.000	37	TYCKETFLY	27.000.000
3	DOMINO'S PIZZA (FRANCE)	600.000	38	HAUTELOOK	28.517.244
4	INTERNAL REVENUE SERVICE	720.000	39	TARINGA!	28.722.877
5	HEALTH SCIENCES AUTHORITY (SINGAPORE)	808.000	40	ASHLEY MADISON	32.000.000
6	ORBITZ	880.000	41	MYSPACE	36.000.000
7	CAREFIRST BLUECROSS BLUE SHIELD-MARYLAND	1.100.000	42	PANERA	37.000.000
8	NEIMAN MARCUS	1.100.000	43	WEEBLY	43.430.316
9	NIVAL NETWORKS	1.500.000	44	FACEBOOK	50.000.000
10	VERIZON COMMUNICATIONS	1.500.000	45	PHILIPPINES COMMISSION ON ELECTIONS	55.000.000
11	BELL CANADA	1.900.000	46	HOME DEPOT	56.000.000
12	T-MOBILE	2.000.000	47	UBER	57.000.000
13	EARL ENTERPRISES	2.000.000	48	UNITED STATES POSTAL SERVICE	60.000.000
14	21ST CENTURY ONCOLOGE	2.200.000	49	JP MORGAN CHASE	76.000.000
15	PATREON	2.300.000	50	ANTHEM INC	80.000.000
16	AOL	2.400.000	51	MYHERITAGE	92.283.889
17	DESJARDINS	2.900.000	52	QUORA	100.000.000
18	MICHAELS	3.000.000	53	JUSTIDIAL	100.000.000
19	MEDICAL INFORMATICS ENGINEERING	3.900.000	54	MOBILE TELESYSTEMS (MTS)	100.000.000
20	SCOTTRADE	4.500.000	55	CAPITAL ONE	106.000.000
21	UCLA MEDICAL CENTER, SANTA MONICA	4.500.000	56	CANVA	140.000.000
22	COMMUNITY HEALTH SYSTEMS	4.500.000	57	EBAY	145.000.000
23	SNAPCHAT	4.600.000	58	UNDER ARMOUR	150.000.000
24	VTECH	5.000.000	59	TRUECALLER	299.055.819
25	GMAIL	5.000.000	60	TWITTER	330.000.000
26	STOCKX	6.800.000	61	FRIEND FINDER NETWORKS	412.214.295
27	CATHAY PACIFIC AIRWAYS	9.400.000	62	MARRIOTT INTERNATIONAL	500.000.000
28	EXCELLUS BLUECROSS BLUESHIELD	10.000.000	63	YAHOO	500.000.000

29	PREMERA	11.000.000	64	FACEBOOK	540.000.000
30	QUEST DIAGNOSTICS	11.900.000	65	FIRST AMERICAN CORPORATION	885.000.000
31	CAREEM	14.000.000	66	SINGHEALTH	1.500.00
32	EXPERIAN-T-MOBILE US	15.000.000	67	EQUIFAX	143.000.000
33	TAOBAO	20.000.000	68	EYEWIRE	UNKNOWN
34	KOREA CREDIT BUREAU	20.000.000	69	REDDIT	UNKNOWN
35	TIMEHOP	21.000.000	70	TYPEFORM	UNKNOWN

Αυτός ο μεγάλος όγκος δεδομένων είναι που κάνει όλες αυτές τις περιπτώσεις τόσο αξιοσημείωτες, διότι πρόκειται για περιστατικά τα οποία δεν πέρασαν απαρατήρητα και είχαν μεγάλες επιπτώσεις στις εταιρείες που συνέβησαν.

Οικονομικό κόστος

Ετήσια έρευνα του Cambridge (Lalan, 2019), μελετά τις οικονομικές επιπτώσεις των παραβιάσεων δεδομένων σχετικά με τους οργανισμούς. Σύμφωνα με την έρευνα, το κόστος παραβίασης των δεδομένων έχει αυξηθεί κατά 12% τα τελευταία πέντε χρόνια και στις μέρες μας μια παραβίαση κοστίζει κατά μέσο όρο 3.92 εκατομμύρια δολάρια. Τα έξοδα αυτά είναι αντιπροσωπευτικά των πολυετών οικονομικών επιπτώσεων των παραβιάσεων και την περίπλοκης διαδικασίας επίλυσης επιθέσεων (Lalan, 2019).

Οι οικονομικές συνέπειες μιας παραβίασης των δεδομένων μπορεί να είναι ιδιαίτερα έντονες για τις μικρές και μεσαίες επιχειρήσεις. Στη μελέτη του Cambridge (Lalan, 2019), οι επιχειρήσεις με λιγότερους από 500 υπαλλήλους υπέστησαν απώλειες άνω των 2,5 εκατομμυρίων δολαρίων κατά μέσο όρο - ένα σημαντικό όμως ποσό για τις μικρές επιχειρήσεις, οι οποίες συνήθως κερδίζουν 50 εκατομμύρια δολάρια ή λιγότερα σε ετήσια έσοδα (Lalan, 2019). Ενώ κατά μέσο όρο το 67% των δαπανών παραβίασης των δεδομένων πραγματοποιήθηκαν εντός του πρώτου έτους μετά την παραβίαση, το 22% συσσωρεύτηκε κατά το δεύτερο έτος και ένα άλλο 11% συσσωρεύτηκε περισσότερο από δύο χρόνια μετά την παραβίαση (Lalan, 2019). Τα μακροπρόθεσμα κόστη ήταν υψηλότερα κατά το δεύτερο και το τρίτο έτος για οργανισμούς σε ιδιαίτερα ρυθμισμένο περιβάλλον, όπως η υγειονομική περίθαλψη, οι χρηματοπιστωτικές υπηρεσίες, η ενέργεια και τα φαρμακευτικά προϊόντα.

Τα αποτελέσματα της έρευνας του Cambridge, περιλαμβάνουν κάποιες κατηγορίες παραβιάσεων, οι οποίες είναι οι εξής: οι κακόβουλες παραβιάσεις είναι πιο συνηθισμένες και πιο ακριβές, καθώς έχουν κόστος κατά μέσο όρο 1 εκατομμύριο δολάρια περισσότερα από τις παραβιάσεις που προκλήθηκαν από τυχαία αίτια (Lalan, 2019). Ταυτόχρονα, όσο μεγαλύτερη είναι η παραβίαση, τόσο μεγαλύτερο είναι και το κόστος της, αν για παράδειγμα υπάρξει περιστατικό με περισσότερα από 1 εκατομμύριο αρχεία, το κόστος

μπορεί να φτάσει μέχρι και το ύψος των 42 εκατομμυρίων δολαρίων, ενώ σε περιπτώσεις όπου το σύνολο των αρχείων περνάει τα 50 εκατομμύρια, το κόστος αναμένεται γύρω στα 300 εκατομμύρια δολάρια (Lalan, 2019). Παρόλα αυτά, παρατηρήθηκε ότι όσοι οργανισμοί είχαν κάποια ομάδα αντιμετώπισης περιστατικών, αντιμετώπισαν κατά μέσο όρο 1,23 εκατομμύρια δολάρια χαμηλότερα από το κόστος παραβίασης των δεδομένων από οργανισμούς που δεν είχαν εφαρμόσει κανένα μέτρο. Επίσης, σημειώθηκε ότι οι παραβιάσεις της υγειονομικής περίθαλψης κοστίζουν περισσότερο, με ποσοστό 60% περισσότερο από οποιαδήποτε άλλη βιομηχανία (Lalan, 2019). Οι αθέλητες παραβιάσεις από το ανθρώπινο λάθος και οι δυσλειτουργίες του συστήματος εξακολουθούσαν να αποτελούν την αιτία για σχεδόν το ήμισυ (49%) των παραβιάσεων δεδομένων, κοστίζοντας στους οργανισμούς 3,50 και 3,24 εκατομμύρια δολάρια αντίστοιχα.

Ταυτόχρονα, οι οργανισμοί τείνουν να αποφεύγουν να ειδοποιούν τους χρήστες ή τους υπαλλήλους τους ότι τα προσωπικά τους δεδομένα έχουν παραβιαστεί, λόγω του ότι θα χρειαστεί να αντιμετωπίσουν μια σειρά εξόδων. Εκτός από κάθε άμεσο κόστος που συνδέεται με την αντιμετώπιση των τρωτών σημείων ασφαλείας που οδήγησαν στο συμβάν της ασφάλειας, οι εταιρείες συχνά υποχρεούνται να ξοδεύουν χρήματα επικοινωνώντας με τους χρήστες, προσφέροντας και πληρώνοντας για τις υπηρεσίες των οργανισμών αναφοράς πιστώσεων, βοηθώντας την επιβολή του νόμου, τις δαπάνες διαταραχής των επιχειρήσεων και τα δικαστικά έξοδα. Εκτός από το φόβο του κόστους από αγωγές, διαπιστώθηκε ότι όταν οι χρήστες ενημερώνονται για συμβάντα ασφαλείας, είναι πιθανό να αποφύγουν τις συναλλαγές στο μέλλον και να στραφούν σε άλλους οργανισμούς. Η συμπεριφορά αυτή επηρεάζεται ιδιαίτερα από τη σημασία των βλαβών που αντιμετωπίζουν τα άτομα καθώς και από τις υπάρχουσες εναλλακτικές λύσεις.

Με βάση την έρευνα της συγκεκριμένης διπλωματικής, εντοπίστηκαν αρκετές διαφορετικές πτυχές οικονομικού κόστους για το κάθε περιστατικό παραβίασης δεδομένων. Αρχικά να αναφερθεί ότι πολλοί από τους οργανισμούς των περιστατικών που εντοπίστηκαν στην έρευνα, χρειάστηκε, ακόμα και μετά από δύο με τρία χρόνια, μέσω δικαστικής απόφασης, να καταβάλλουν μεγάλα χρηματικά ποσά είτε για την αποζημίωση των χρηστών της εταιρείας είτε για την αντιμετώπιση άλλων προβλημάτων.

Αρκετές εταιρείες παρατήρησαν σημαντική μείωση των μετοχών του οργανισμού την ίδια ακριβώς μέρα που συνέβη η παραβίαση. Για παράδειγμα, οι μετοχές της Orbitz (Dujmovic, 2018; Olenick, 2018; Weise, 2018) μειώθηκαν κατά 2% την ημέρα του περιστατικού, της Taobao (Cox, 2016; Reuters, 2016; Duckhin, 2016) κατά 3.7%, της Under Armour (Aiello, 2018; Bradley, 2018; Lamkin, 2018) μειώθηκαν κατά 3.8%, ενώ την μεγαλύτερη πτώση μετοχών παρατήρησε η εταιρεία Marriot International (Volodzko and Word, 2016; Ogden, 2016), η οποία είχε απώλεια 5.6% των μετοχών της.

Σημαντικές, επίσης, περιπτώσεις αποτελούν η εταιρεία Michaels (Harris, 2014; Kitten, 2015; Krebs, 2014), στην οποία την περίοδο της παραβίασης επηρεάστηκαν 7% των συναλλαγών της, καθώς και στην εταιρεία StockX (StockX, 2019; Deng, 2019; Whittaker, 2019) επέβαλαν πρόστιμο το 4% των ετησίων εσόδων της. Εκτός από την επιρροή στις μετοχές των οργανισμών όμως, η παραβίαση δεδομένων, πολλές φορές προκάλεσε την άμεση καταβολή χρηματικού ποσού για την αντιμετώπιση του προβλήματος, κυρίως σε περιπτώσεις όπου υπήρξε επίθεση από χάκερ. Η Uber (Khosrowshohi, 2017; Lerson, 2017; Lee,

2017) χρειάστηκε να καταβάλει το ποσό των $100.000 λύτρα έτσι ώστε η βάση δεδομένων η οποία κλάπηκε να μην δημοσιεύονταν στο Διαδίκτυο. Στην περίπτωση της Verizon Communications (Balakrishnam, 2016), οι χάκερ πουλούσαν στο Διαδίκτυο τα αρχεία και οι τιμές που ζητούσαν ήταν $10.000- $100.000, ανάλογα το μέγεθος των αρχείων που επιθυμούσε κάποιος να αγοράσει. Κάτι παρόμοιο συνέβη και στην επιχείρηση Hautelook (Newcomb, 2019; O'Flaherty, 2019; Williams, 2019) , όπου ο χάκερ κοστολόγησε με $28.000.000 την βάση δεδομένων που υπέκλεψε για όποιον ενδιαφέρονταν να την αποκτήσει. Αλλά και στην περίπτωση της Truecaller (Goswami, 2019; Mares, 2019), ο χάκερ πουλούσε την βάση δεδομένων στην τιμή των 2.000€ για την Ινδία ενώ για την υπόλοιπη Ευρώπη, η βάση κόστιζε 25.000€.

Αξιοσημείωτη είναι η περίπτωση της εταιρείας Ashley Madison (Basu, 2015; Hern, 2015; Thomsen, 2015), στην οποία είχε γίνει αρκετά μεγάλο σκάνδαλο λόγω της παραβίασης των δεδομένων τους από χάκερ. Η εταιρεία, λοιπόν, πρόσφερε $500.000 σε όποιον μπορούσε να εντοπίσει τον χάκερ. Κάποιοι οργανισμοί χρειάστηκε να πληρώσουν αποζημίωση στους χρήστες των οποίων τα δεδομένα διακυβεύτηκαν. Η Anthem Inc (McNeal, 2015; Reuters, 2017; Riley, 2015) έδωσε συνολικά $115.000.000 στους χρήστες της, ενώ η Equifax (Leonhardt, 2019; Mathews, 2017) προσέφερε έως $20.000 σε όποιον χρήστη ήθελε να ζητήσει αποζημίωση για την απώλεια των προσωπικών πληροφοριών του.

Παρατηρείται, γενικά, ότι σε όλους τους οργανισμούς, υπήρξε κάποιο οικονομικό κόστος, είτε μεγάλο είτε μικρό, το οποίο χρειάστηκε να δοθεί προκειμένου να αντιμετωπιστεί η εκάστοτε παραβίαση δεδομένων. Όπως έδειξε και η έρευνα του Cambridge (Lalan, 2019), τα τελευταία χρόνια έχει αυξηθεί σημαντικά το ποσό που είναι αναγκαίο να καταβάλουν οι εταιρείες σε περίπτωση παραβίασης προσωπικών πληροφοριών, ενώ σημαντικό ρόλο στη μείωση του ζητήματος αποτελεί η ύπαρξη μιας ομάδας αντιμετώπισης περιστατικών από τον οργανισμό.

Μέσω της έρευνας, λοιπόν, εντοπίστηκε ελάχιστος αριθμός περιστατικών παραβίασης δεδομένων που να σχετίζονται με τον ανθρώπινο παράγοντα. Παρόλα αυτά, ο ρόλος του αποτελεί καθοριστικό παράγοντα τις περισσότερες φορές και οδηγεί σε σοβαρές παραβιάσεις με μεγάλες επιπτώσεις.

4.3 Ανθρώπινο λάθος

Έχει εντοπιστεί ότι οι κύριοι τύποι παραβιάσεων δεδομένων που αντιμετωπίζουν οι οργανισμοί αφορούν το ανθρώπινο λάθος και τα τεχνικά προβλήματα ευπάθειας στο κυβερνοχώρο. Αρκετοί ερευνητές τονίζουν ότι οι υπάλληλοι θεωρούνται ως ο βασικός ασθενής δεσμός και οι οργανισμοί συχνά αγνοούν το ανθρώπινο λάθος ως κύρια αιτία παραβιάσεων της ασφάλειας, δίνοντας την προσοχή τους σε τεχνικούς ελέγχους (Evans et al., 2018). Ο ανθρώπινος παράγοντας έχει καθοριστικό ρόλο τις περισσότερες φορές σε παραβιάσεις δεδομένων. Τα τελευταία πέντε χρόνια έχουν γίνει χιλιάδες περιστατικά, στα οποία κύριο ρόλο έπαιξε η ανθρώπινη απροσεξία και όχι τόσο κάποιο σφάλμα του υπολογιστή. Η απρόσεκτη αποστολή πληροφοριών, η αποκάλυψη πληροφοριών κατά λάθος, η απώλεια, κλοπή ή ανεπαρκή διάθεση εγγράφων

και υλικού, όλα αυτά οφείλονται στον ανθρώπινο παράγοντα. Μόνο το 2019, σημειώθηκε ότι περίπου το 60% των παραβιάσεων δεδομένων ήταν αποτέλεσμα ανθρώπινου λάθους (Lawyer Monthly, 2019). Από αυτά, σχεδόν τα μισά περιστατικά ήταν αποτέλεσμα λανθασμένης αποκάλυψης. Παρατηρήθηκε επίσης, ότι τα περισσότερα περιστατικά, σχετίζονται κυρίως με τον τομέα της υγείας και των κυβερνητικών υπηρεσιών.

Το ανθρώπινο λάθος είναι ένας σημαντικός παράγοντας στην κατάσταση του κινδύνου και της αξιοπιστίας. Ο Dhillon (2003) (Evans et al., 2018) ορίζει τον όρο ανθρώπινο λάθος ως αδυναμία εκτέλεσης συγκεκριμένης εργασίας ή αποστολής που θα μπορούσε να οδηγήσει σε διακοπή των προγραμματισμένων εργασιών. Ο ορισμός περιλαμβάνει επίσης την ανάληψη απαγορευμένης δράσης που θα μπορούσε επίσης να οδηγήσει στην ίδια αρνητική έκβαση. Ο όρος σφάλμα μπορεί να εφαρμοστεί μόνο σε σκόπιμες ενέργειες (Evans et al., 2018). Αυτό οφείλεται στους τύπους σφαλμάτων που εξαρτώνται κριτικά είτε από την αποτυχία των ενεργειών να προχωρήσουν όπως προβλέπεται είτε από την αποτυχία των σκοπούμενων ενεργειών να επιτύχουν το επιθυμητό αποτέλεσμα.

Η Ανάλυση Ανθρώπινης αξιοπιστίας (Human Reliability Analysis,HRA) περιλαμβάνει τη χρήση ποιοτικών και ποσοτικών μεθόδων για την αξιολόγηση της ανθρώπινης συμβολής σε κίνδυνο ή είναι ένας όρος που χρησιμοποιείται για την περιγραφή των επιδόσεων του ανθρώπου όσον αφορά την ολοκλήρωση ενός έργου χωρίς σφάλμα σε δεδομένες συνθήκες σε δεδομένο χρονικό διάστημα (Evans et al., 2018). Το HRA είναι μια μέθοδος τόσο πρόβλεψης όσο και αξιολόγησης, ως συμπλήρωμα στην εκτίμηση κινδύνου, των βλαβών της ανθρώπινης δράσης ή αδράνειας και όχι της αποτυχίας ενός φυσικού στοιχείου, που θα είχε αρνητική επίδραση στην αξιοπιστία του συστήματος ή διαθεσιμότητα. Ο τελικός στόχος του HRA είναι να βελτιώσει την αξιοπιστία μέσω του εντοπισμού των σφαλμάτων και των αδυναμιών σε ένα σύστημα μέσω της εξέτασης των συστημάτων εργασίας και επίσης εκείνων που εργάζονται στο σύστημα (Evans et al., 2018). Οι τρεις κύριοι λόγοι για τη διεξαγωγή ανάλυσης αξιοπιστίας του ανθρώπου είναι ο εντοπισμός σφαλμάτων, η ποσοτικοποίηση σφαλμάτων και η μείωση των σφαλμάτων. Υπάρχουν διάφορες μέθοδοι HRA που είναι διαθέσιμες για την αντιμετώπιση της ανθρώπινης αποτυχίας στο πλαίσιο προγνωστικών αξιολογήσεων κινδύνου.

Έχουν αναφερθεί προηγουμένως κάποιες παραβιάσεις δεδομένων οι οποίες οφείλονταν σε ανθρώπινο λάθος. Από τα 70 περιστατικά της έρευνας, τα 46 έχουν ως κύριο αίτιο την έλλειψη ασφάλειας, σε οποιοδήποτε επίπεδο και ο αριθμός αυτός αποδεικνύει από μόνος του ότι το πληροφοριακό σύστημα, δεν είναι πάντοτε υπεύθυνο για την παραβίαση των δεδομένων.

Ένα χαρακτηριστικό παράδειγμα παραβίασης με βασικό αίτιο την έλλειψη ή την κακή ασφάλεια, είναι η περίπτωση του Slack (Kovacs, 2019; Mihalcik, 2019; Truong, 2015). Το Slack αποτελεί ένα μέσο κοινωνικής δικτύωσης που χρησιμοποιείται κυρίως από τις επιχειρήσεις για την επικοινωνία των υπαλλήλων. Το 2015, επιτιθέμενοι κατάφεραν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στην βάση δεδομένων και στη συνέχεια εισήγαγαν κακόβουλο λογισμικό στο σύστημα, το οποίο υπέκλεβε τους κωδικούς πρόσβασης της βάσης. Αυτό έγινε λόγω του ότι οι κωδικοί πρόσβασης ήταν αποθηκευμένη σε

μορφή απλού κειμένου (plaintext). Η εταιρεία μετά τον εντοπισμό της επίθεσης, πρόσθεσε επιπλέον προστασία με την χρήση της αυθεντικοποίησης δύο παραγόντων και του password kill switch. Στο συγκεκριμένο παράδειγμα, η μη κωδικοποιημένη αποθήκευση των κωδικών πρόσβασης είναι αποτέλεσμα ανθρώπινου λάθους καθώς ο υπολογιστής δεν μπορεί να γνωρίζει τον κίνδυνο που μπορεί να διατρέχουν τα δεδομένα αυτά.

Εξίσου καλό παράδειγμα ανθρώπινου λάθους είναι και η περίπτωση της Google Plus (Brandom, 2018; O'Flaherty, 2018; Statt, 2018). Το λογισμικό σύστημα είχε αρκετά προβλήματα κενών ασφάλειας καθώς υπήρχε bug στο API το οποίο δημιούργησε διαρροή δεδομένων. Παρόλο που εντοπίστηκε το πρόβλημα και προσπάθησαν να το αντιμετωπίσουν, λίγους μήνες αργότερα κατά την διάρκεια μιας αναβάθμισης του συστήματος, υπήρξε κι άλλο ελάττωμα που δημιούργησε πρόβλημα. Η εταιρεία αποφάσισε να σταματήσει εντελώς την λειτουργία της υπηρεσίας Google Plus, καθώς έκρινε ότι ήταν ο πιο αποτελεσματικός τρόπος για να αντιμετωπιστεί το ζήτημα.

Συνολικά, λοιπόν, παρατηρείται η ύπαρξη πολλών διαφορετικών παραγόντων οι οποίοι προκαλούν παραβίαση των δεδομένων σε έναν οργανισμό, από τον χάκερ, την εισβολή κακόβουλου λογισμικού, μέχρι και την κλοπή υλικού της εταιρείας αλλά και την ύπαρξη επιτιθέμενου μέσα από το προσωπικό της εταιρείας. Επίσης, υπήρξαν και περιπτώσεις όπου η κακή ασφάλεια τόσο των πληροφοριακών συστημάτων ενός οργανισμού, όσο και απαραίτητων υλικών αγαθών, όπως για παράδειγμα ένα μηχάνημα πιστωτικών συναλλαγών, ήταν καθοριστικοί παράγοντες για την παραβίαση των δεδομένων.

Τα περισσότερα από αυτά τα παραδείγματα παραβιάσεων δεδομένων, αποδεικνύουν ότι υπάρχει μεγάλο θέμα έλλειψης ενημέρωσης στις εταιρείες και στους οργανισμούς ως προς τη σωστή διαχείριση και προστασία των συστημάτων. Παρόλο που χρησιμοποιούνται εργαλεία για την διαφύλαξη των δεδομένων, εμφανίζεται το φαινόμενο να είναι ανεπαρκή και να μην μπορούν να ανταπεξέλθουν στις προκλήσεις που προκύπτουν. Χρειάζεται καλύτερη ενημέρωση του προσωπικού των εταιρειών για να έχουν επίγνωση της ασφάλειας των δεδομένων, να χειρίζονται καλύτερα τόσο το λογισμικό όσο και το λειτουργικό σύστημα, έτσι ώστε να περιοριστούν οι περιπτώσεις που οφείλονται σε ανθρώπινο λάθος. Επίσης είναι απαραίτητη και η βελτίωση των εργαλείων που χρησιμοποιούνται για την προστασία των πληροφοριακών συστημάτων, καθώς οι επιτιθέμενοι αυξάνονται και εξελίσσονται καθημερινά και οι τεχνολογίες αλλάζουν με μεγάλες ταχύτητες.

5

Πρόληψη και αντιμετώπιση περιστατικών παραβίασης δεδομένων

Έχοντας κατηγοριοποιήσει και αναλύσει τα περιστατικά παραβίασης δεδομένων της έρευνας, παρατηρείται η ανάγκη για την βελτίωση της ασφάλειας αυτών των οργανισμών. Εκτός από τα περιστατικά που συνέβησαν μέσω Διαδικτύου στις ιστοσελίδες των εταιρειών, υπάρχουν παραβιάσεις στα πληροφοριακά συστήματα των οργανισμών, καθώς επίσης και σε υλικό εξοπλισμό. Δημιουργείται συνεπώς η ανάγκη για την εύρεση των κατάλληλων μέτρων ασφαλείας. Σε αυτό το κεφάλαιο, θα συζητηθεί το κύριο θέμα της επίγνωσης ασφάλειας των συστημάτων, μαζί με τρόπους διαχείρισης των κινδύνων. Παράλληλα, θα δοθούν ενδεικτικές πολιτικές ασφάλειας ανάλογα με την κατηγορία του περιστατικού και τον τομέα από τον οποίο προέρχεται, καθώς και τρόποι πρόληψης και αντιμετώπισης περιστατικών παραβίασης δεδομένων.

5.1 Επίγνωση ασφάλειας (Security Awareness)

Ένα βασικό πρόβλημα που παρατηρείται στους οργανισμούς είναι η έλλειψη ενημέρωσης των υπαλλήλων ως προς τα θέματα ασφάλειας των πληροφοριών. Η σωστή εκπαίδευση τους πάνω σε θέματα επίγνωσης ασφάλειας θα έχει ως αποτέλεσμα την καλύτερη προστασία των συστημάτων και την άμεση ανταπόκριση σε περίπτωση προβλήματος.

Δεν υπάρχει κάποιος ακριβής ορισμός της επίγνωσης ασφάλειας (security awareness). Πάρα πολλοί συγγραφείς έχουν προσπαθήσει να δώσουν έναν συγκεκριμένο ορισμό για αυτό το ζήτημα, παρόλα

αυτά δεν έχει καθιερωθεί μια συγκεκριμένη έννοια (Joeger, 2018). Οι Rhee et al. ορίζουν την επίγνωση ασφάλειας πληροφοριών ως «την εγρήγορση στην κατανόηση των διαφόρων απειλών της ασφάλειας πληροφοριών και στην αντίληψη του κάθε ατόμου σχετικά με αυτές τις απειλές».

Οι Ernst & Young (2004) (Tsohou et al., 2008) αναγνωρίζουν την έλλειψη της επίγνωσης ασφάλειας από τους χρήστες ως ένα εμπόδιο στην αποτελεσματική ασφάλεια των πληροφοριών. Οι ίδιοι ασχολήθηκαν και αργότερα με το θέμα, αναγνωρίζοντας την επίγνωση ασφάλειας ως ένα από τα μέτρα που χρήζουν σημασίας για την κάλυψη του κενού που υπάρχει ανάμεσα στους αυξανόμενους κινδύνους ασφάλειας πληροφοριακών συστημάτων και στα μέτρα που είναι απαραίτητο να ληφθούν για την αντιμετώπισή τους. Επιπλέον, οι Ernst & Young (2006) (Tsohou et al., 2008) θεωρούν την επίγνωση ως μια διαδικασία, που θα πρέπει να θεωρείται μια από τις πιο σημαντικές προτεραιότητες παγκοσμίως για την ασφάλεια των πληροφοριών, η οποία θα έχει επιταχυνόμενη επίδραση στην ικανότητα των οργανισμών να διαχειρίζονται τους κινδύνους τους.

Οι περισσότεροι ορισμοί υπονοούν ότι η επίγνωση ασφάλειας πληροφοριών είναι το κατώτερο επίπεδο της πυραμίδας της μάθησης ασφάλειας, έχει δηλαδή ως στόχο να προσελκύσει τους χρήστες πληροφοριακών συστημάτων στο να καταλάβουν τη σημαντικότητα της ασφάλειας της πληροφορίας και των υποχρεώσεων τους ως προς την ασφάλεια. Η εξάσκηση έχει ως στόχο την ανάπτυξη της γνώσης και την ανάπτυξη σχετικών ικανοτήτων, ενώ η εκπαίδευση στοχεύει στη δημιουργία εξειδίκευσης πάνω σε ζητήματα ασφάλειας (Tsohou et al., 2008).

Ο οδηγός από τον ENISA (2006) (Tsohou et al., 2008) διαφοροποιεί την επίγνωση (awareness) από την εξάσκηση (training) και την εκπαίδευση (education), προσφέροντας «μια προσέγγιση διαχείρισης αλλαγών», η οποία έρχεται σε αντίθεση με το στόχο της αύξησης της προσοχής του κοινού σε ζητήματα ασφάλειας. Αυτή η αλλαγή αναγνωρίζεται ως μια πολιτιστική αλλαγή και αναφέρεται στην αλλαγή:

α) της αντίληψης του χρήστη (user's perception),

β) της οργανωτικής κουλτούρας (organizational culture),

γ) της συμπεριφοράς του χρήστη (user's behavior),

δ) της οικειότητας του κοινού με τις πολιτικές ασφάλειας (audience's familiarity with security policies and procedures) και

ε) του ενδιαφέροντος του κοινού προς την ασφάλεια (audience's interest towards security).

Το Εθνικό Ινστιτούτο Πρωτοτύπων και Τεχνολογίας (NIST) το 2003 (Wilson and Hash, 2003), δημοσίευσε ένα κείμενο με τους κανονισμούς και τις τεχνικές για τη δημιουργία προγραμμάτων επίγνωσης ασφάλειας πληροφοριών και εξάσκησης. Σύμφωνα με το NIST, ένα πετυχημένο πρόγραμμα ασφάλειας πληροφοριών αποτελείται από: 1) την ανάπτυξη της πολιτικής ασφάλειας πληροφοριών, η οποία αντανακλάται στις ανάγκες της επιχείρησης και μετριάζεται από γνωστούς κινδύνους, 2) την πληροφόρηση των χρηστών για τις υποχρεώσεις τους στην ασφάλεια πληροφοριών, όπως καταγράφονται στην πολιτική

ασφάλειας του οργανισμού και 3) την θέσπιση διαδικασιών για την παρακολούθηση και την αναθεώρηση του προγράμματος (Wilson and Hash, 2003).

Η επίγνωση της ασφάλειας και η εξάσκηση θα πρέπει να είναι επικεντρωμένες στο σύνολο του πληθυσμού των χρηστών του οργανισμού. Η διαχείριση πρέπει να θέσει το παράδειγμα για τη κατάλληλη συμπεριφορά στην ασφάλεια των πληροφοριών σε έναν οργανισμό (Wilson and Hash, 2003). Ένα πρόγραμμα επίγνωσης οφείλει να ξεκινήσει με μια προσπάθεια που μπορεί να αναπτυχθεί και να υλοποιηθεί με διάφορους τρόπους και απευθύνεται σε όλα τα επίπεδα της οργάνωσης συμπεριλαμβανομένων των ανώτερων και εκτελεστικών διευθυντών. Η αποτελεσματικότητα αυτής της προσπάθειας συνήθως θα καθορίσει την αποτελεσματικότητα του προγράμματος επίγνωσης και εξάσκησης. Αυτό είναι κάτι που είναι απαραίτητο για ένα πετυχημένο πρόγραμμα ασφάλειας πληροφοριών (Wilson and Hash, 2003).

Ένα πρόγραμμα επίγνωσης και εξάσκησης σε μια επιχείρηση είναι βασικό, καθώς είναι το «μέσο» για τη διάδοση των πληροφοριών στους χρήστες, συμπεριλαμβανομένων και των διευθυντών, και απαιτείται για να μπορούν να ολοκληρώσουν με ασφάλεια τις αρμοδιότητές τους (Wilson and Hash, 2003). Στη περίπτωση του προγράμματος ασφάλειας πληροφοριών, το «μέσο» χρησιμοποιείται για να μεταφέρει τις απαιτήσεις της ασφάλειας σε όλη την επιχείρηση.

Ένα αποτελεσματικό πρόγραμμα επίγνωσης ασφάλειας πληροφοριών και εξάσκησης εξηγεί τους κύριους κανόνες συμπεριφοράς των χρηστών ενός συστήματος πληροφοριών τεχνολογίας. Το πρόγραμμα κοινοποιεί τις πολιτικές ασφάλειας πληροφοριών και τονίζει ότι είναι σημαντικό να ακολουθηθούν. Αυτό πρέπει να προηγείται και να θέτει τη βάση για τυχόν κυρώσεις που επιβάλλονται λόγω μη εκπαίδευσης (Wilson and Hash, 2003). Οι χρήστες πρώτα πρέπει να πληροφορούνται για τις προσδοκίες. Η λογοδοσία πρέπει να προέρχεται από ένα πλήρως ενημερωμένο, καλά εκπαιδευμένο και ευαισθητοποιημένο εργατικό δυναμικό.

Οι προσπάθειες της επίγνωσης ασφάλειας είναι σχεδιασμένες για να αλλάξουν τη συμπεριφορά ή να ενισχύσουν τις καλές πρακτικές ασφάλειας. Ο NIST (Wilson and Hash, 2003) ορίζει την επίγνωση (awareness) ως εξής: «Η επίγνωση δεν είναι εξάσκηση. Ο σκοπός της παρουσίασης της επίγνωσης είναι απλώς για να επικεντρώσει την προσοχή στην ασφάλεια. Η παρουσίαση της επίγνωσης έχει ως στόχο να επιτρέψει στα άτομα να αναγνωρίζουν τις ανησυχίες της ασφάλειας πληροφοριών και να αντιδρούν άμεσα. Στις δραστηριότητες επίγνωσης, οι μαθητές είναι οι δέκτες της πληροφορίας, ενώ ο μαθητής σε ένα εκπαιδευτικό περιβάλλον έχει πιο ενεργό ρόλο (Wilson and Hash, 2003),. Η επίγνωση βασίζεται στην επίτευξη ευρέων ακροατηρίων με ελκύστηκες τεχνικές. Η εξάσκηση είναι πιο επίσημη, έχοντας στόχο την απόκτηση γνώσης και δεξιοτήτων που θα διευκολύνουν την απόδοση της εργασίας.

Η εξάσκηση (training) ορίζεται από το NIST (Wilson and Hash, 2003) με τα εξής: « Το επίπεδο της εξάσκησης στο συνεχές της μάθησης στοχεύει στην παραγωγή σχετικών και απαραίτητων ικανοτήτων ασφάλειας από τους υπαλλήλους, οι οποίοι έχουν γνώσης σε θέματα διαφορετικά από την ασφάλεια πληροφοριών». Η βασική διαφορά της εξάσκησης με την επίγνωση είναι ότι η εξάσκηση στοχεύει στην

διδασκαλία ικανοτήτων που επιτρέπουν στο άτομο να διαχειριστεί συγκεκριμένες λειτουργίες, ενώ η επίγνωση στοχεύει στην προσοχή του ατόμου σε ένα θέμα ή ένα σύνολο θεμάτων. Οι ικανότητες που χρειάζονται κατά την εξάσκηση δημιουργούνται στη βάση της επίγνωσης, και συγκεκριμένα, στις βασικές γνώσης για την ασφάλεια. Ένα εκπαιδευτικό πρόγραμμα δεν πρέπει απαραίτητα να οδηγεί σε πτυχίο από πανεπιστήμιο τριτοβάθμιας εξάσκησης (Wilson and Hash, 2003). Παρόλα αυτά, ένα εκπαιδευτικό μάθημα μπορεί να περιέχει το ίδιο περιεχόμενο με ένα μάθημα από κολέγιο ή πανεπιστήμιο που συμπεριλαμβάνεται σε ένα συγκεκριμένο πρόγραμμα σπουδών.

Η εκπαίδευση (education) είναι: «Το επίπεδο που ενσωματώνει όλες τις δεξιότητες και τις ικανότητες ασφάλειας των διάφορων λειτουργικών ειδικοτήτων σε ένα κοινό σώμα της γνώσης, προσθέτει μια διεπιστημονική μελέτη των εννοιών, των ζητημάτων και των αρχών (τεχνολογικών και κοινωνικών) και προσπαθεί να παραγάγει ειδικούς και επαγγελματίες ικανούς για όραμα και προορατική ανταπόκριση» (Wilson and Hash, 2003). Για παράδειγμα, ένα εκπαιδευτικό πρόγραμμα σε κάποιο πανεπιστήμιο ή κολλέγιο αποτελεί ένα παράδειγμα εκπαίδευσης. Κάποια άτομα επιλέγουν ένα μάθημα για να αναπτύξουν τις δεξιότητές τους με ιδιαίτερη πειθαρχία. Αυτό είναι εξάσκηση σε αντίθεση με την εκπαίδευση. Πολλά πανεπιστήμια και κολλέγια προσφέρουν προγράμματα με πιστοποίηση, στα οποία ο φοιτητής μπορεί να παρακολουθήσει αρκετά μαθήματα, με μια σχετική πειθαρχία και να απονεμηθεί ένα πιστοποιητικό κατά την ολοκλήρωση των μαθημάτων. Συχνά, αυτά τα προγράμματα πιστοποίησης διεξάγονται ως μια κοινή προσπάθεια ανάμεσα στα σχολεία και στους πωλητές λογισμικού (Wilson and Hash, 2003). Οι υπεύθυνοι των εκπαιδευτικών προγραμμάτων είναι αρμόδιοι να κρίνουν τι είναι κατάλληλο ως περιεχόμενο εκπαίδευσης ανάλογα με τις ανάγκες του κοινού.

Το 2010 ο ENISA (ENISA, 2010) δημοσίευσε έναν οδηγό για τη σωστή ανάπτυξη της επίγνωσης της ασφάλειας. Δίνεται έμφαση στο σωστό χρόνο που θεωρείται απαραίτητη η δημιουργία προγραμμάτων για την ασφάλεια των πληροφοριών. Διαχωρίζει τις περιπτώσεις, ανάλογα με τους παράγοντες που μπορεί να επηρεάσουν τη χρησιμότητα της δημιουργίας προγράμματος, σε εξωτερικούς και εσωτερικούς. Οι εξωτερικοί παράγοντες είναι η ψήφιση νέων νόμων σχετικά με την ασφάλεια των πληροφοριών, μια νέα κυβέρνηση, τα νέα εθνικά, περιφερειακά ή τοπικά προγράμματα ασφάλειας βασικών πληροφοριών για τους πολίτες κ.α. (ENISA, 2010). Οι εσωτερικοί παράγοντες που μπορεί να οδηγήσουν στην ανάγκη δημιουργίας προγράμματος ασφάλειας πληροφοριών είναι οι νέοι κανονισμοί που σχετίζονται με τον οργανισμό, μια νέα πολιτική απορρήτου, η αναβάθμιση ή η αλλαγή της πολιτικής ασφάλειας των πληροφοριών, των διαδικασιών και των οδηγιών. Επίσης, η εφαρμογή νέων τεχνολογιών, η πρόσληψη νέου προσωπικού, η αλλαγή διαχείρισης, η αυτονομία και η βασική εκπαίδευση του προσωπικού σε θέματα ασφάλειας πληροφοριών, οι καινούργιοι κίνδυνοι κ.α. εντάσσονται στους εσωτερικούς παράγοντες.

Η στρατηγική λοιπόν, που προτείνει ο ENISA (ENISA, 2010) για τη διαχείριση προγραμμάτων επίγνωσης ασφάλειας πληροφοριών, περιέχει τρείς βασικές διαδικασίες, οι οποίες είναι: α) η οργάνωση, η αξιολόγηση και ο σχεδιασμός, β) η εκτέλεση και διαχείριση, και γ) η αξιολόγηση και προσαρμογή. Στον πίνακα 2 δίνεται μια περιγραφή για αυτές τις τρεις διαδικασίες.

Στην πρώτη διαδικασία τα προγράμματα επίγνωσης θα πρέπει να σχεδιαστούν έχοντας κατά νου το στόχο του οργανισμού. Είναι σημαντικό να υποστηρίζουν τις ανάγκες της επιχείρησης του οργανισμού και να σχετίζονται με την κουλτούρα και την αρχιτεκτονική του. Τα πιο πετυχημένα προγράμματα είναι αυτά στα οποία οι χρήστες τους αισθάνονται ότι σχετίζονται με το θέμα και τα προβλήματα που παρουσιάζονται.

Η δεύτερη διαδικασία περιλαμβάνει οποιαδήποτε δραστηριότητα είναι απαραίτητη για την εφαρμογή του προγράμματος επίγνωσης ασφάλειας πληροφοριών. Η πρωτοβουλία μπορεί να εκτελεστεί και να διαχειριστεί μόνο όταν έχει διεξαχθεί αξιολόγηση των αναγκών, έχει αναπτυχθεί μια στρατηγική, έχει ολοκληρωθεί η σχεδίαση ενός προγράμματος επίγνωσης για την εφαρμογή της στρατηγικής και έχει αναπτυχθεί το υλικό του προγράμματος (ENISA, 2010).

Στην τρίτη διαδικασία, η επίσημη αξιολόγηση και οι μηχανισμοί ανατροφοδότησης είναι κριτικά στοιχεία οποιουδήποτε προγράμματος. Η συνεχιζόμενη βελτίωση δεν μπορεί να εγγυηθεί χωρίς την γνώση του πώς λειτουργεί το υπάρχον πρόγραμμα. Επιπλέον, ο μηχανισμός ανατροφοδότησης πρέπει να σχεδιαστεί με τέτοιο τρόπο ώστε να είναι σε θέση να ανταπεξέρχεται στους αρχικούς στόχους του προγράμματος. Μόλις σταθεροποιηθούν οι βασικές απαιτήσεις, η στρατηγική ανατροφοδότησης μπορεί να σχεδιαστεί και να υλοποιηθεί (ENISA, 2010).

Τα προγράμματα επίγνωσης και εκπαίδευσης θα πρέπει να είναι σχεδιασμένα έχοντας υπόψη το σκοπό του οργανισμού για τον οποίο σχεδιάζονται. Είναι σημαντικό το πρόγραμμα να υποστηρίζει τις επιχειρησιακές ανάγκες του οργανισμού και να σχετίζεται με την κουλτούρα και την αρχιτεκτονική της τεχνολογίας πληροφοριών. Τα πιο πετυχημένα προγράμματα είναι αυτά στα οποία οι χρήστες θεωρούν ότι σχετίζονται με το αντικείμενο και τα θέματα που παρουσιάζονται (ENISA, 2010).

5.2 Μεθοδολογία διαχείρισης κινδύνων

Εκτός από την ενημέρωση και την επίγνωση πάνω σε θέματα ασφάλειας, είναι απαραίτητο να υπάρχει γνώση και ως προς το πώς να διαχειρίζεται ο οργανισμός τον οποιοδήποτε κίνδυνο προκύψει. Σε αυτό έρχεται να βοηθήσει η μεθοδολογία διαχείρισης κινδύνων, μέσω της οποίας, θα αντιμετωπιστεί με τον σωστό τρόπο ο κίνδυνος που μπορεί να εμφανιστεί στο σύστημα (Κάτσικας, 2014). Ο σκοπός της διαχείρισης κινδύνων μπορεί να είναι είτε η υποστήριξη του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, είτε η συμμόρφωση με απαιτήσεις, είτε η προετοιμασία ενός σχεδίου επιχειρησιακής συνέχειας είτε η περιγραφή προδιαγραφών ασφάλειας. Η μεθοδολογία διαχείρισης κινδύνων χωρίζεται σε έξι βήματα: Καθορισμός πλαισίου, Εκτίμηση κινδύνων, Διαχείριση κινδύνων, Αποδοχή κινδύνων, Παρουσίαση κινδύνων και διαβούλευση και Παρακολούθηση και επανεξέταση κινδύνων.

Στο πρώτο βήμα, στον καθορισμό του πλαισίου, ορίζεται στην ουσία όλος ο σκοπός της μεθόδου διαχείρισης κινδύνων που θα ακολουθηθεί (Κάτσικας, 2014). Καθορίζονται κάποια κριτήρια τα οποία θα χρησιμοποιηθούν στη συνέχεια, το μέγεθος της μεθόδου και το οργανωτικό πλαίσιο λειτουργίας της για

την δημιουργία των προδιαγραφών των παραμέτρων αυτών. Τα βασικά κριτήρια είναι κυρίως κριτήρια αξιολόγησης κινδύνων, κριτήρια επιπτώσεων και κριτήρια αποδοχής κινδύνου. Τα κριτήρια αξιολόγησης ασχολούνται με την αξία των πληροφοριών, την κρισιμότητα των αγαθών που διακυβεύονται στο περιστατικό, τις πιθανές νομικές υποχρεώσεις, την επιχειρησιακή σημασία των ιδιοτήτων της ασφάλειας πληροφοριών, τις προσδοκίες των μετόχων και τις ενδεχόμενες αρνητικές συνέπειες του περιστατικού. Τα κριτήρια επιπτώσεων ασχολούνται με το κόστος και το μέγεθος της ζημιάς που προκάλεσε το περιστατικό στον οργανισμό. Στην διαμόρφωση τους συνυπολογίζεται το πόσο ευάλωτο είναι το πληροφοριακό αγαθό που τέθηκε σε κίνδυνο, η ιδιότητα της παραβιασμένης ασφάλειας, οι λειτουργίες που επηρεάστηκαν, οι οικονομικές απώλειες, η ανατροπή σχεδίων, η απώλεια φήμης και η παραβίαση νομικών υποχρεώσεων (Κάτσικας, 2014). Αντίστοιχα, τα κριτήρια αποδοχής κινδύνου βασίζονται στα επιχειρησιακά κριτήρια, στις νομικές απαιτήσεις και σε διάφορους παράγοντες που σχετίζονται με τον οργανισμό.

Τα όρια και το πεδίο εφαρμογής της διαχείρισης κινδύνων είναι απαραίτητα για την σωστή εκτίμηση των κινδύνων. Στον καθορισμό τους είναι σημαντικό να λαμβάνονται υπόψη οι επιχειρησιακοί στόχοι, οι λειτουργίες και η δομή του οργανισμού, οι νομικές υποχρεώσεις, η πολιτική ασφάλειας πληροφοριών, το πώς αντιμετωπίζει ο οργανισμός την διαχείριση κινδύνων, τα πληροφοριακά αγαθά, οι εγκαταστάσεις του, οι περιορισμοί, το κοινωνικό περιβάλλον του οργανισμού και η ανταλλαγή πληροφοριών με αυτό (Κάτσικας, 2014). Μια οργανωσιακή δομή, η οποία θα αναλάβει την διαχείριση κινδύνων, θα πρέπει να μπορεί να ανταπεξέλθει στην δημιουργία και ανάπτυξη μιας διαχείρισης κινδύνων κατάλληλη για τον οργανισμό, να μπορεί να αναγνωρίσει τους μετόχους, να καθορίσει τους ρόλους και τις αρμοδιότητες των ατόμων που θα συνεισφέρουν στη διαχείριση, να ορίσεις την λήψη των αποφάσεων και τα αρχεία τα οποία θα τηρούνται.

Το δεύτερο βήμα είναι η εκτίμηση του κινδύνου, όπου χωρίζεται σε τρεις φάσεις: την αναγνώριση, τη ανάλυση και την αξιολόγηση κινδύνων (Κάτσικας, 2014). Σκοπός αυτού του βήματος είναι η αναγνώριση του κινδύνου και ο εντοπισμός του σύμφωνα με τα κριτήρια αξιολόγησης. Στην φάση της αναγνώρισης πρώτα γίνεται η εύρεση των αγαθών, μετά η αναγνώριση των απειλών και των υπαρχόντων μέτρων ασφάλειας, έπειτα ο εντοπισμός των ευπαθειών και τέλος η αναγνώριση των συνεπειών. Στην ανάλυση των κινδύνων αρχικά γίνεται εκτίμηση των συνεπειών και της πιθανότητας εμφάνισης περιστατικού και στη συνέχεια γίνεται ο υπολογισμός του βαθμού κινδύνου. Στην αξιολόγηση κινδύνων συγκρίνεται ο βαθμός κινδύνου με τα κριτήρια αξιολόγησης και τα κριτήρια αποδοχής που καθορίστηκαν νωρίτερα (Κάτσικας, 2014). Η τελική αυτή φάση έχει ως στόχο να κατευθύνει σε αποφάσεις που σχετίζονται με τις μελλοντικές ενέργειες.

Στην διαχείριση κινδύνων, ο τελικός στόχος είναι να βρεθούν τα κατάλληλα μέτρα ασφάλειας έτσι ώστε είτε να μειωθεί είτε να διατηρηθεί ο κίνδυνος και να διαμορφωθεί ένα σχέδιο διαχείρισης του (Κάτσικας, 2014). Σε αυτό το σημείο πρέπει να παρθούν κάποιες αποφάσεις οι οποίες μπορεί να επηρεαστούν από το κόστος του περιστατικού, την συχνότητα του, τον τρόπο αντιμετώπισης του οργανισμού, την υλοποίηση των μέτρων ασφαλείας, τους διαθέσιμους πόρους, τις παρούσες

προτεραιότητες και την πολιτική του οργανισμού. Υπάρχουν πολλές πιθανότητες να συμβεί κάποιο περιστατικό, καθώς υπάρχουν πολλές απειλές ως προς το πληροφοριακό σύστημα λόγω του περιβάλλοντος του, δεν μπορεί να προβλεφθεί η συμπεριφορά των υπαλλήλων και επίσης επηρεάζει και το γεγονός ότι τα συστήματα και τα υλικά που έχει στη διάθεση του ένας οργανισμός μπορεί να είναι πεπερασμένα (Κάτσικας, 2014). Γι' αυτό το λόγο, η διαχείριση εστιάζει κυρίως στην μείωση του βαθμού κινδύνου, μέσω της μείωσης της πιθανότητας μιας απειλής να εκμεταλλευτεί μια ευπάθεια. Αρκετές φορές όμως υπάρχουν και κάποιοι περιορισμοί που μπορεί να έχουν σχέση με οικονομικά θέματα, με το πώς λειτουργεί ο οργανισμός, με το περιβάλλον στο οποίο βρίσκεται και διάφορα άλλα. Σε αυτές τις περιπτώσεις βοηθάει η κατανομή του κινδύνου. Αυτό μπορεί να γίνει με την εξουσιοδότηση σε τρίτους για την διαχείριση του κινδύνου ή μέσω συμβολαίου ασφάλισης. Από τις βασικές ενέργειες που γίνονται, η αποφυγή κινδύνου, χρησιμοποιείται για να τροποποιηθεί η λειτουργία του οργανισμού με τέτοιο τρόπο ώστε να μην υπάρξει κάποιος κίνδυνος και συνδέεται με το γεγονός ότι ο οργανισμός αναγνωρίζει την πιθανότητα ύπαρξης κινδύνου (Κάτσικας, 2014). Στο τέλος της διαχείρισης κινδύνου, υπάρχουν πάντα και οι απομείναντες κίνδυνοι οι οποίοι θα πρέπει να εκτιμηθούν ώστε να προστατευτεί ο οργανισμός.

Στην συνέχεια και αφού ολοκληρωθεί η διαδικασία της διαχείρισης κινδύνων, γίνεται παρουσίαση και διαβούλευση του περιστατικού (Κάτσικας, 2014). Κύριος λόγος είναι η ενημέρωση των μετόχων του οργανισμού για το περιστατικό και η αναγνώριση του κινδύνου. Θα πρέπει να υπάρξει μια οργανωμένη παρουσίαση του περιστατικού, με ανάλυση του κινδύνου για την ευκολότερη κατανόηση του από τους μετόχους.

Το τελευταίο βήμα είναι η παρακολούθηση και η επανεξέταση της διαχείρισης κινδύνων. Τα μέτρα ασφαλείας τα οποία πάρθηκαν, θα πρέπει να ελέγχονται τακτικά ώστε να εξασφαλίζεται η σωστή λειτουργία τους, καθώς επίσης και να διασφαλίζεται το ενδεχόμενο ότι αν υπήρξαν κάποιες αλλαγές στο περιβάλλον, δεν επηρεάστηκε η λειτουργία τους (Κάτσικας, 2014). Είναι αναγκαία η παρακολούθηση των μέτρων ασφαλείας λόγω του ότι υπάρχουν πολλοί παράγοντες που μπορούν να αλλάξουν τα μέχρι ως τότε δεδομένα, όπως μια νέα επιχειρησιακή λειτουργία ή η εμφάνιση νέων απειλών. Ο τακτικός έλεγχος θα έχει τα αναμενόμενα θετικά αποτελέσματα που επιθυμεί και το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών.

Στη σημερινή εποχή, υπάρχουν αμέτρητες διαθέσιμες μέθοδοι διαχείρισης κινδύνων. Ενδεικτικά, θα αναφερθούν στη συνέχεια οι πιο γνωστές από αυτές. Η διαφορά τους είναι ως προς το επίπεδο ανάλυσης όπου χρησιμοποιούν κατά την εκτέλεση τους, ενώ αρκετές από αυτές τις μεθόδους, δεν είναι ελεύθερα διαθέσιμες στην αγορά.

Η μέθοδος CRAMM (CCTA Risk Analysis and Management Methodology) αναπτύχθηκε το 1985 από την Κεντρική Υπηρεσία Υπολογιστών και Τηλεπικοινωνιών (CCTA) της Βρετανίας (CRAMM, 2012). Χρησιμοποιείται κυρίως από οργανισμούς μεγάλου μεγέθους και η προσέγγιση της είναι βαθμιαία και συγκρατημένη ως προς την ασφάλεια. Αποτελείται από τρία στάδια, τα οποία είναι η αναγνώριση και εκτίμηση της αξίας των αγαθών, η εκτίμηση των απειλών και των ευπαθειών και η επιλογή των

κατάλληλων μέτρων ασφάλειας. Περιέχει επίσης μια σειρά βοηθητικών λειτουργιών, ενώ είναι συμβατή με τα πρότυπα ISO/IEC 17799, ISO/IEC 27001 και ISO/IEC 27005 (CRAMM, 2012).

Η πιο γνωστή μέθοδος είναι η OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) (OCTAVE, 2012). Αναπτύχθηκε το 1999 από το Ινστιτούτο Μηχανικής Λογισμικού του αμερικανικού Πανεπιστημίου Carnegie- Mellon και βασίζεται στην εκτίμηση και τον σχεδιασμό διαχείρισης κινδύνων. Διαφέρει από τις υπόλοιπες μεθόδους, καθώς στοχεύει στον οργανωσιακό κίνδυνο και τις πρακτικές ασφάλειας. Επιπλέον, υπάρχουν και κάποιες παραλλαγές της συγκεκριμένης μεθόδου (OCTAVE, 2012). Η OCTAVE-S βασίζεται κυρίως στα μέσα και στους περιορισμούς που υπάρχουν στους οργανισμούς. Η OCTAVE Allegro χρησιμοποιείται από οργανισμούς οι οποίοι εστιάζουν στα πληροφοριακά αγαθά. Υπάρχει επίσης και ένα λογισμικό εργαλείο, το Octave Automated Tool όπου υποστηρίζει την χρήση της μεθόδου OCTAVE.

Η μέθοδος MAGERIT δημιουργήθηκε το 1997 από το ισπανικό Υπουργείο Δημόσιας Διοίκησης και η τρέχουσα έκδοση της ισχύει από το 2005 και μοιράζεται σε τρία βιβλία (Κάτσικας, 2014). Το πρώτο βιβλίο ασχολείται με την Μεθοδολογία και περιλαμβάνει τα βασικά βήματα που είναι απαραίτητα για την ανάλυση και διαχείριση κινδύνου, την περιγραφή της διαδικασίας και την εφαρμογή της σε πληροφοριακά συστήματα. Το δεύτερο βιβλίο, ο Κατάλογος στοιχείων, δίνει κριτήρια και πληροφορίες για την μοντελοποίηση των πληροφοριακών συστημάτων και κινδύνων. Το τρίτο βιβλίο με τις Πρακτικές τεχνικές, περιγράφει τις απαραίτητες ενέργειες για την ανάλυση και διαχείριση κινδύνων (Κάτσικας, 2014). Η μέθοδος αυτή χρησιμοποιείται σαν οδηγός για την διαχείριση.

Το Πρότυπο Καλής Πρακτικής (Standard of Good Practice) δημιουργήθηκε από το Information Security Forum (ISF) και περιλαμβάνει μια συλλογή στόχων ασφάλειας πληροφοριών μαζί με δηλώσεις καλής πρακτικής. Χωρίζεται σε πέντε τμήματα τα οποία έχουν και διαφορετικό ρόλο. Το πρώτο είναι η διαχείριση της ασφάλειας, το δεύτερο οι κρίσιμες επιχειρησιακές εφαρμογές, το τρίτο οι υπολογιστικές εγκαταστάσεις, το τέταρτο τα δίκτυα και το πέμπτο η ανάπτυξη συστημάτων.

Η μέθοδος EBIOS (Expression des Besoins et Identification des Objectifis de Securite) αναπτύχθηκε το 1995 και υποστηρίζεται από την Κεντρική Διεύθυνση Ασφάλειας Πληροφοριακών Συστημάτων (DCSSI) (EBIOS, 2010). Περιέχει όλες τις απαραίτητες πληροφορίες για τα πληροφοριακά συστήματα. Δίνει τη δυνατότητα σε όλους τους υπαλλήλους του οργανισμού να ενημερωθούν για θέματα ασφάλειας και να αλληλεπιδράσουν μεταξύ τους ώστε να αποκτήσουν γνώση για ολόκληρο τον κύκλο ζωής του συστήματος. Αποτελείται από πέντε φάσεις. Στην πρώτη γίνεται ανάλυση του περιβάλλοντος, στην δεύτερη και στην τρίτη αναλύονται οι ανάγκες ασφάλειας και οι απειλές. Στην τέταρτη και πέμπτη φάση γίνεται μια αντικειμενική διάγνωση των κινδύνων και ταυτόχρονα ορίζονται οι κατάλληλοι στόχοι ασφάλειας (EBIOS, 2010). Η EBIOS συμβαδίζει με τα πρότυπα ISO/IEC 27001, ISO/IEC 13335, ISO/IEC 15408, ISO/IEC 17799 και ISO/IEC 21827.

Η μέθοδος IT- Grundschutz είναι μια γερμανική μεθοδολογία για την θέσπιση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών και σημαίνει βασική προστασία πληροφορικής υποδομής (IT-

Grundschutz). Περιγράφει ένα ΣΔΑΠ το οποίο περιέχει μια δομή διακυβέρνησης και ένα σύνολο μέτρων ασφάλειας και αποτελείται από διάφορα μέρη. Επίσης, περιέχει το πρότυπο BSI Standard 100-3 για την περιγραφή της μεθόδου ανάλυσης κινδύνων, την οποία την χρησιμοποιεί για τον εντοπισμό επιπλέον κινδύνων και απαιτήσεων ασφάλειας. Είναι συμβατή και με τα πρότυπα ISO/IEC 17799 και ISO/IEC 27001 (Κάτσικας, 2014). Η συγκεκριμένη μέθοδος ακολουθεί τα εξής βήματα: αρχικά γίνεται εκκίνηση της διεργασίας, καθορίζονται οι στόχοι ασφάλειας και επιχειρησιακού πλαισίου, θεσπίζεται η οργανωτική δομή για την ασφάλεια πληροφοριών, εξασφαλίζονται οι απαραίτητοι πόροι, στη συνέχεια καθορίζεται η έννοια της ασφάλειας, αναλύεται η δομή της πληροφορικής υποδομής, εκτιμούνται οι απαιτήσεις προστασίας, έπειτα γίνεται η μοντελοποίηση και ο έλεγχος ασφάλειας της πληροφοριακής υποδομής, ακολουθεί η συμπληρωματική ανάλυση ασφάλειας, ο σχεδιασμός και η εκτέλεση υλοποίησης, η συντήρηση, παρακολούθηση και βελτίωση της διεργασίας και τέλος γίνεται πιστοποίηση με βάση το IT-Grundschutz (Κάτσικας, 2014).

Μαζί με τις μεθόδους διαχείρισης κινδύνων που υπάρχουν σε διεθνές επίπεδο, έχουν δημιουργηθεί και κάποια πρότυπα, τα οποία έχουν άμεση σχέση με την διαχείριση κινδύνων (Κάτσικας, 2014). Από την σειρά ISO27k, το πρότυπο ISO/IEC 27005 περιλαμβάνει κάποιες οδηγίες για την διαχείριση κινδύνων σε πληροφοριακά συστήματα. Έχει δημιουργηθεί για να συμβάλει στην υλοποίηση του σχεδίου ασφάλειας πληροφοριών και μπορεί να εφαρμοστεί σε όλους τους οργανισμούς (Κάτσικας, 2014). Το συγκεκριμένο πρότυπο αντικατέστησε τα πρότυπα ασφάλειας ISO/IEC TR 13335-3:1998 και ISO/IEC TR 13335-4:2000 και περιγράφει την μεθοδολογία διαχείρισης κινδύνων χωρίς να επικεντρώνεται σε κάποια συγκεκριμένη μέθοδο.

Πριν από το ISO/IEC 27005, εφαρμόζονταν το πρότυπο BS 7799-3:2006. Αυτό το πρότυπο δίνει οδηγίες για τις απαιτήσεις του προτύπου ISO/IEC 27001:2005 (Κάτσικας, 2014). Περιλαμβάνει την εκτίμηση και αξιολόγηση κινδύνων, την υλοποίηση μέτρων ασφάλειας για την αντιμετώπιση των κινδύνων, την παρακολούθηση και επανεξέταση των κινδύνων και τη συντήρηση και βελτίωση του συστήματος διαχείρισης κινδύνων. Κύριος στόχος του είναι η όσο το δυνατόν καλύτερη ασφάλεια των πληροφοριών με τη χρήση της διαχείρισης κινδύνων (Κάτσικας, 2014).

Παράλληλα, υπάρχει το πρότυπο ISO/IEC 31000:2009, το οποίο περιλαμβάνει αρχές και γενικές οδηγίες για την διαχείριση κινδύνων. Μπορεί επίσης να χρησιμοποιηθεί σε οποιονδήποτε οργανισμό και να εφαρμοστεί σε πολλούς και διαφορετικούς τύπους κινδύνων (Κάτσικας, 2014). Στόχος του προτύπου αυτού είναι η χρήση του για διεργασίες διαχείρισης κινδύνων σε υπάρχοντα αλλά και μελλοντικά πρότυπα, χωρίς να αντικαθιστά κάποιο άλλο υπάρχων πρότυπο.

Το πρότυπο IEC 31010:2009 χρησιμοποιείται συνδυαστικά με το ISO 31000 και περιέχει οδηγίες για την εκτίμηση κινδύνων (Κάτσικας, 2014). Η εκτίμηση κινδύνων σε αυτό το πρότυπο αντιμετωπίζεται ως αναπόσπαστο τμήμα της διαχείρισης κινδύνων, βοηθώντας έτσι τον οργανισμό να κατανοήσει τους κινδύνους που μπορεί να επηρεάσουν την λειτουργία του. Μαζί με τα πρότυπα του ISO υπάρχει και ο

οδηγός ISO Guide 73:2009 στον οποίο καταγράφονται οι ορισμοί που σχετίζονται με τη διαχείριση κινδύνων για την καλύτερη κατανόηση της.

Ταυτόχρονα, ο NIST έχει δημιουργήσει δύο αμερικανικά πρότυπα, το NIST SP 800-30 και το NIST SP 800-39 (Κάτσικας, 2014). Το πρώτο, αναπτύχθηκε το 2002 και οι οδηγίες του χρησιμοποιούνται κυρίως από ομοσπονδιακούς οργανισμούς για την επεξεργασία ευαίσθητων πληροφοριών και σχετίζονται με τις απαιτήσεις του OMB Circular A-130. Το δεύτερο πρότυπο του NIST, περιέχει και αυτό οδηγίες για την διαχείριση κινδύνων, μαζί με μια προσέγγιση για την αντιμετώπιση κινδύνων οι οποίοι προκύπτουν από την ενσωμάτωση των πληροφοριακών συστημάτων στις επιχειρησιακές διεργασίες του οργανισμού.

Παρατηρείται, ότι υπάρχουν πολλές μέθοδοι για την διαχείριση κινδύνων, μερικές παρόμοιες μεταξύ τους ενώ άλλες διαφορετικές, έχουν όμως έναν κοινό στόχο, την προστασία των πληροφοριακών συστημάτων. Η δημιουργία όλων αυτών των προτύπων βοηθάει στην καλύτερη αντιμετώπιση των περιστατικών παραβίασης δεδομένων και συγκεκριμένα στην διαχείριση των κινδύνων.

5.3 Πολιτικές ασφάλειας

Έχοντας αναλύσει προηγουμένως την ανάγκη για επίγνωση ασφάλειας και τις υπάρχουσες μεθόδους διαχείρισης κινδύνων που χρησιμοποιούνται στις μέρες μας, είναι σημαντικό να γίνει αναφορά και στις πολιτικές ασφάλειας των εταιρειών (Karat et al., 2005). Μια πολιτική (policy) είναι μια δήλωση ή ένα νομικό έγγραφο που αποκαλύπτει κάποιους ή όλους τους τρόπους που ένας οργανισμός συλλέγει, χρησιμοποιεί, αποκαλύπτει και διαχειρίζεται δεδομένα πελατών (Karyda et al., 2005). Οι πολιτικές ασφάλειας είναι πολύ σημαντικές για έναν οργανισμό καθώς διευκρινίζουν τους στόχους του και τον προστατεύουν από οποιοδήποτε νομικό ζήτημα. Μια πολιτική ασφάλειας συνήθως περιέχει τα σχέδια του οργανισμού σχετικά με την ασφάλεια των πληροφοριών, τα καθήκοντα των υπαλλήλων, τονίζει την σημασία της έτσι ώστε οι υπάλληλοι να συμμορφώνονται σε αυτή, ο οργανισμός δεσμεύεται σχετικά με το ποιους πόρους θα διαθέσει για την δημιουργία ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, μαζί με τα άτομα τα οποία θα συμβάλλουν σε αυτό.

Κατά την δημιουργία μιας πολιτικής ασφάλειας, υπάρχουν κάποια χαρακτηριστικά τα οποία είναι απαραίτητα για την υλοποίηση της. Για να θεωρείται μια πολιτική ασφάλειας καλή, θα πρέπει να είναι αρχικά εύκολα κατανοητή, έτσι ώστε ακόμα και ένας απλός χρήστης χωρίς ιδιαίτερες γνώσεις πάνω σε θέματα πληροφορικής, να μπορεί να καταλάβει το περιεχόμενο της (Karyda et al., 2005). Δεύτερον, θα πρέπει να είναι εφαρμόσιμη, δηλαδή το σχέδιο που περιγράφει να βασίζεται στις ανάγκες του οργανισμού, καθώς πολλές φορές οι περισσότεροι οργανισμοί χρησιμοποιούν κάποιο από τα έτοιμα πρότυπα που υπάρχουν, χωρίς όμως αυτό να αντιπροσωπεύει τις δικές τους ανάγκες. Επιπλέον, μια καλή πολιτική ασφάλειας πρέπει να είναι και εφικτή από τον οργανισμό, να μην ξεφεύγει από τους στόχους του και τις δυνατότητες του (Karat et al., 2005). Επίσης χρειάζεται να είναι εκτελεστή, οι στόχοι και οι οδηγίες που περιέχει να μην διαφέρουν εντελώς από τις ικανότητες του οργανισμού. Ταυτόχρονα, θα πρέπει να

εφαρμόζεται σταδιακά, καθώς είναι δύσκολο από την αρχή να εκτελούνται πλήρως. Χρειάζεται κάποιος χρόνος για να μελετηθεί η καταλληλότητα της σε σχέση με τις απαιτήσεις του οργανισμού. Τέλος, είναι χρήσιμο να έχει προληπτικό χαρακτήρα και να μην είναι απόλυτη ως προς την διατύπωση της. Ο τρόπος με τον οποίο δίνονται οι οδηγίες έχει σημαντικό ρόλο στο πως θα το εκλάβει ο αναγνώστης.

Πριν γίνει αναφορά σε κάποιες από τις πολιτικές ασφάλειας που χρησιμοποιούν οι εταιρείες στα περιστατικά παραβίασης δεδομένων της έρευνας, θα αναλυθεί ο τρόπος δημιουργίας μιας πολιτικής ασφάλειας (Karat et al., 2005). Ο τρόπος δημιουργίας περιέχει έντεκα βήματα τα οποία χωρίζονται σε τέσσερις φάσεις. Υπάρχει η φάση της Ανάπτυξης, η φάση της Υλοποίησης, η φάση της Συντήρησης και η φάση της απόσυρσης της πολιτικής.

Στην φάση της Ανάπτυξης, περιλαμβάνονται τρία βήματα, η δημιουργία, ο έλεγχος και η έγκριση (Karyda et al., 2005). Κατά την δημιουργία, τονίζεται η ανάγκη για ύπαρξη πολιτικής ασφάλειας, ορίζονται οι στόχοι και οι ρόλοι της και ερευνούνται οι απαιτήσεις της. Στη συνέχεια η πολιτική περνάει από έλεγχο για να αξιολογηθεί, να γίνουν οι απαραίτητες αλλαγές και προσαρμογές. Έπειτα, γίνεται η έγκριση της πολιτικής από κάποιον υπεύθυνο του οργανισμού.

Μόλις γίνει η έγκριση της πολιτικής ασφάλειας, ξεκινάει η φάση της Υλοποίησης, η οποία περιέχει και αυτή τρία βήματα, την γνωστοποίηση, την αρχική εφαρμογή και τις εξαιρέσεις. Στο πρώτο βήμα, γίνεται γνωστοποίηση της πολιτικής αρχικά στους υπαλλήλους του οργανισμού και σε αυτούς που επηρεάζονται άμεσα από αυτή (Karyda et al., 2005). Ακολουθεί η αρχική εφαρμογή της η οποία γίνεται για την συμμόρφωση του οργανισμού σε αυτή. Στις εξαιρέσεις πολλές φορές κάποιο από το περιεχόμενο της πολιτικής δεν πραγματοποιείται αμέσως, λόγω έλλειψης κατάλληλου προσωπικού ή χρονικών περιορισμών.

Στη συνέχεια και αφού ξεκινήσει η χρήση της πολιτικής ασφάλειας, ακολουθεί η φάση της Συντήρησης, στην οποία συμπεριλαμβάνονται τέσσερα βήματα, η επίγνωση, η παρακολούθηση των αποτελεσμάτων, η επιβολή της πολιτικής και η παρακολούθηση των αλλαγών (Karat et al., 2005). Στην αρχή είναι απαραίτητο οι υπάλληλοι να έχουν επίγνωση της πολιτικής για να συμμορφωθούν σε αυτή. Έπειτα, παρακολουθούνται τα αποτελέσματα των προσπαθειών στη συμμόρφωση με την πολιτική. Στο τρίτο βήμα, σε περίπτωση όπου παραβιάζεται ή παραλείπεται κάτι από την πολιτική, γίνεται επιβολή της από τους ανώτερους του οργανισμού για να αποφύγουν μελλοντικά προβλήματα. Τέλος, αν γίνουν αλλαγές στο περιεχόμενο της πολιτικής, είναι χρήσιμη η παρακολούθηση τους για την περίπτωση ανάγκης τροποποίησης κάποιων στοιχείων της πολιτικής.

Μετά από όλες αυτές τις διαδικασίες και όταν σταματήσει να είναι χρήσιμη η πολιτική, ξεκινάει η φάση της απόσυρσης στην οποία γίνεται διαγραφή της πολιτικής από τις ήδη υπάρχουσες, αρχειοθέτηση της σε περίπτωση που χρειαστεί κάποια στιγμή στο μέλλον να ξαναχρησιμοποιηθεί και τεκμηρίωση της απόφασης απόσυρσης της.

Έχοντας εξηγήσει λοιπόν, συνοπτικά, τη διαδικασία με την οποία δημιουργείται μια πολιτική ασφάλειας, είναι απαραίτητο να γίνει αναφορά στα περιστατικά παραβίασης δεδομένων της έρευνας.

Επιλέχθηκε ένα περιστατικό από κάθε κατηγορία για την έρευνα πάνω στις πολιτικές ασφάλειας των εταιριών αυτών. Στον παρακάτω πίνακα, φαίνονται ποια περιστατικά επιλέχθηκαν για την ανάλυση της πολιτικής ασφάλειας τους. Το βασικό κριτήριο επιλογής τους ήταν το μέγεθος των δεδομένων που διακυβεύτηκαν.

Πίνακας 3, Περιστατικά από τα οποία επιλέχθηκαν οι πολιτικές ασφάλειας

ΠΕΡΙΣΤΑΤΙΚΟ	ΚΑΤΗΓΟΡΙΑ	ΧΡΟΝΟΛΟΓΙΑ
Eyewire	Web	2016
Friend Finder Networks	Social Networks	2016
MyHeritage	Healthcare	2018
Experian T-Mobile	Telecommunication	2018
First American Corporation	Restaurant	2019
US Postal Service	Government	2018
Marriot International	Hotel	2018
Tycketfly	Transport	2018
Equifax	Financial	2017

Κατά την έρευνα των πολιτικών ασφάλειας των παραπάνω περιστατικών, εντοπίστηκε ότι λόγω της αλλαγής της νομοθεσίας, οι εταιρίες μετέτρεψαν τις πολιτικές τους έτσι ώστε να συμμορφώνονται με βάση τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR). Αυτό αποτέλεσε πρόβλημα στην έρευνα, καθώς δεν είναι δυνατό να εντοπιστούν οι πολιτικές που ίσχυαν την περίοδο όπου συνέβησαν τα περιστατικά παραβίασης, αν και τα περισσότερα περιστατικά συνέβησαν το 2018.

Παρόλο που έγινε επιλογή περιστατικών από διαφορετικούς τομείς οργανισμών, παρατηρείται ότι σχεδόν όλες οι εταιρίες ακολουθούν παρόμοια τακτική ως προς το περιεχόμενο των πολιτικών τους. Αυτό μπορεί να δικαιολογηθεί, καθώς οι πολιτικές ασφάλειας που εντοπίστηκαν, απευθύνονται στην προστασία των δεδομένων στον ιστότοπο του οργανισμού και όχι στο φυσικό περιβάλλον του, οπότε οι απαιτήσεις είναι συγκεκριμένες.

Το περιεχόμενο των πολιτικών αυτών αφορά κυρίως την συλλογή των προσωπικών δεδομένων των χρηστών και την χρήση τους από τον οργανισμό. Παραδείγματος χάριν, η πολιτική της ιστοσελίδας της εταιρίας MyHeritage, η οποία είναι μια εταιρία που σχετίζεται με την ανακάλυψη της οικογενειακής ιστορίας του ατόμου, είναι πρόσφατα ανανεωμένη και στο περιεχόμενο της αναφέρει αρχικά τι ορίζει η πολιτική ασφάλειας της εταιρίας, τι υπάρχει σχετικά με την υπηρεσία, πώς κάποιες οικογενειακές ιστοσελίδες της εταιρίας σχετίζονται με την συγκεκριμένη και στη συνέχεια επεξηγεί κάποιες από τις ορολογίες που χρησιμοποιεί η ιστοσελίδα σχετικά με θέματα του DNA (MyHeritage). Έπειτα, γίνεται διευκρίνιση ως προς το ποιες από τις πληροφορίες των χρηστών συλλέγονται καθώς και το πώς χρησιμοποιούνται αυτές οι πληροφορίες από την εταιρία. Περιέχει επίσης μια ενότητα στην οποία εξηγείται η χρήση των δεδομένων της εταιρίας από τρίτες ιστοσελίδες και κατά πόσο ο χρήστης έχει την

δυνατότητα να αρνηθεί στην παραχώρηση των δεδομένων του. Παράλληλα, δίνονται κάποιες πρόσθετες οδηγίες για το πώς μπορεί ο χρήστης να κάνει τροποποιήσεις στα δεδομένα του και εξηγείται το ποιοι έχουν πρόσβαση σε αυτά τα δεδομένα, κάποιες πληροφορίες σχετικά με το DNA των χρηστών και πως αξιοποιείται από την εταιρία και το πώς η εταιρία θα διαχειριστεί τις πληροφορίες του (MyHeritage). Επίσης, γίνεται αναφορά στα νομικά δικαιώματα που έχει ο χρήστης και στους νόμους που ισχύουν για τα δεδομένα. Αυτό που αξίζει να σημειωθεί, είναι ότι υπάρχει μια ενότητα στην πολιτική ασφάλειας που διευκρινίζει τις απαιτήσεις ασφάλειας σε σχέση με πληροφορίες παιδιών.

Η πολιτική ασφάλειας της T-Mobile έχει ανανεωθεί επίσης πρόσφατα, Δεκέμβριο 2019, έχοντας αρκετά κοινά στοιχεία με την πολιτική της MyHeritage. Αρχικά, γίνεται αναφορά στο τι καλύπτει αυτή η πολιτική και στο πως συλλέγονται τα προσωπικά δεδομένα των χρηστών (T-Mobile). Επεξηγούνται ποια από τα δεδομένα παρέχονται άμεσα στην εταιρία, ποια συλλέγονται αυτόματα, καθώς και ποια από τα δεδομένα συλλέγονται από άλλες εταιρίες και ποια εξάγονται από την εταιρία. Στη συνέχεια, αναφέρεται στο πως χρησιμοποιούνται αυτά τα δεδομένα από την εταιρία, τι συμβαίνει όταν εξάγονται τα δεδομένα και πως τα προστατεύει η εταιρία (T-Mobile). Ταυτόχρονα, τονίζονται οι περιπτώσεις χρήσης των δεδομένων από διαφημιστικές εταιρίες, η προστασία που υπάρχει σε περίπτωση δεδομένων που αφορούν παιδιά, τι επιλογές έχει ο χρήστης ως προς τα δεδομένα του και το πώς η εταιρία επικοινωνεί στους χρήστες τις αλλαγές της πολιτικής.

Η εταιρία US Postal Services, στην πολιτική ασφάλειας της αρχικά ορίζει το πεδίο εφαρμογής της πολιτικής ενώ στη συνέχεια εξηγεί την χρήση των δεδομένων. Χρησιμοποιεί διαφορετικό τρόπο διατύπωσης καθώς δίνει στον χρήστη τις πληροφορίες που χρειάζεται να ξέρει μέσα από συγκεκριμένα θέματα (US Postal Services). Υπάρχει μια παράγραφος που ανακοινώνει τις πρακτικές απορρήτου της εταιρίας, συμπεριλαμβανομένων των δικαιωμάτων του Privacy Act, ένα κομμάτι αναφέρεται στις επιλογές και τις προτιμήσεις των χρηστών, ένα άλλο στα χαρακτηριστικά ασφάλειας και στα στοιχεία ελέγχου του πάροχου υπηρεσιών, στο που πρέπει να υποβάλλονται σχετικές ερωτήσεις, ποιες τεχνολογίες χρησιμοποιούνται για την αποτελεσματική λειτουργία της ιστοσελίδας και επίσης υπάρχει κομμάτι για την προστασία των παιδιών (US Postal Services).

Άλλη μια από τις εταιρίες που ενημέρωσε τον Δεκέμβριο της πολιτική της είναι η Equifax. Σε αυτή την πολιτική, εξηγείται η συλλογή των προσωπικών δεδομένων, μαζί με τις πηγές από τις οποίες συλλέγονται (Equifax.). Αναλύεται το πώς χρησιμοποιούνται αυτά τα δεδομένα από την εταιρία και ποια από αυτά κοινοποιούνται σε άλλες εταιρίες για διαφημιστικούς σκοπούς. Επίσης, δίνονται λύσεις του εργατικού δυναμικού της εταιρίας και εξηγούνται οι τεχνολογίες που χρησιμοποιούνται για την προστασία των δεδομένων στον ιστότοπο, όπως η χρήση των cookies, το web beacons και άλλλων (Equifax.). Αναφέρονται οι επιλογές και ο έλεγχος που δικαιούται να έχει ο χρήστης ως προς τις πληροφορίες του ενώ δίνονται γενικά κάποιες πληροφορίες για την ασφάλεια.

Η Tycketfly, παρόλο που το περιστατικό παραβίασης της συνέβη το 2018, δεν έχει αναθεωρήσει την πολιτική ασφάλειας της από τον Οκτώβριο του 2017. Αρχικά, παρέχει τρόπους επικοινωνίας με την

εταιρία (Tycketfly). Στη συνέχεια, αναλύεται η συγκατάθεση των χρηστών, καθώς και το τι ισχύει για τα παιδιά. Ένα σημαντικό κομμάτι που αξίζει να σημειωθεί είναι ότι η πολιτική περιέχει πληροφορίες για χρήστες οι οποίοι βρίσκονται εκτός των Ηνωμένων Πολιτειών. Επεξηγούνται τα δεδομένα που συλλέγονται, η χρήση τους και η γνωστοποίηση τους (Tycketfly). Γίνεται αναφορά στις ιστοσελίδες και εφαρμογές τρίτων και στο πως επεξεργάζονται τα δεδομένα των χρηστών και δίνονται οι επιλογές όπου έχουν οι χρήστες σχετικά με τις πληροφορίες τους.

Η Marriot International, ως εταιρία διαχείρισης ξενοδοχείων, περιέχει κάποιες επιπλέον ενότητες στην πολιτική της. Στην αρχή αναφέρεται στις προτιμήσεις απορρήτου, cookies, επικοινωνίας και κοινής χρήσης των δεδομένων, έπειτα αναλύει τα δικαιώματα απορρήτου και ποια προσωπικά δεδομένα συλλέγονται μαζί με το πώς συλλέγονται και επίσης ποια άλλα δεδομένα συγκεντρώνονται (Marriot International). Πως χρησιμοποιούνται αυτά τα δεδομένα και τι δικαίωμα έχει ο χρήστης για να αποσύρει την συγκατάθεση του. Ταυτόχρονα, η πολιτική αναφέρεται στο που αποκαλύπτονται τα δεδομένα και ποιες είναι οι χρήσεις και γνωστοποιήσεις τους, καθώς και η διαφήμιση σε τρίτους οργανισμούς. Οι επιπλέον ενότητες τις πολιτικής περιλαμβάνουν θέματα ασφάλειας, πρόσβασης και διατήρησης, πως μπορεί ο χρήσεις να ζητήσει πρόσβαση στην επεξεργασία των δεδομένων του, δίνονται πληροφορίες για την κράτηση στο ξενοδοχείο, τα ευαίσθητα δεδομένα, την χρήση των υπηρεσιών από ανήλικους καθώς και την διασυνοριακή μεταφορά (Marriot International). Παρέχεται πιστοποιητικό προστασίας του ιδιωτικού απορρήτου, ενημέρωση της δήλωσης και τρόποι επικοινωνίας.

Ενδιαφέρον αποτελεί η πολιτική ασφάλειας της εταιρίας Eyewire λόγω του γεγονός ότι δεν έχει ανανεωθεί από το 2013, ενώ το περιστατικό παραβίασης δεδομένων συνέβη το 2016. Περιέχει όρους χρήσης, στους οποίους διευκρινίζει κάποιους ορισμούς και έννοιες τόσο της πληροφορικής όσο και της εταιρίας (Eyewire). Στην πολιτική της αναφέρει ποιες από τις πληροφορίες συλλέγονται, πως χρησιμοποιούνται από την εταιρία, πως προστατεύονται οι πληροφορίες αυτές και ποια είναι η πολιτική διατήρησης των δεδομένων των χρηστών. Επίσης, δίνεται απάντηση στο ερώτημα της χρήσης cookies από την εταιρία, αν και σε ποιους ανακοινώνονται οι πληροφορίες σε εξωτερικούς φορείς, πως συνδέονται οι τρίτες ιστοσελίδες, καθώς και ποια είναι η προστασία των παιδικών πληροφοριών (Eyewire). Ως προς το θέμα της ενημέρωσης των αλλαγών της πολιτικής, η εταιρία δηλώνει σε μια φράση ότι «Αν αποφασίσουμε να αλλάξουμε την πολιτική απορρήτου, θα δημοσιεύσουμε αυτές τις αλλαγές σε αυτήν τη σελίδα».

Τέλος, το μέσο κοινωνικής δικτύωσης Friend Finder Newtork, διατήρησε την πολιτική που είχε και πρόσθεσε επιπλέον κείμενο στο οποίο συμμορφώνεται με τους κανονισμούς του GDPR (Friend Finder Newtork). Διευκρινίζει ότι η πολιτική ισχύει για όλους τους ιστότοπους και τις θυγατρικές της εταιρίας και όπως και οι υπόλοιπες πολιτικές, εξηγεί την συλλογή, χρήση και αποκάλυψη των πληροφοριών, ποιες πληροφορίες συλλέγονται και πως χρησιμοποιούνται, πότε και σε ποιους θα αποκαλυφθούν, ποια είναι η χρήση των cookies, ποια η συλλογή, χρήση και αποκάλυψη πληροφοριών από τρίτες ιστοσελίδες, δίνεται μια σημείωση για τα παιδιά, καθώς επίσης και οδηγίες για το πώς ο χρήστης μπορεί να προστατεύσει τον κωδικό πρόσβασης του (Friend Finder Newtork). Δίνονται επίσης, διευκρινίσεις για την σχέση των

θυγατρικών της εταιρίας με τις πληροφορίες των χρηστών. Στην ενότητα της εφαρμογής του GDPR στην πολιτική ασφάλειας της εταιρίας, γίνεται επεξήγηση των όρων «προσωπικά δεδομένα» και «ευαίσθητα προσωπικά δεδομένα», αναλύοντας παράλληλα το νομικό πλαίσιο για την επεξεργασία των δεδομένων με βάση τα άρθρα του νέου νόμου. Διευκρινίζονται τα δικαιώματα των χρηστών και οι περιορισμοί της εταιρίας.

Παρατηρείται λοιπόν, το γεγονός ότι παρόλο που τα περιστατικά προέρχονται από διαφορετικούς τομείς οργανισμών, οι πολιτικές ασφάλειας τους δεν διαφέρουν ως προς την συλλογή, επεξεργασία και αποκάλυψη των δεδομένων. Εκεί που διαφέρουν είναι στην τήρηση ή όχι του Γενικού Κανονισμού Προστασίας Δεδομένων, στην συχνότητα αναθεώρησης της πολιτικής και στον τρόπο με τον οποίο εξηγούν στους χρήστες το περιεχόμενο της. Γενικά, η γλώσσα που χρησιμοποιείται είναι απλή και κατανοητή για τους χρήστες χωρίς ιδιαίτερες γνώσεις, ενώ δίνονται αρκετές πληροφορίες σε διάφορες ερωτήσεις όπου μπορεί να έχουν. Είναι σημαντικό το ότι υπάρχει ξεχωριστή ενότητα για τις πληροφορίες ανηλίκων, καθώς υπάρχει μεγαλύτερη ανάγκη για προστασία των πληροφοριών τους. Είναι απαραίτητη η συχνή αναθεώρηση της πολιτικής, καθώς και η ενημέρωση των χρηστών για οποιαδήποτε αλλαγή προκύπτει ως προς την προστασία των δεδομένων τους.

5.4 Αντιμετώπιση περιστατικών παραβίασης

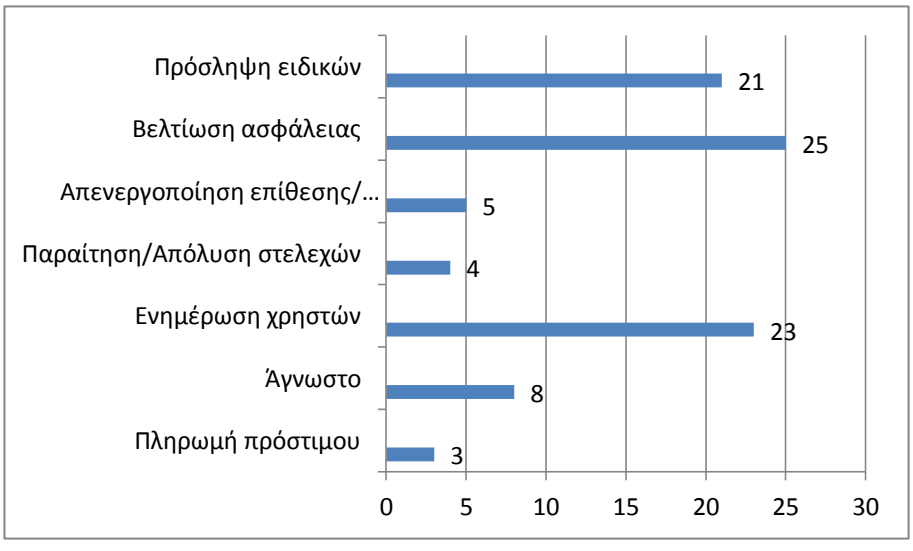
Παρόλο που κάθε χρόνο οι οργανισμοί πιστεύουν ότι τα περιστατικά παραβίασης δεδομένων έχουν λιγότερες πιθανότητες να συμβούν, παρατηρείται ότι ιδιαίτερα τα τελευταία χρόνια, αυξάνονται ολοένα και περισσότερο οι παραβιάσεις δεδομένων. Η ύπαρξη ενός σχεδίου απόκρισης σε περιστατικά παραβίασης είναι σημαντική για την λειτουργία του οργανισμού. Σύμφωνα με μια μελέτη για την ανθεκτικότητα στον κυβερνοχώρο από την IBM, το 77% των ανώτερων των οργανισμών παραδέχθηκε ότι δεν έχουν ένα επίσημο σχέδιο αντιμετώπισης περιστατικών που να εφαρμόζεται με συνέπεια στον οργανισμό τους (Go anywhere, 2018). Η δημιουργία και η διατήρηση ενός σχεδίου αντιμετώπισης παραβίασης δεδομένων δεν πρέπει να αποτελεί προαιρετικό βήμα, καθώς οι επιπτώσεις μιας παραβίασης μπορεί να αποβούν μοιραίες για τον οργανισμό.

Έχουν αναπτυχθεί κάποια πρότυπα παραβίασης δεδομένων με βέλτιστες πρακτικές, τα οποία μπορούν να αξιοποιηθούν από έναν οργανισμό (Go anywhere, 2018). Η Διεθνής Ένωση Επαγγελματιών Προστασίας Προσωπικών Δεδομένων (ή IAPP) δημιούργησε ένα εργαλείο σχεδίου αντιμετώπισης παραβιάσεων ασφαλείας για όλους τους επαγγελματίες στον τομέα της ασφάλειας στον κυβερνοχώρο ή τους επαγγελματίες πληροφορικής που πρέπει να καταρτίσουν λεπτομερή σχέδιο επίθεσης (Go anywhere, 2018). Το Security Breach Response Plan Toolkit, περιλαμβάνει ένα ερωτηματολόγιο 31 σημείων που καθοδηγεί προς τη σωστή κατεύθυνση και τα επόμενα βήματα που θα βοηθήσουν σε ένα σταθερό και εφαρμόσιμο σχέδιο για το μέλλον.

Το Σχέδιο Αντιμετώπισης Παραβίασης Δεδομένων (Data Breach Response Plan) της Experian, αποτελεί έναν οδηγό για την ανταπόκριση σε παραβιάσεις δεδομένων (Go anywhere, 2018). Περιλαμβάνει την επιλογή της C-Suite στα σχέδια του οργανισμού, το πώς να δημιουργείται και να εφαρμόζεται το σχέδιο αντιμετώπισης, πώς να ελέγχεται η ετοιμότητα του και το πώς να διαχειριστούν οι υπάλληλοι την παραβίαση. Επίσης, η Federal Trade Commission (FTC), δημιούργησε τον οδηγό Ανταπόκρισης στην παραβίαση δεδομένων (Data Breach Response: A Guide for Business) για τις επιχειρήσεις. Αυτός ο οδηγός είναι προετοιμασία παραίτησης κατά το ήμισυ των δεδομένων (πριν από την παραβίαση) και απόκριση κατά το ήμισυ των παραβιάσεων δεδομένων (για μετά την παραβίαση) (Go anywhere, 2018). Γίνεται χρήση ενός έγγραφου 12 σελίδων από την Ομοσπονδιακή Επιτροπή Εμπορίου για τον έλεγχο και την κατανόηση του τι θα πρέπει να γίνει εάν διακυβεύονται τα δεδομένα. Ακόμα κι αν υπάρχει ήδη ένα σχέδιο αντιμετώπισης περιστατικών, θα μπορέσει να συμπληρώσει τυχόν κενά που ενδεχομένως να υπάρχουν. Ο NIST δημιούργησε έναν Οδηγό για την Ανάκτηση Γεγονότων στον Κυβερνοχώρο για τον σχεδιασμό και την ανάκαμψη περιστατικών ασφάλειας. Παρέχει αναλυτικές οδηγίες για τα στάδια σχεδιασμού, βελτίωσης, οικοδόμησης και κατανόησης της πολιτικής αποκατάστασης.

Στην έρευνα αυτής της διπλωματικής, τα περιστατικά παραβίασης δεδομένων που συλλέχθηκαν, έχουν διαφορετικούς τρόπους αντιμετώπισης μεταξύ τους, παρόλα αυτά μπορούν να κατηγοριοποιηθούν με βάση την μέθοδο που χρησιμοποίησαν. Στο παρακάτω γράφημα, φαίνονται πόσα περιστατικά αντιμετώπισαν την παραβίαση με την βοήθεια κάποιου ειδικού, με την βελτίωση της ασφάλειας του συστήματος, με την απενεργοποίηση της επίθεσης ή κάποιου προϊόντος της εταιρίας, με την παραίτηση ή απόλυση στελεχών του οργανισμού, πόσα περιστατικά ενημέρωσαν τους χρήστες για την παραβίαση, αν κάποιο περιστατικό έπρεπε να πληρώσει κάποιο πρόστιμο και πόσα από τα περιστατικά δεν γνωστοποίησαν τον τρόπο αντιμετώπισης της παραβίασης δεδομένων τους.

Γράφημα 4, Αντιμετώπιση περιστατικών παραβίασης



Γενικά, παρατηρείται ότι από τα 70 περιστατικά, μόνο τα 23 ενημέρωσαν τους χρήστες, ενώ τα 25 από αυτά παρενέβη σε ενέργειες για την βελτίωση της ασφάλειας του συστήματος τους. Στην κατηγορία πρόσληψης ειδικών, συμπεριλήφθησαν 21 περιστατικά τα οποία για να αντιμετωπίσουν την παραβίαση προσέλαβαν κάποιον ειδικό πάνω σε θέματα ασφάλειας έτσι ώστε να τους βοηθήσει στην καλύτερη αντιμετώπιση του ζητήματος. Επίσης, σε αυτή την κατηγορία υπάρχουν περιστατικά τα οποία αντιμετωπίστηκαν με την βοήθεια της αστυνομίας και του FBI, εντοπίζοντας και φυλακίζοντας τον επιτιθέμενο.

Στην κατηγορία βελτίωση ασφάλειας, αναφέρονται 25 περιστατικά, εκ των οποίων τα περισσότερα σχετίζονται με αναβαθμίσεις της ασφάλειας και των μέτρων προστασίας του συστήματος. Παρόλα αυτά, υπάρχουν και κάποιες περιπτώσεις όπου η εταιρία επέλεξε τον περιορισμό των επηρεασμένων δεδομένων, ζητώντας από τους χρήστες της να αλλάξουν τους κωδικούς πρόσβασης τους.

Στην επόμενη κατηγορία, 5 από τα περιστατικά χρειάστηκε να προβούν στην απενεργοποίηση είτε ολόκληρου του συστήματος τους είτε ενός μέρους του. Για παράδειγμα, όπως έχει αναφερθεί και σε προηγούμενο κεφάλαιο, η Google αναγκάστηκε να απενεργοποιήσει τελείως την λειτουργία του Google Plus, καθώς δεν μπόρεσε να βρεθεί κάποιος πιο αποτελεσματικός τρόπος. Κάποιες εταιρίες χρειάστηκε να διαγράψουν κάποια από τα δεδομένα τους για να μπορέσουν να αποκαταστήσουν το περιστατικό.

Υπήρξαν ωστόσο και 4 παραβιάσεις δεδομένων, οι οποίες για να αντιμετωπιστούν, είχαν ως αποτέλεσμα την παραίτηση ή απόλυση κάποιων στελεχών της εταιρίας. Αυτό συνέβη είτε γιατί το άτομο εμπλέκονταν στην παραβίαση, οπότε θεωρήθηκε απαραίτητη η απομάκρυνση του, είτε γιατί το μέγεθος της ζημιάς στον οργανισμό ήταν μεγάλο και έτσι τα στελέχη δεν άντεξαν να ανταπεξέλθουν στο ζήτημα και δήλωσαν την παραίτηση τους.

Παρόλο που 23 από τα 70 περιστατικά ενημέρωσαν τους χρήστες για την παραβίαση των δεδομένων τους, θεωρείται αναγκαίο και επίσης, σύμφωνα με τον Γενικό Κανονισμό, υποχρεωτικό οι οργανισμοί να ενημερώνουν τους χρήστες για οτιδήποτε επηρεάζει την ασφάλεια των προσωπικών δεδομένων τους. Αυτός ο αριθμός της έρευνας δείχνει ότι σχεδόν το 1/3 των περιπτώσεων ενημερώνει έγκαιρα τους χρήστες, ενώ υπάρχουν περιστατικά όπου επιλέγουν να μην αναφέρουν καθόλου την παραβίαση. Ένας λόγος για τον οποίο δεν δημοσιοποιούν τις παραβιάσεις τους οι εταιρίες είναι ότι υπάρχει ο κίνδυνος να χάσουν τους χρήστες τους μετά την κοινοποίηση προβλήματος στο σύστημα τους, κάτι το οποίο δεν τους συμφέρει οικονομικά και επηρεάζει την φήμη του οργανισμού.

Στην κατηγορία των περιστατικών που χρειάστηκε να πληρώσουν κάποιο οικονομικό πρόστιμο, συμπεριλαμβάνονται μόνο 3 περιστατικά, τα οποία όμως έπρεπε να πληρώσουν για την άμεση αντιμετώπιση της παραβίασης. Ακόμα και σήμερα, γίνονται πολλές δίκες για περιστατικά παραβίασης δεδομένων που έχουν γίνει στο παρελθόν και αποδεικνύεται ότι χρειάζεται να καταβάλουν κάποιο ποσό είτε στους χρήστες που επηρεάστηκαν είτε λόγω απόφασης του δικαστηρίου.

Τέλος, 8 από τις 70 εταιρίες, επέλεξαν να μην γνωστοποιήσουν τους τρόπους με τους οποίους αντιμετώπισαν την παραβίαση. Αρκετές μάλιστα δεν θέλησαν να κάνουν κάποιο σχόλιο για το περιστατικό ενώ υπήρξαν και περιπτώσεις όπου η εταιρία αρνήθηκε την ύπαρξη προβλήματος στο σύστημα της.

Με βάση την έρευνα που έγινε σε αυτή τη διπλωματική εργασία, για τα περιστατικά παραβίασης δεδομένων που συζητήθηκαν και αναφέρθηκαν, προτείνεται η βελτίωση της ασφάλειας των πληροφοριακών συστημάτων των οργανισμών με συνεχή παρακολούθηση των εξελίξεων και αναβάθμιση των συστημάτων τους, καθώς λόγω της ταχείας εξέλιξης των τεχνολογιών, υπάρχουν πολύ συχνές αλλαγές ως προς την προστασία των δεδομένων αλλά και ως προς τις μεθόδους που χρησιμοποιούν οι επιτιθέμενοι για την παραβίαση τους.

Επίσης, κρίνεται απαραίτητη η σωστή ενημέρωση τόσο των υπαλλήλων των οργανισμών όσο και του ανώτερου προσωπικού της εκάστοτε εταιρείας, έτσι ώστε να υπάρχει η κατάλληλη προετοιμασία και να είναι όλα τα άτομα κατάλληλα εκπαιδευμένα και σε ετοιμότητα για την αντιμετώπιση οποιουδήποτε περιστατικού προκύψει. Μέσω ενημερωτικών ημερίδων και σεμιναρίων, οι υπάλληλοι ενός οργανισμού θα είναι σε θέση να γνωρίζουν τις απαραίτητες πληροφορίες και μεθόδους για να μπορέσουν να ανταπεξέλθουν σε οτιδήποτε τους ζητηθεί. Η σωστή οργάνωση του οργανισμού, θα συμβάλει στην καλύτερη και αποτελεσματικότερη προστασία των πληροφοριακών συστημάτων του.

Σε γενικές γραμμές, όλοι οι τρόποι πρόληψης και αντιμετώπισης που αναφέρθηκαν σε αυτό το κεφάλαιο συμβάλουν τόσο στην προστασία όσο και στην επίλυση ενός περιστατικού παραβίασης δεδομένων. Ο κυριότερος τρόπος πρόληψης είναι η σωστή ενημέρωση των υπαλλήλων και η επίγνωση τους σε θέματα ασφάλειας, καθώς η έλλειψη εκπαίδευσης είναι αυτή που πολλές φορές οδηγεί σε προβλήματα ασφάλειας. Παράλληλα με την σωστή εκπαίδευση, η δημιουργία πολιτικών ασφάλειας και σχεδίων διαχείρισης κινδύνων βοηθούν στην άμεση αντιμετώπιση οποιουδήποτε προβλήματος προκύψει στον οργανισμό.

6

Συμπεράσματα

6.1 Συμπεράσματα με βάση τα περιστατικά παραβίασης δεδομένων

Το θέμα της παρούσας διπλωματικής εργασίας είναι η έρευνα των περιστατικών παραβίασης δεδομένων που έχουν δημοσιοποιηθεί και η σχέση τους με το ανθρώπινο λάθος. Κατά τη διεξαγωγή της εργασίας, έγινε μια έρευνα πάνω σε περιστατικά παραβίασης δεδομένων που έχουν δημοσιευθεί τα τελευταία πέντε χρόνια. Επιπλέον, τα περιστατικά που εντοπίστηκαν, ταξινομήθηκαν σε κατηγορίες για την καλύτερη παρακολούθηση τους και την αποτελεσματικότερη εξαγωγή συμπερασμάτων.

Στα πλαίσια της εργασίας, αναλύθηκαν οι ορισμοί των προσωπικών δεδομένων και των παραβιάσεων δεδομένων, μαζί με το νομικό πλαίσιο που υπάρχει για την προστασία τους. Στη συνέχεια, έγινε εξήγηση της ανάγκης ύπαρξης ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών για τον οργανισμό, καθώς και η μέθοδος που ακολουθείται για την δημιουργία του. Έπειτα, δόθηκαν τα υπάρχοντα εργαλεία για τη διαχείριση των περιστατικών ασφάλειας, η μεθοδολογία διαχείρισης κινδύνων, η ανάγκη ύπαρξης πολιτικών ασφάλειας και τρόποι πρόληψης και αντιμετώπισης περιστατικών παραβίασης δεδομένων.

Κατά την έρευνα, συγκεντρώθηκαν 70 δημοσιοποιημένα περιστατικά παραβίασης δεδομένων, κυρίως από πηγές ηλεκτρονικών σελίδων, τα οποία συνέβησαν τα τελευταία πέντε χρόνια, από το 2014 έως το 2019. Για την καλύτερη εξαγωγή αποτελεσμάτων, επιλέχθηκαν περιστατικά των οποίων το μέγεθος της απώλειας των δεδομένων τους ήταν μεγαλύτερο από 500.000. Στη συνέχεια, οι περιπτώσεις αυτές κατηγοριοποιήθηκαν ανάλογα με την χρονολογία στην οποία συνέβησαν, τον τομέα του οργανισμού, την

αιτία που προκάλεσε την παραβίαση και τους τρόπους αντιμετώπισης που χρησιμοποίησε ο κάθε οργανισμός.

Τα αποτελέσματα της έρευνας, δείχνουν, ότι τα περισσότερα περιστατικά παραβίασης δεδομένων συνέβησαν κυρίως το 2015 και το 2018, με το 2017 να αποτελεί την χρονιά με τα λιγότερα περιστατικά. Ανησυχητικό παρατηρείται το γεγονός ότι παρόλο που έχουν θεσπιστεί νέοι νόμοι για την προστασία των πληροφοριών, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), το 2018 και το 2019 υπήρξε μεγάλος αριθμός περιπτώσεων παραβίασης δεδομένων, κάτι που υποδηλώνει την μη συμμόρφωση των οργανισμών με τα υπάρχοντα εργαλεία που διατίθενται για την ασφάλεια των πληροφοριακών συστημάτων τους.

Με βάση τα αποτελέσματα, συμπεραίνεται επίσης, ότι οι βασικές αιτίες που συμβαίνουν παραβιάσεις δεδομένων είναι η επίθεση από κακόβουλους (χάκερ) και η έλλειψη ασφάλειας των πληροφοριακών συστημάτων, με τουλάχιστον 50 και 46 περιστατικών αντίστοιχα, από τις 70 περιπτώσεις να βρίσκονται σε αυτές τις κατηγορίες. Η έλλειψη ασφάλειας οφείλεται τις περισσότερες φορές σε μη ενημερωμένο προσωπικό, κακή προστασία των πληροφοριακών συστημάτων αλλά και σε εσωτερικούς επιτιθέμενους οι οποίοι απέκτησαν μη εξουσιοδοτημένη πρόσβαση σε βάσεις δεδομένων. Ένα ποσοστό των περιστατικών περιλαμβάνει την διαρροή δεδομένων λόγω λανθασμένων μηχανισμών προστασίας των πληροφοριών και πολλών ευπαθειών του συστήματος.

Τα περιστατικά παραβίασης δεδομένων της έρευνας, κατηγοριοποιήθηκαν με βάση τον τομέα στον οποίο ανήκει η κάθε επιχείρηση. Παρατηρήθηκε ότι οι περισσότερες παραβιάσεις συνέβησαν σε εταιρείες που είτε ασχολούνται αποκλειστικά με την ιστοσελίδα τους είτε την έχουν συμπληρωματικά για την ενίσχυση των υπηρεσιών τους. Τα 18 από τα 70 περιστατικά συνέβησαν σε ιστοσελίδες ενώ μόνο τα 7 από τα 70 σχετίζονται με μέσα κοινωνικής δικτύωσης, στα οποία όμως κύρια αιτία ήταν η έλλειψη ασφάλειας των πληροφοριακών συστημάτων τους. Παράλληλα, τα 13 από τα 70 περιστατικά συνέβησαν στον τομέα της υγείας, με αρκετά περιστατικά επίσης να αφορούν τομείς τηλεπικοινωνιών, μέσων μεταφοράς, οικονομικών επιχειρήσεων αλλά και κυβερνητικών οργανισμών. Να σημειωθεί ότι στην παρούσα έρευνα δεν υπήρχαν περιστατικά παραβίασης δεδομένων από Πανεπιστημιακούς φορείς, οι οποίοι πολλές φορές είχαν αντίστοιχες περιπτώσεις.

Ο βασικός σκοπός της έρευνας ήταν η συσχέτιση των παραβιάσεων με το ανθρώπινο λάθος. Με βάση τα αποτελέσματα, εντοπίστηκε ότι ένας συγκεκριμένος αριθμός περιπτώσεων οφείλονται συγκεκριμένα από επίθεση υπαλλήλου κατά των δεδομένων. Η βασική αιτία του ανθρώπινου παράγοντα είναι η μη εξουσιοδοτημένη πρόσβαση αλλά και η λανθασμένη αποκάλυψη των δεδομένων. Αυτό έχει ως αποτέλεσμα να σημειώνονται περισσότερα από τα μισά περιστατικά παραβίασης τα οποία οφείλονται σε κακόβουλη επίθεση (χακάρισμα) ενώ αρκετά περιστατικά είχαν διαρροή των δεδομένων τους. Παρόλα αυτά, η έλλειψη ασφάλειας και ενημέρωσης του προσωπικού των οργανισμών, αποτελεί ένα από τα σημαντικότερα προβλήματα και υπολογίζεται ως ανθρώπινο λάθος. Πολλές φορές οι οργανισμοί, στην προσπάθεια τους να προστατεύσουν αποτελεσματικά τα πληροφοριακά συστήματα τους, δίνουν

περισσότερη σημασία στην ασφάλεια των υλικών αγαθών και ξεχνούν τον ανθρώπινο παράγοντα, ο οποίος όμως αποτελεί την μεγαλύτερη απειλή για τα συστήματα τους.

Όπως προτάθηκε και στο προηγούμενο κεφάλαιο, η επίγνωση ασφάλειας των υπαλλήλων, η χρήση μεθοδολογίας διαχείρισης κινδύνων, η ύπαρξη πολιτικής ασφάλειας και η σωστή αντιμετώπιση περιστατικών παραβίασης δεδομένων, παίζουν καθοριστικό ρόλο τόσο στην πρόληψη, όσο και στην άμεση αντιμετώπιση τέτοιων περιπτώσεων.

Σε γενικές γραμμές, για την πρόληψη και αντιμετώπιση των περιστατικών παραβίασης δεδομένων της έρευνας, προτείνεται αρχικά η συμμόρφωση των εταιρειών με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR), η δημιουργία επιμορφωτικών σεμιναρίων για τους υπαλλήλους των οργανισμών πάνω σε θέματα αντιμετώπισης καταστάσεων παραβίασης δεδομένων αλλά και η ανάγκη για την καλύτερη και αποτελεσματικότερη διασφάλιση των προσωπικών πληροφοριών. Επίσης, συνιστάται η συνεχής ενημέρωση και αναβάθμιση των πολιτικών ασφάλειας των εταιρειών, έτσι ώστε να είναι σε θέση να ανταπεξέλθουν σε οποιοδήποτε ζήτημα προκύψει μέσα στον οργανισμό. Οι υπεύθυνοι της ασφάλειας των πληροφοριακών συστημάτων των εταιρειών, θα πρέπει να γνωρίζουν τις συνεχόμενα αναπτυσσόμενες εξελίξεις πάνω σε θέματα ασφάλειας αλλά και τις νέες απειλές που δημιουργούνται αρκετά συχνά λόγω της εξέλιξης της τεχνολογίας.

Η μείωση των περιστατικών παραβίασης δεδομένων, αποτελεί ένα σημαντικό ζήτημα των τελευταίων χρόνων, λόγω της συνεχώς αυξημένης χρήσης ηλεκτρονικών υπηρεσιών, οι οποίες παρόλο που διευκολύνουν την καθημερινότητα του ανθρώπου σε πολλούς τομείς, αποτελούν και εύκολο στόχο των επιτιθέμενων για την απόκτηση όλου αυτού του όγκου προσωπικών πληροφοριών που διαθέτουν οι οργανισμοί. Με τη σωστή ενημέρωση, τη χρήση αποτελεσματικών εργαλείων και την άμεση ανταπόκριση σε οποιοδήποτε ζήτημα προκύψει, μπορεί να επιτευχθεί η αποτελεσματικότερη προστασία των προσωπικών δεδομένων των χρηστών αλλά και των πληροφοριακών συστημάτων των οργανισμών από τις παραβιάσεις δεδομένων.

Το συγκεκριμένο ζήτημα είναι ένα θέμα που απασχολεί και θα απασχολήσει αρκετά τους ερευνητές τα επόμενα χρόνια. Γι’ αυτό τονίζεται η ανάγκη για περεταίρω διερεύνηση του πεδίου αυτού, με σκοπό την εξάλειψη του προβλήματος.

7

Αναφορές

Abel R. (2019), 2M credit cards exposed in Buca di Beppo, Earl of Sandwich, Planet Hollywood parent company breach. Διαθέσιμο στην ιστοσελίδα: https://www.scmagazine.com/home/security-news/data-breach/2m-credit-cards-exposed-in-buca-di-beppo-earl-of-sandwich-planet-hollywood-parent-company-breach/

Abigail T. (2015), In wake of T-Mobile and Experian data breach, John Legere did what all CEOs should do after a hack. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/abigailtracy/2015/10/02/in-wake-of-t-mobile-and-experian-data-breach-john-legere-did-what-all-ceos-should-do-after-a-hack/

Acquisti A, Friedman A. and Telang R. (2006) 'Is there a cost to privacy breaches? An event study', Twenty-Seventh International Conference on Information Systems, Milwaukee, pp. 1563-1580

Acquisti A, Friedman A. and Telang R. (2006) 'Is there a cost to privacy breaches? An event study', Twenty-Seventh International Conference on Information Systems, Milwaukee, pp. 1563-1580

Acquisti A. (2004) Privacy and Security of Personal Information. In: Camp L.J., Lewis S. (eds) Economics of Information Security. Advances in Information Security, vol 12. Springer, Boston, MA

Acquisti A. (2004) Privacy and Security of Personal Information. In: Camp L.J., Lewis S. (eds) Economics of Information Security. Advances in Information Security, vol 12. Springer, Boston, MA

Aiello C. (2018), Under Armour says data breach affected about 150 million MyFitnessPal accounts. Διαθέσιμο στην ιστοσελίδα: https://www.cnbc.com/2018/03/29/under-armour-stock-falls-after-company-admits-data-breach.html

Alfred Ng (2018), Ticketfly takes websites offline after hack and ransom demand. Διαθέσιμο στην ιστοσελίδα: https://www.cnet.com/news/ticketfly-takes-websites-offline-after-series-of-cyberattacks/

Ashford W. (2019), Breach cost $53m in Q2, says Desjardins. Διαθέσιμο στην ιστοσελίδα: https://www.computerweekly.com/news/252468297/Breach-cost-53m-in-Q2-says-Desjardins

Associated press (2018), Cathay Pacific Airways: data breach affected 9.4 million. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/travel/flights/todayinthesky/2018/10/25/cathay-pacific-airways-data-breach-affected-9-4-million/1759773002/

Augenbraun E. (2014), Hackers post millions of stolen Gmail passwords on Russian site. Διαθέσιμο στην ιστοσελίδα: https://www.cbsnews.com/news/russian-hackers-steal-5-million-gmail-passwords/

Balakrishnan A. (2016), 1.5 million Verizon Enterprise customers hacked: Report. Διαθέσιμο στην ιστοσελίδα: https://www.cnbc.com/2016/03/24/15-million-verizon-enterprise-customers-hacked-report.html

Baraniuk C. (2015), Ashley Madison: 'suicides' over website hack. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-34044506

Barrabi T. (2018), Panera Bread data breach exposes customer records. Διαθέσιμο στην ιστοσελίδα: https://www.foxbusiness.com/markets/panera-bread-data-breach-exposes-customer-records

Barrabi T. (2018), TimeHop data breach exposes key information for millions of users. Διαθέσιμο στην ιστοσελίδα: https://www.foxbusiness.com/markets/timehop-data-breach-exposes-key-information-for-millions-of-users

Barth B. (2017), Nearly 29M records stolen in breach of Latin American social network Taringa! Διαθέσιμο στην ιστοσελίδα: https://www.scmagazine.com/home/security-news/data-breach/nearly-29m-records-stolen-in-breach-of-latin-american-social-network-taringa/

Basu E. (2015), Cybersecurity lessons learned from the Ashley Madison hack. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/

BBC Business News (2015), Hackers steal T-Mobile data on 15 million US customers. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/business-34420879

BBC Business News (2018), Cathay Pacific data hach hits 9.4 million passengers. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/business-45974020

BBC News (2015), Extortion attempt on victims of Patreon site hack. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-34899705

BBC News-Technology (2015), Cyber-attacks hit British Airways, GitHub and Slack. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-32115292

BBC Technology News (2014), Community Health Systems data hack hits 4.5 million. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-28838661

BBC Technology News (2014), Credit card details on 20 million South Koreans stolen. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-25808189

BBC Technology News (2014), Home Depot admits hack attack dates back to April. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-29125204

BBC Technology News (2016), Up to 400 million accounts in adult FriendFinder breach. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-37974266

BBC Technology News (2016), Yahoo 'state' hackers stole data from 500 million users. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/world-us-canada-37447016

BBC Technology News (2018), Marriot hack hits 500 million Starwood guests. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-46401890

BBC Technology News (2018), Toy firm VTech fined $650.000 over data breach. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-42620717

BBC Technology News (2018), Twitter users told to change passwords after internal leak. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/business-43995168

BBC Technology News (2018), Uber pays $148M over data breach cover-up. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-45666280

BBC US & Canada News (2015), Millions of US government works hit by data breach. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/world-us-canada-33017310

Belton B. (2014), Michaels retailer probing possible data breach. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/money/business/2014/01/25/michaels-retailer-credit-card-breach-reported/4895123/

Biggs J. (2015), Patreon Hacked, Gigabytes Of Data And Code Leaked. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2015/10/05/patreon-hacked-gigabytes-of-data-and-code-leaked/

Bisson D. (2017), Over 28 million Taringa! Users records exposed in data breach. Διαθέσιμο στην ιστοσελίδα: https://www.tripwire.com/state-of-security/latest-security-news/over-28-million-taringa-user-records-exposed-in-data-breach/

Blake A. (2015), Excellus BlueCross BlueShield hacked; 10.5M patients affected. Διαθέσιμο στην ιστοσελίδα: https://www.washingtontimes.com/news/2015/sep/10/excellus-bluecross-blueshield-hacked-105m-patients/

Bradley T. (2018), Security experts weigh in on massive data breach of 150 million MyFitnessPal accounts. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/tonybradley/2018/03/30/security-experts-weigh-in-on-massive-data-breach-of-150-million-myfitnesspal-accounts/

Brandom R. (2018), The breach that killed Google+ wasn't a breach at all. Διαθέσιμο στην ιστοσελίδα: https://www.theverge.com/2018/10/9/17957312/google-plus-vulnerability-privacy-breach-law

Brett Molina B. (2018), T-Mobile discloses data breach of consumer information. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/tech/nation-now/2018/08/24/t-mobile-hit-data-breach-consumer-information/1086512002/

Brewster T. (2015), Ashley Madison breach could expose privates of 37 million cheaters. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/thomasbrewster/2015/07/20/ashley-madison-attack/

Brewster T. (2016), Yahoo admits 500 million hit in 2014 breach. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/thomasbrewster/2016/09/22/yahoo-500-million-hacked-by-nation-state/

Bronstad A. (2019), Class actions over data breach involving Quest Diagnostics sent to New Jersey. Διαθέσιμο στην ιστοσελίδα: https://www.law.com/njlawjournal/2019/07/31/class-actions-over-data-breach-involving-quest-diagnostics-sent-to-new-jersey/?slreturn=20200008180553

Brook C. (2018), ORBITZ BREACH EXPOSES CUSTOMER DATA, 880,000 PAYMENT CARDS. Διαθέσιμο στην ιστοσελίδα: https://digitalguardian.com/blog/orbitz-breach-exposes-customer-data-880000-payment-cards

Brook C. (2019), SEC looking into First American breach. Διαθέσιμο στην ιστοσελίδα: https://digitalguardian.com/blog/sec-looking-first-american-breach

Brumfield J, Pritam N. and Ward C. (2016), Verizon's 2016 Data Breach Investigations Report finds cybercriminals are exploiting human nature. Διαθέσιμο στην ιστοσελίδα: https://www.prnewswire.com/news-releases/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-nature-300258134.html

Burgess C. (2018), How did the TimeHop data breach happen? Διαθέσιμο στην ιστοσελίδα: https://www.csoonline.com/article/3296486/how-did-the-timehop-data-breach-happen.html

Cain A. (2019), Buca di Beppo diners may have had their credit-card details stolen after the restaurant chain's parent company was hit with a major data breach. Διαθέσιμο στην ιστοσελίδα: https://www.businessinsider.com/buca-di-beppo-data-breach-2019-4

CAN (2019), Blood donor data leak: HSA's vendor says information that went online was accessed illegally and possibly extracted. Διαθέσιμο στην ιστοσελίδα: https://www.channelnewsasia.com/news/singapore/personal-data-of-800-000-blood-donors-accessed-illegally-hsa-ssg-11395364

Canva (2019), Canva security incident – May 24 FAQs. Διαθέσιμο στην ιστοσελίδα: https://support.canva.com/contact/customer-support/may-24-security-incident-faqs/#section1

Capital One (2019), Informatio on the Capital One cyber incident. Διαθέσιμο στην ιστοσελίδα: https://www.capitalone.com/facts2019/

Carte B. (2014), AOL confirms mail service hacked. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/tech/2014/04/22/aol-email-hacked/8003859/

Cathay Pacific Airways (2018), Cathay Pacific announces data security event affecting passenger data. Διαθέσιμο στην ιστοσελίδα: https://news.cathaypacific.com/cathay-pacific-announces-data-security-event-affecting-passenger-data

CBS News (2014), JP Morgan discloses data breach affected millions. Διαθέσιμο στην ιστοσελίδα: https://www.cbsnews.com/news/jp-morgan-chase-discloses-massive-data-breach-at-new-york-based-bank/

CBS News (2016), Massive IRS data breach much bigger than first thought. Διαθέσιμο στην ιστοσελίδα: https://www.cbsnews.com/news/irs-identity-theft-online-hackers-social-security-number-get-transcript/

Chacos B. (2018), Quora data breach FAQ: what 100 million hacked users need to know. Διαθέσιμο στην ιστοσελίδα: https://www.pcworld.com/article/3325199/quora-data-breach-faq-100-million-hacked-users.html

Cheng R. (2015), Data breach hits roughly 15M T-Mobile customers, applicants. Διαθέσιμο στην ιστοσελίδα: https://www.cnet.com/news/data-breach-snags-data-from-15m-t-mobile-customers/

Chi L. (2016), Philippines elections hack 'leaks voter data'. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-36013713

Chin M. (2018), 21 million exposed in TimeHop data breach: what to do now. Διαθέσιμο στην ιστοσελίδα: https://www.tomsguide.com/us/timehop-data-breach,news-27575.html

Choo F and Kurohi R.(2019), Personal information of over 800,000 blood donors was accessible online for 2 months: HSA. Διαθέσιμο στην ιστοσελίδα: https://www.straitstimes.com/singapore/health/personal-information-of-over-800000-blood-donors-exposed-online-hsa

Chuck E. (2018), Panera Bread's website exposed customer data, security experts says. Διαθέσιμο στην ιστοσελίδα: https://www.nbcnews.com/tech/security/panera-bread-s-website-exposed-customer-data-security-expert-says-n862381

Cichonski P, Millar T, Grance T. and Scarfone K. (2012), 'Computer security incident handling guide', NIST Special Publication 800-61 Revision 2

Cimpanu C. (2018), Premera BlueCross accused of destroying evidence in data breach lawsuit. Διαθέσιμο στην ιστοσελίδα: https://www.zdnet.com/article/premera-blue-cross-accused-of-destroying-evidence-in-data-breach-lawsuit/

Cimpanu C. (2019), Australian tech unicorn Canva suffers security breach. Διαθέσιμο στην ιστοσελίδα: https://www.zdnet.com/article/australian-tech-unicorn-canva-suffers-security-breach/

Cluley G. (2014), Domino's Pizza refuses to pay ransom after customer database hacked. Διαθέσιμο στην ιστοσελίδα: https://www.welivesecurity.com/2014/06/16/dominos-pizza-hacked/

Cluley G. (2018), Travel site Orbitz warns data breach may have exposed 880,000 payment card details. Διαθέσιμο στην ιστοσελίδα: https://www.tripwire.com/state-of-security/security-data-protection/orbitz-data-breach/

CNNMoney Staff (2015), The Ashley Madison hack… in 2 minutes. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2015/08/24/technology/ashley-madison-hack-in-2-minutes/

Colby C. (2019), Capital One data breach: what you can do now following bank hack. Διαθέσιμο στην ιστοσελίδα: https://www.cnet.com/how-to/capital-one-data-breach-what-you-can-do-now-following-bank-hack/

Coldewey D. (2018), Reddit breach exposes non-critical user data. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2018/08/01/reddit-breach-exposes-user-data-but-not-much/

Collins K. (2015), A rare detailed look inside the IRS's massive data breach, via a security expert who was a victim. Διαθέσιμο στην ιστοσελίδα: https://qz.com/445233/inside-the-irss-massive-data-breach/

Conger K. and Roof K. (2016), Weebly hacked, 43 million credentials stolen. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2016/10/20/weebly-hacked-43-million-credentials-stolen/

Connolly A. (2019), MP probe massive Desjardins data breach in emergency committee meeting. Διαθέσιμο στην ιστοσελίδα: https://globalnews.ca/news/5495478/desjardins-data-breach-public-safety-committee/

Contributor, Agence France Presse (2014), Huge South Korean data leak affects almost half the country. Διαθέσιμο στην ιστοσελίδα: https://www.businessinsider.com/south-korea-data-leak-2014-1

Cox J. (2016), *Another day, another hack: 20 million – Million – accounts on Taobao, China's Amazon*. Διαθέσιμο στην ιστοσελίδα: https://www.vice.com/en_us/article/xygx3n/another-day-another-hack-20-millionmillionaccounts-on-taobao-chinas-amazon

Crowe P. (2015), JP Morgan fell victim to the largest theft of customer data from a financial institution in US history. Διαθέσιμο στην ιστοσελίδα: https://www.businessinsider.com/jpmorgan-hacked-bank-breach-2015-11

Cyber Insurance (2016), Nival. Διαθέσιμο στην ιστοσελίδα: https://www.cyberinsurance.com/breaches/nival/

Dale B. (2015), Patreon Hacked: Some User Information Compromised. Διαθέσιμο στην ιστοσελίδα: https://observer.com/2015/09/patreon-hacked-some-user-information-compromised/

Dangerfield K. (2018), Ticketfly hacked: what to know about the online ticketing service's data breach. Διαθέσιμο στην ιστοσελίδα: https://globalnews.ca/news/4250616/ticketfly-breach-hacked-online-conert/

Davis J. (2019), Community Health Systems reaches settlement over 2014 breach of 4.5M. Διαθέσιμο στην ιστοσελίδα: https://healthitsecurity.com/news/community-health-systems-reaches-settlement-over-2014-breach-of-4.5m

Davis J. (2019), Massive SingHealth data breach caused by lack of basic security. Διαθέσιμο στην ιστοσελίδα: https://healthitsecurity.com/news/massive-singhealth-data-breach-caused-by-lack-of-basic-security

Davis J. (2019), Medical Informatics settles with state AGs for $900K over 2015 breach. Διαθέσιμο στην ιστοσελίδα: https://healthitsecurity.com/news/medical-informatics-settles-with-state-ags-for-900k-over-2015-breach

Davis J. (2019), UCLA Health reaches $7.5M Settlement Over 2015 breach of 4.5M. Διαθέσιμο στην ιστοσελίδα: https://healthitsecurity.com/news/ucla-health-reaches-7.5m-settlement-over-2015-breach-of-4.5m

Davis J. (2019), Vendor Compromises Data of 808,000 Singapore Blood Donors. Διαθέσιμο στην ιστοσελίδα: https://healthitsecurity.com/news/vendor-compromises-data-of-808000-singapore-blood-donors

Deah D. (2018), Orbitz says a possible data breach has affected 880,000 credit cards. Διαθέσιμο στην ιστοσελίδα: https://www.theverge.com/2018/3/20/17144482/orbitz-data-breach-credit-cards

Deah D. (2018), Panera Bread leaked customer data on its website for eight months. Διαθέσιμο στην ιστοσελίδα: https://www.theverge.com/2018/4/3/17192348/panera-bread-leaked-customer-data-breach-website

Deahl D. (2018), Ticketfly hack exposed the personal information of 27 million accounts. Διαθέσιμο στην ιστοσελίδα: https://www.theverge.com/2018/6/7/17438516/ticketfly-hack-personal-information-26-million-customers-leaked

Dellinger A.J. (2019), Quest Diagnostics hit with class action lawsuit over breach that exposed patient data. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/ajdellinger/2019/06/12/quest-dynamics-hit-with-class-action-lawsuit-over-breach-that-exposed-patient-data/

Dellinger A.J. (2019), Understanding the First American Financial data leak: how did it happen and what does it mean? Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/

Deng V. (2019), StockX offering free fraud and identify theft protection after hack. Διαθέσιμο στην ιστοσελίδα: https://www.complex.com/sneakers/2019/08/stockx-reportedly-hacked-over-6-million-users

DeNunzio D. (2014), AOL confirms email breach, tells users to change passwords. Διαθέσιμο στην ιστοσελίδα: https://www.cnet.com/news/aol-confirms-email-breach-tells-users-to-change-passwords/

Dickey M.R. (2016), FriendFinder Networks hack reportedly exposed over 412 million accounts. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2016/11/13/friendfinder-hack-412-million-accounts-breached/

Dickey M.R. (2018), Ride-hailing app Careem reveals data breach affecting 14 million people. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2018/04/23/careem-data-breach/

Digital Privacy Wise (2018), Typeform data breach. Διαθέσιμο στην ιστοσελίδα: https://medium.com/digitalprivacywise/typeform-data-breach-f066f7c930e8

Disterer G. (2013), 'ISO/IEC 27000, 27001 and 27002 for Information Security Management', Journal of Information Security, 2013, vol.4, pp. 92-100

Donohue B. (2014), What you need to know about the Community Health Systems breach. Διαθέσιμο στην ιστοσελίδα: https://www.kaspersky.com/blog/community_health_systems_breach/5765/

Ducklin P. (2016), *Data breach in China: 100 million records used to hack 20 million Taobao users*. Διαθέσιμο στην ιστοσελίδα: https://nakedsecurity.sophos.com/2016/02/05/data-breach-in-china-100-million-records-used-to-hack-20-million-taobao-users/

Dujmovic A. (2018), Possible data breach at Orbitz affects 880,000 payment cards. Διαθέσιμο στην ιστοσελίδα: https://www.cnet.com/news/possible-orbitz-data-security-breach-affects-880000-payment-cards/

Dunn J.E. (2018), Typeform data breach hits thousands of survey accounts. Διαθέσιμο στην ιστοσελίδα: https://nakedsecurity.sophos.com/2018/07/03/typeform-data-breach-hits-thousands-of-survey-accounts/

ENISA (2006), Risk Management: Implementation principles and inventories for risk management / Risk assessment methods and tools. Διαθέσιμο στην ιστοσελίδα: https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools

ENISA (2010), 'The new users' guide: How to raise information security awareness'

Equifax, Equifax data breach settlement. Διαθέσιμο στην ιστοσελίδα: https://www.equifaxbreachsettlement.com/

Escobar M.C. (2019), More Than 2M Customer Payment Cards Affected in Earl Enterprises 10-Month Long Data Breach. Διαθέσιμο στην ιστοσελίδα: https://hospitalitytech.com/more-2m-customer-payment-cards-affected-earl-enterprises-10-month-long-data-breach

ET Bureau (2019), Data breach at JustDial leaks 100 million user details. Διαθέσιμο στην ιστοσελίδα: https://economictimes.indiatimes.com/tech/internet/data-breach-at-justdial-leaks-100-million-user-details/articleshow/68930607.cms

Etherington D. (2017), Uber data breach from 2016 affected 57 million rides and drivers. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2017/11/21/uber-data-breach-from-2016-affected-57-million-riders-and-drivers/

European Commission, What is personal data? Διαθέσιμο στην ιστοσελίδα: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

European Commission, What is personal data? Διαθέσιμο στην ιστοσελίδα: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

Evans M, He Y, Maglaras L and Janicke H. (2018), 'HEART-IS: A novel technique for evaluating human error-related information security incidents', Computers & Security, vol.80, 2019, pp. 74-89

Evfimievski A, Gehrke J. and Srikant R. (2003), 'Limiting Privacy Breaches in Privacy Preserving Data Mining', PODS 2003, San Diego, CA

Farahmand F, Navathe S.B, Sharp G.P. and Enslow P.H. (2003), 'Managing Vulnerabilities of Information Systems to Security Incidents', ICEC '03: Proceedings of the 5th international conference on Electronic commerce, September 2003, pp. 348–354

Farahmand F, Navathe S.B, Sharp G.P. and Enslow P.H. (2003), 'Managing Vulnerabilities of Information Systems to Security Incidents', ICEC '03: Proceedings of the 5th international conference on Electronic commerce, September 2003, pp. 348–354

Fiegerman S. (2016), Yahoo says 500 million accounts stolen. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2016/09/22/technology/yahoo-data-breach/

Finkle, J. Reuters (2014), Crafts retailer Michaels investigating possible data breach involving credit cards. Διαθέσιμο στην ιστοσελίδα: https://www.businessinsider.com/michaels-data-breach-2014-1

Franceschi- Bicchierai L. (2016), Hacker tries to sell 427 million stolen MySpace passwords for $2.800. Διαθέσιμο στην ιστοσελίδα: https://www.vice.com/en_us/article/pgkk8v/427-million-myspace-passwords-emails-data-breach

Franceschi-Bicchierai L. (2015), Crowdfunding Site Patreon Gets Hacked. Διαθέσιμο στην ιστοσελίδα: https://www.vice.com/en_us/article/xywedn/crowdfunding-site-patreon-gets-hacked

Franceschi-Bicchierai L. (2016), A Teen Hacker Is Targeting Russian Sites as Revenge for the MH17 Crash. Διαθέσιμο στην ιστοσελίδα: https://www.vice.com/en_us/article/pgkp57/a-teen-hacker-is-targeting-russian-sites-as-revenge-for-the-mh17-crash

Franceschi-Bicchierai L. (2018), Hacker defaces Ticketfly's website, steals customer database. Διαθέσιμο στην ιστοσελίδα: https://www.vice.com/en_us/article/mbk3nx/ticketfly-website-database-hacked-data-breach

Franceschi-Bicchierai L. (2018), Hackers Stole Personal Data of 2 Million T-Mobile Customers. Διαθέσιμο στην ιστοσελίδα: https://www.vice.com/en_us/article/a3qpk5/t-mobile-hack-data-breach-api-customer-data

Franceshi L. (2015), Hacked toymaker VTech admits breach actually hit 6.3 million children. Διαθέσιμο στην ιστοσελίδα: https://www.vice.com/en_us/article/jpgx4p/hacked-toymaker-vtech-admits-breach-actually-hit-63-million-children

Frank B.H. (2015), Scottrade had no idea about data breach until the feds showed up. Διαθέσιμο στην ιστοσελίδα: https://www.pcworld.com/article/2988993/scottrade-had-no-idea-about-data-breach-until-the-feds-showed-up.html

Fruhlinger J. (2018), The OPM hack explained: Bad security practices meet China's Captain America. Διαθέσιμο στην ιστοσελίδα: https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Garcia A. (2019), Slack is resetting thousands of passwords after 2015 hack. Διαθέσιμο στην ιστοσελίδα: https://edition.cnn.com/2019/07/18/tech/slack-hack-reset-passwords-2015/index.html

Garrison C. and Ncube M. (2010) 'A longitudinal analysis of data breaches', Information Management & Computer Security Vol. 19 No. 4, 2011, pp. 216-230

Garrison C. and Ncube M. (2010) 'A longitudinal analysis of data breaches', Information Management & Computer Security Vol. 19 No. 4, 2011, pp. 216-230

Gartenberg C. (2018), T-Mobile was hit by a data breach affecting around 2 million customers. Διαθέσιμο στην ιστοσελίδα: https://www.theverge.com/2018/8/24/17776836/tmobile-hack-data-breach-personal-information-two-million-customers

Gartenberg C. (2018), Twitter advising all 330 million users to change passwords after bug exposed then in plain text. Διαθέσιμο στην ιστοσελίδα: https://www.theverge.com/2018/5/3/17316684/twitter-password-bug-security-flaw-exposed-change-now

Gary NG (2018), Bell Canada Hacked Again, New Data Breach Affects Up to 100,000 Customers. Διαθέσιμο στην ιστοσελίδα: https://www.iphoneincanada.ca/carriers/bell/bell-canada-hacked-data-breach-100-000/

GDPR (2016), General Data Protection Regulation. Διαθέσιμο στην ιστοσελίδα: https://gdpr.eu/

Geer D. (2019), Medical Informatics Engineering breach: the gift that keeps on giving. Διαθέσιμο στην ιστοσελίδα: https://medium.com/the-aftermath-of-a-data-breach/medical-informatics-engineering-breach-the-gift-that-keeps-on-giving-9948231d2e95

Gibbs S. (2014), The €30k data takeaway: Domino's Pizza faces ransom demand after hack. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/technology/2014/jun/16/dominos-pizza-ransom-hack-data

Gibbs S. (2015), Toy firm VTech hack exposes private data of parents and children. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/technology/2015/nov/30/vtech-toys-hack-private-data-parents-children

Gibbs S. (2016), Adult FriendFinder and Penthouse hacked in massive personal data breach. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/technology/2016/nov/14/adult-friend-finder-and-penthouse-hacked-in-largest-personal-data-breach-on-record

Gibbs S. (2018), Reddit user data compromised in sophisticated hack. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/technology/2018/aug/02/reddit-user-information-usernames-passwords-email-addresses-hack

Gibson K. (2018), T-Mobile breach may have impacted 2 million customers. Διαθέσιμο στην ιστοσελίδα: https://www.cbsnews.com/news/t-mobile-breach-may-have-impacted-2-million-customers/

Go anywhere (2018), Data Breach and Incident Response Plans : 2019 Templates & Best Practices. Διαθέσιμο στην ιστοσελίδα: https://www.goanywhere.com/blog/2018/12/27/data-breach-and-incident-response-plans-2019-templates-and-best-practices

Goh T. (2019), 800,000 blood donors' personal data accessed illegally and possibly stolen; police investigating. Διαθέσιμο στην ιστοσελίδα: https://www.straitstimes.com/singapore/health/800000-blood-donors-personal-data-accessed-illegally-and-possibly-stolen-police

Goldman J. (2015), CareFirst BlueCross BlueShield Data Breach Impacts 1.1 Million People. Διαθέσιμο στην ιστοσελίδα: https://www.esecurityplanet.com/network-security/carefirst-bluecross-blueshield-data-breach-impacts-1.1-million-people.html

Goldman J. (2015), Slack Hacked. Διαθέσιμο στην ιστοσελίδα: https://www.esecurityplanet.com/hackers/slack-hacked.html

Goldman J. (2016), 21st Century Oncology Notifies 2.2 Million Patients of Data Breach. Διαθέσιμο στην ιστοσελίδα: https://www.esecurityplanet.com/network-security/21st-century-oncology-notifies-2.2-million-patients-of-data-breach.html

Gordon K. (2014), eBay suffers massive security breach, all users must change their passwords. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/

Gorey C. (2018), Major US Postal Service data breach exposes 60M users. Διαθέσιμο στην ιστοσελίδα: https://www.siliconrepublic.com/enterprise/us-postal-service-data-breach

Goswami S. (2019), Researcher: data leaked for 300 million Truecaller users. Διαθέσιμο στην ιστοσελίδα: https://www.bankinfosecurity.asia/researcher-data-leaked-for-300-million-truecaller-users-a-12519

Goswami S. (2019), Researcher: JustDial leaks information on 100 million users. Διαθέσιμο στην ιστοσελίδα: https://www.bankinfosecurity.asia/researcher-justdial-leaks-information-on-100-million-users-a-12385

Grant K.B (2015), IRS: Breach affected 2x as many taxpayers as expected. Διαθέσιμο στην ιστοσελίδα: https://www.cnbc.com/2015/08/17/irs-breach-affected-2x-as-many-taxpayers-as-expected.html

Greenberg A. (2015), Hack brief: Hackers steal 15M T-Mobile Customers' data from Experian. Διαθέσιμο στην ιστοσελίδα: https://www.wired.com/2015/10/hack-brief-hackers-steal-15m-t-mobile-customers-data-experian/

Greenberg A. (2015), Hack brief: Health insurer Excellus says attackers breached 10M records. Διαθέσιμο στην ιστοσελίδα: https://www.wired.com/2015/09/hack-brief-health-insurance-firm-excellus-says-attackers-breached-10m-records/

Greenberg A. (2015), Slack Says It Was Hacked, Enables Two-Factor Authentication. Διαθέσιμο στην ιστοσελίδα: https://www.wired.com/2015/03/slack-admits-hacked-enables-2-factor-authentication/

Gressin S. (2016), 21st Century Oncology breach exposes patients' info. Διαθέσιμο στην ιστοσελίδα: https://www.consumer.ftc.gov/blog/2016/04/21st-century-oncology-breach-exposes-patients-info

Hackett R. (2015), Experian data breach affects 15 million people including T-Mobile customers. Διαθέσιμο στην ιστοσελίδα: https://fortune.com/2015/10/01/experian-data-breach-tmobile/

Hackett R. (2015), What to know about the Ashley Madison hack. Διαθέσιμο στην ιστοσελίδα: https://fortune.com/2015/08/26/ashley-madison-hack/

Hackett R. (2018), Expedia's Orbitz Says Data Breach Affected 880,000 Payment Cards. Διαθέσιμο στην ιστοσελίδα: https://fortune.com/2018/03/20/expedia-orbitz-data-breach-cards/

Hackett R. (2018), How Panera Bread fumbled its data leak – and what to learn from its mistake. Διαθέσιμο στην ιστοσελίδα: https://fortune.com/2018/04/04/panera-bread-data-leak-lessons/

Hall A. and Wright C. (2018) 'Data security: a review of major security breaches between 2014 and 2018', Federation of Business Disciplines Journal, vol. 6, 2018, pp.50-63

Hamidovic H. (2011), 'An Introduction to Information Security Incident Management Based on ISO/IEC TR 18044:2004', ISACA Journal vol.6, 2011, pp. 1-7

Harris E.A, Perlroth N. and Popper N. (2014), Neiman Marcus Data Breach Worse Than First Said. Διαθέσιμο στην ιστοσελίδα: https://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html

Harris E.A. (2014), Michaels stores' breach involved 3 million customers. Διαθέσιμο στην ιστοσελίδα: https://www.nytimes.com/2014/04/19/business/michaels-stores-confirms-breach-involving-three-million-customers.html

Hatmaker T. (2018), Healthcare data breach in Singapore affected 1.5M patients, targeted the prime minister. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2018/07/20/singapore-hack-health/

Hautala L. (2018), Smart toy maker VTech settles privacy changes with FTC. Διαθέσιμο στην ιστοσελίδα: https://www.cnet.com/news/vtech-ftc-children-privacy-settlement-hacker-data-breach/

Hautelook (2018):

Hayes C.M. (2019), 'Comparative analysis of data breach laws: Comprehension, Interpretation and External Sources of Legislative text, Lewis & Clark Law Review, Forthcoming, SSRN

Hayes C.M. (2019), 'Comparative analysis of data breach laws: Comprehension, Interpretation and External Sources of Legislative text, Lewis & Clark Law Review, Forthcoming, SSRN

Hern A. (2015), Ashley Madison hackers release vast database of 33m accounts. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/technology/2015/aug/19/ashley-madison-hackers-release-10gb-database-of-33m-infidelity-site-accounts

Hern A. (2016), Philippine electoral records breached in 'largest ever' government hack. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/technology/2016/apr/11/philippine-electoral-records-breached-government-hack

Hern A. (2016), Snapchat leaks employee pay data after CEO email scam. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/technology/2016/feb/29/snapchat-leaks-employee-data-ceo-scam-email

Hill K. (2014), Google says not to worry about 5 million 'Gmail passwords' leaked. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/kashmirhill/2014/09/11/google-says-not-to-worry-about-5-million-gmail-passwords-leaked/

HIPPA Journal (2015), UCLA Health system hacked: 4.5 million patient records exposed. Διαθέσιμο στην ιστοσελίδα: https://www.hipaajournal.com/ucla-health-system-hacked-4-5-million-patient-records-exposed-8033/

Home Depot (2014), The Home Depot reports finding in payment data breach investigation. Διαθέσιμο στην ιστοσελίδα: https://ir.homedepot.com/news-releases/2014/11-06-2014-014517315

Horton W. (2019), Cathay Pacific faulted for data breach, but hackers objective unclear. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/willhorton1/2019/06/06/cathay-pacific-faulted-for-data-breach-but-hackers-objective-unclear/

Humphreys E. (2011), 'Information security management system standards', Datenschutz and Datensicherheit, vol.1, pp. 7-11

Info Security (2014), Dominos Pizza Customers Exposed After Massive Data Breach. Διαθέσιμο στην ιστοσελίδα: https://www.infosecurity-magazine.com/news/dominos-pizza-customers-exposed/

IRS, Data Breach: Tax-Related Information for Taxpayers. Διαθέσιμο στην ιστοσελίδα: https://www.irs.gov/identity-theft-fraud-scams/data-breach-information-for-taxpayers

ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems

ISO27k Forum, ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements (second edition). Διαθέσιμο στην ιστοσελίδα: https://www.iso27001security.com/html/27001.html

ISO27k Forum, About the ISO27k standards. Διαθέσιμο στην ιστοσελίδα: https://www.iso27001security.com/html/iso27000.html

Ivanova I. (2019), Data for nearly 12 million Quest Diagnostics patients may have been exposed. Διαθέσιμο στην ιστοσελίδα: https://www.cbsnews.com/news/quest-diagnostics-data-breach-nearly-12-million-patients-had-personal-info-exposed/

Jackon E. (2017), Hacker steals data from up to 100,000 Bell Canada customers in second breach in eight months. Διαθέσιμο στην ιστοσελίδα: https://business.financialpost.com/telecom/hacker-steals-data-from-up-to-100000-bell-canada-customers-in-second-breach-in-eight-months

Jaeger L., (2018), 'Information Security Awareness: Literature Review and Integrative Framework', Hawaii: Proceedings of the 51st Hawaii International Conference on System Sciences, p. 4703-4712

Jayakumar A. (2014), Michaels says 3 million customers hit by data breach. Διαθέσιμο στην ιστοσελίδα: https://www.washingtonpost.com/business/economy/michaels-says-nearly-3-million-customers-hit-by-data-breach/2014/04/18/3074e432-c6fc-11e3-8b9a-8e0977a24aeb_story.html

JC Gotinga (2016), Comelec faces complaint over voters' data leak. Διαθέσιμο στην ιστοσελίδα: https://cnnphilippines.com/news/2016/06/17/Comelec-hack-data-breach.html

Karat J, Karat C.M, Brodie C. and Feng J. (2005), 'Privacy in information technology: Designing to enable privacy policy management in organizations', International journal of Human-Computer Studies 63 (2005), pp.153-174

Karyda M, Kiountouzis E. and Kokalakis S. (2004), 'Information systems security policies: a contextual perspective', Computers & Security (2005), pp.246-260

Karyda M. and Mitrou L. (2016), 'Data Breach Notification: Issues and challenges for security management', Association for Information Systems AIS Electronic Library (AISeL), Mediterranean Conference on Information Systems (MCIS), Paphos, Cyprus, September 2016

Kasperkevic J. (2015), IRS data breach would have been 'much more difficult' with security upgrades. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/world/2015/jun/02/irs-data-breach-senate-hearing-security-upgrades

Keane S. (2018), T-Mobile hack may have exposed data of 2 million customers. Διαθέσιμο στην ιστοσελίδα: https://www.cnet.com/news/t-mobile-hack-may-have-exposed-2-million-customers-data/

Kelion L. (2016), MySpace and Tumblr hit by 'mega breach'. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-36416855

Kerr D. and Mihalcik C. (2018), Uber to pay $148 million for failing to report 2016 hack. Διαθέσιμο στην ιστοσελίδα: https://www.cnet.com/news/uber-to-pay-148-million-for-failing-to-report-2016-hack/

Khaleel S. (2019), StockX data breach reportedly exposes millions of customers' data. Διαθέσιμο στην ιστοσελίδα: https://www.metrotimes.com/news-hits/archives/2019/08/05/stockx-data-breach-reportedly-exposes-millions-of-customers-data

Khalid A. (2019), Online sneaker reseller StockX faces lawsuit over data breach. Διαθέσιμο στην ιστοσελίδα: https://www.engadget.com/2019/08/21/stockx-faces-class-action-lawsuit/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJoRAs1h6bwVex1gGYNZparI0MAjnjleggVwWN_a7RocnHiEjSlLg67XOmV7juJv3KVDiT7mvMmcXAoSBGsU1s1zC15n8_TSlL1UKPE9gW9Y6emtbqpL6tPAfXnxAJlzcx1-1pFyLpeqa9UhGDt0-BNSy3Mn0tyE0W8UCG_b6uwg&guccounter=2

Kharpal A. (2018), Middle East Uber rival Careem says data of 14 million drivers and riders stolen in cyberattack. Διαθέσιμο στην ιστοσελίδα: https://www.cnbc.com/2018/04/23/careem-says-data-of-14-million-drivers-and-riders-stolen-in-cyberattack.html

Khondelwal S. (2018), US Postal Service left 60 million users data exposed for over a year. Διαθέσιμο στην ιστοσελίδα: https://thehackernews.com/2018/11/usps-data-breach.html

Khosrowshahi D. (2017), 2016 data security incident. Διαθέσιμο στην ιστοσελίδα: https://www.uber.com/newsroom/2016-data-incident/

King H. (2016), Snapchat employee fell for phishing scam. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2016/02/29/technology/snapchat-phishing-scam/index.html

Kirk J. (2015), Premera, Anthem data breaches linked by similar hacking tactics. Διαθέσιμο στην ιστοσελίδα: https://www.computerworld.com/article/2898419/premera-anthem-data-breaches-linked-by-similar-hacking-tactics.html

Kirk J. (2019), Report: SEC investigates First American data exposure. Διαθέσιμο στην ιστοσελίδα: https://www.bankinfosecurity.com/report-sec-investigates-first-american-data-exposure-a-12910

Kitten T. (2015), Michaels breach: how the Fraudsters pulled it off. Διαθέσιμο στην ιστοσελίδα: https://www.bankinfosecurity.com/michaels-breach-how-fraudsters-pulled-off-a-8696

Koerner B.I. (2016), Inside the cyberattack that shocked the US Government. Διαθέσιμο στην ιστοσελίδα: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

Kolbasuk McGee M (2015), Excellus BlueCross BlueShield hacked. Διαθέσιμο στην ιστοσελίδα: https://www.bankinfosecurity.com/excellus-bcbs-breach-affects-xxxxxxxx-a-8527

Kolbasuk McGee M. (2016), Cancer Center Chain: Hacker Attack Affects 2.2 Million. Διαθέσιμο στην ιστοσελίδα: https://www.careersinfosecurity.com/cancer-center-chain-hacker-attack-affects-22-million-a-8950

Kovacs E. (2018), Typeform data breach hits many organizations. Διαθέσιμο στην ιστοσελίδα: https://www.securityweek.com/typeform-data-breach-hits-many-organizations

Kovacs E. (2019), Slack Resetting More User Passwords in Response to 2015 Breach. Διαθέσιμο στην ιστοσελίδα: https://www.securityweek.com/slack-resetting-more-user-passwords-response-2015-breach

Kraus R. (2017), 1.7 million accounts hacked in 2014 Imgur data breach. Διαθέσιμο στην ιστοσελίδα: https://www.aol.com/article/finance/2017/11/27/17-million-accounts-hacked-in-2014-imgur-data-breach/23289417/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAA15ZAvsTgguFlNMMQIHN7sQ9Ygsx3t-JZ3KkaHwbF8fIfOR9Mvz4XpaxNf1WU6dtcPZyQvIYAPJb1HS3PI4oYxYNWZW7v3CbBG50ekZQzGLLUlcofATAtEnQqsoEHoEQZIKOmk5dFvyrDr2JieF1EoNWbtoo-LR3Eb093dkNkFr&guccounter=2

Kreb B. (2014), Banks: credit card breach at Home Depot. Διαθέσιμο στην ιστοσελίδα: https://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/

Kreb B. (2015), At Experian, security attrition amid acquisitions. Διαθέσιμο στην ιστοσελίδα: https://krebsonsecurity.com/tag/t-mobile-breach/

Kreb B. (2015), Online cheating site Ashley Madison hacked. Διαθέσιμο στην ιστοσελίδα: https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/

Kreb B. (2016), Congressional report slams OPM on data breach. Διαθέσιμο στην ιστοσελίδα: https://krebsonsecurity.com/tag/opm-breach/

Kreb B. (2019), First American Financial Corp. leaked hundreds of millions of title insurance records. Διαθέσιμο στην ιστοσελίδα: https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

Krebs B. (2014), 3 million customer credit, debit cards stolen in Michaels, Aaron Brothers breaches. Διαθέσιμο στην ιστοσελίδα: https://krebsonsecurity.com/2014/04/3-million-customer-credit-debit-cards-stolen-in-michaels-aaron-brothers-breaches/

Krebs B. (2015), Carefirst Blue Cross Breach Hits 1.1M. Διαθέσιμο στην ιστοσελίδα: https://krebsonsecurity.com/2015/05/carefirst-blue-cross-breach-hits-1-1m/

Krebs B. (2015), Premera BluCross breach exposes financial, medical records. Διαθέσιμο στην ιστοσελίδα: https://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/

Krebs B. (2015), Scottrade breach hits 4.6 million customers. Διαθέσιμο στην ιστοσελίδα: https://krebsonsecurity.com/2015/10/scottrade-breach-hits-4-6-million-customers/

Krebs B. (2018), Panerabread.com leaks millions of customer records. Διαθέσιμο στην ιστοσελίδα: https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/

Krebs B. (2018), USPS site exposed data on 60 million users. Διαθέσιμο στην ιστοσελίδα: https://krebsonsecurity.com/2018/11/usps-site-exposed-data-on-60-million-users/

Kumar M. (2017), Bell Canada Hacked: Data of 1.9 Million Customers Stolen. Διαθέσιμο στην ιστοσελίδα: https://thehackernews.com/2017/05/bell-telecom-hacked.html

Kumar M. (2017), Taringa: over 28 million users' data exposed in massive data breach. Διαθέσιμο στην ιστοσελίδα: https://thehackernews.com/2017/09/taringa-data-breach-hacking.html

Kumar M. (2019), Over 100 million JustDial users' personal data found exposed on the internet. Διαθέσιμο στην ιστοσελίδα: https://thehackernews.com/2019/04/justdial-hacked-data-breach.html

Kumparak G. (2015), Slack Got Hacked. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2015/03/27/slack-got-hacked/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=fTY4D0a9oxWFxQsyOxHekg

Lalan C. (2019), IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years. Διαθέσιμο στην ιστοσελίδα: https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

Lamkin P. (2018), Under Armour admits huge MyFitnessPal data hack. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/paullamkin/2018/03/30/under-armour-admits-huge-myfitnesspal-data-hack/

Langheinrich M. (2001) 'Privacy by Design- Principles of Privacy-Aware Ubiquitous Systems', International conference on Ubiquitous Computing, Distributed Systems Group, Institute of Information Systems, IFW, Switzerland:

Langheinrich M. (2001) 'Privacy by Design- Principles of Privacy-Aware Ubiquitous Systems', International conference on Ubiquitous Computing, Distributed Systems Group, Institute of Information Systems, IFW, Switzerland:

Larson S. (3017), Uber's massive hack: what we know. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2017/11/22/technology/uber-hack-consequences-cover-up/index.html

Lawyer Monthly (2019), Human error remains primary cause of personal data breaches. Διαθέσιμο στην ιστοσελίδα: https://www.lawyer-monthly.com/2019/10/human-error-remains-primary-cause-of-personal-data-breaches/ (30/9/19)

Lee D. (2017), Uber concealed huge data breach. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-42075306

Legere J. (2015), A letter from CEO John Legere on Experian data breach. Διαθέσιμο στην ιστοσελίδα: https://www.t-mobile.com/news/experian-data-breach

Leonhardt M. (2019), Equifax to pay $700 million for massive data breach. Here's what you need to know about getting a cut. Διαθέσιμο στην ιστοσελίδα: https://www.cnbc.com/2019/07/22/what-you-need-to-know-equifax-data-breach-700-million-settlement.html

Leventhal R. (2014), Community Health Systems reports data breach affecting 4.5M patients. Διαθέσιμο στην ιστοσελίδα: https://www.hcinnovationgroup.com/cybersecurity/privacy-security/news/13023790/community-health-systems-reports-data-breach-affecting-45m-patients

Lewis D. (2014), Domino's Pizza: Large breach with a side of ransom. Διαθέσιμο στην ιστοσελίδα: https://www.csoonline.com/article/2364323/domino-s-pizza-large-breach-with-a-side-of-ransom.html

Leyden J. (2017), Bazinga! Social network Taringa 'fesses up to data breach. Διαθέσιμο στην ιστοσελίδα: https://www.theregister.co.uk/2017/09/05/taringa_data_breach/

Liptak A. (2019), 2 million credit card numbers stolen from Earl Enterprise restaurants in 10-month breach. Διαθέσιμο στην ιστοσελίδα: https://www.theverge.com/2019/3/31/18289488/data-breach-planet-hollywood-buca-di-beppo-mixology-earl-enterprises-cybersecurity

Lobosco K. (2014), Michaels hack hit 3 million. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2014/04/17/news/companies/michaels-security-breach/

Locklear M. (2018), Orbitz data breach exposed 880,000 payment cards. Διαθέσιμο στην ιστοσελίδα: https://www.engadget.com/2018/03/20/orbitz-data-breach-exposed-880-000-payment-cards/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAG9yrXSgtdLtmCb8xif9rdmG5DOzbLqesAFcAllTI7RyxFGu97IzaMoursD8sroqQQkZ8Fvi6P26RV-IwWSKNBIYpyA4yoVU_GHLBWwgGWZ0OPRlpVF2HDI3Lr1mXeQqHhKLws2s7_OAwsn8gALABo_H2TCbww87fOH2SLKyd-Dg&_guc_consent_skip=1575026057

Lomas N. (2018), TimeHop discloses July 4 data breach affecting 21 million. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2018/07/09/timehop-discloses-july-4-data-breach-affecting-21-million/

Lord N. (2015), A timeline of the Ashley Madison hack. Διαθέσιμο στην ιστοσελίδα: https://digitalguardian.com/blog/timeline-ashley-madison-hack

Makena K. (2018), MyHeritage breach leaks millions of account details. Διαθέσιμο στην ιστοσελίδα: https://www.theverge.com/2018/6/5/17430146/dna-myheritage-ancestry-accounts-compromised-hack-breach

Mares O. (2019), Millions of users affected by data breach at Truecaller. Διαθέσιμο στην ιστοσελίδα: https://www.securitynewspaper.com/2019/05/27/millions-of-users-affected-by-data-breach-at-truecaller/

Marriot International (2018), Marriott announces starwood guest reservation database security incident. Διαθέσιμο στην ιστοσελίδα: https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident

Mathews L. (2017), Equifax data breach impacts 143 million Americans. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/

Mathews L. (2018), Hackers Swipe Data On 2 Million T-Mobile Subscribers. Διαθέσιμο στην ιστοσελίδα:https://www.forbes.com/sites/leemathews/2018/08/24/t-mobile-hackers-swipe-data-on-2-million-subscribers/

Mathews L. (2018), Office of Personnel Management still vulnerable 3 years after massive hack. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/leemathews/2018/11/15/office-of-personnel-management-still-vulnerable-3-years-after-massive-hack/

Mathews L. (2018), Uber's massive 2016 breach exposed data on more than 25 million Americans. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/leemathews/2018/04/12/ubers-massive-2016-breach-exposed-data-on-more-than-25-million-americans/

McCann E (2015), Excellus BlueCross BlueShield cyberattack impacts 10.5M people. Διαθέσιμο στην ιστοσελίδα: https://www.healthcareitnews.com/news/excellus-bluecross-blueshield-cyberattack-impacts-105m-people

McCoy K. (2016), Cyber hack got access to over 700,000 IRS accounts. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/money/2016/02/26/cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/

McGee M.K (2015), CareFirst BlueCross BlueShield Hacked. Διαθέσιμο στην ιστοσελίδα: https://www.databreachtoday.com/carefirst-bluecross-blueshield-hacked-a-8248

McGrath M. (2014), JP Morgan says 76 million households affected by data breach. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/maggiemcgrath/2014/10/02/jp-morgan-says-76-million-households-affected-by-data-breach/

McLean R. (2018), Quora says 100 million users hit by 'malicious' data breach. Διαθέσιμο στην ιστοσελίδα: https://edition.cnn.com/2018/12/03/tech/quora-hack-data-breach/index.html

McLean R. (2019), A hacker gained access to 100 million Capital One credit card applications and accounts. Διαθέσιμο στην ιστοσελίδα: https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html

McNeal G.S. (2015), Health insurer Anthem struck by massive data breach. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/gregorymcneal/2015/02/04/massive-data-breach-at-health-insurer-anthem-reveals-social-security-numbers-and-more/

Mihalcik C. (2019), Quest Diagnostics says data on nearly 12M patients exposed by breach. Διαθέσιμο στην ιστοσελίδα: https://www.cnet.com/news/quest-diagnostics-says-nearly-12m-patients-exposed-by-data-breach/

Mihalcik C. (2019), Slack is resetting passwords due to 2015 hack. Διαθέσιμο στην ιστοσελίδα: https://www.cnet.com/news/slack-is-resetting-passwords-due-to-2015-hack/

Mitrou L. and Karyda M. (2012), 'EU's Data Protection Reform and the Right to be Forgotten: A Legal Response to a Technological Challenge?', 5th International Conference of Information Law and Ethics 2012, Corfu-Greece

Mitrou L. and Karyda M. (2012), 'EU's Data Protection Reform and the Right to be Forgotten: A Legal Response to a Technological Challenge?', 5th International Conference of Information Law and Ethics 2012, Corfu-Greece

Mitrou L. and Moulinos K. (2003) 'Privacy and Data Protection in Electronic Communications', Computer Network Security, MMM-ACNS 2003, Lecture Notes in Computer Science, vol 2776. Springer, Berlin, Heidelberg

Mitrou L. and Moulinos K. (2003) 'Privacy and Data Protection in Electronic Communications', Computer Network Security, MMM-ACNS 2003, Lecture Notes in Computer Science, vol 2776. Springer, Berlin, Heidelberg

Molina B. (2015), VTEch data breach impacts 5 milion accounts. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/tech/2015/11/30/vtech-data-breach-impacts-5-million-accounts/76562538/

Monegain B. (2016), 21st Century Oncology probes massive data breach as it settles fraud case for $34.7 million. Διαθέσιμο στην ιστοσελίδα: https://www.healthcareitnews.com/news/21st-century-oncology-probes-massive-data-breach-it-settles-fraud-case-347-million

Moscaritolo A. (2016), MySpace breach reportedly affects 360M records. Διαθέσιμο στην ιστοσελίδα: https://www.pcmag.com/news/344876/myspace-breach-reportedly-affects-360m-records

Mullen J. (2018), Cathay Pacific got hacked, compromising the data of millions of passengers. Διαθέσιμο στην ιστοσελίδα: https://edition.cnn.com/2018/10/24/business/cathay-pacific-data-breach/index.html

Muncaster P. (2017), Bell Canada Breach Hits Nearly Two Million Customers. Διαθέσιμο στην ιστοσελίδα: https://www.infosecurity-magazine.com/news/bell-canada-breach-hits-two/

Mungin L. and Sutton J. (2014), Neiman Marcus investigates breach. Διαθέσιμο στην ιστοσελίδα: https://edition.cnn.com/2014/01/11/business/neiman-marcus-data-breach/index.html

Munro D. (2014), Cyber attack nets 4.5 Million records from large hospital system. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/danmunro/2014/08/18/cyber-attack-nets-4-5-million-records-from-large-hospital-system/

Musil S. (2016), Home Depot offers $19M to settle customers' hacking lawsuit. Διαθέσιμο στην ιστοσελίδα: https://www.cnet.com/news/home-depot-offers-19m-to-settle-customers-hacking-lawsuit/

MyHeritage Blog (2018), MyHeritage statement about a Cybersecurity incident. Διαθέσιμο στην ιστοσελίδα: https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/

Naidu-Ghelani R. (2018), Bell Canada alerts customers after data breach. Διαθέσιμο στην ιστοσελίδα: https://www.cbc.ca/news/business/bell-canada-data-breach-1.4500156

Nakashima E. (2015), Hacks of OPM databases compromised 22.1 million people, federal authorities say. Διαθέσιμο στην ιστοσελίδα: https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

Nasr R. (2015), Experian data breach hits more than 15M T-Moblie customers, applicants. Διαθέσιμο στην ιστοσελίδα: https://www.cnbc.com/2015/10/01/experian-reports-data-breach-involving-info-for-more-than-15m-t-mobile-customers.html

Newcomb A. (2018), Twitter scorned for password issue but praised for disclosing it. Διαθέσιμο στην ιστοσελίδα: https://www.nbcnews.com/tech/social-media/twitter-scorned-password-issue-praised-disclosing-it-n871516

Newcomb A. (2019), Hacked MyFitnessPal data goes on sale on the dark web – one year after the breach. Διαθέσιμο στην ιστοσελίδα: https://fortune.com/2019/02/14/hacked-myfitnesspal-data-sale-dark-web-one-year-breach/

Newman J. (2014), AOL traces mystery spam flood to security breach; passwords and more stolen. Διαθέσιμο στην ιστοσελίδα: https://www.pcworld.com/article/2148523/aol-traces-mystery-spam-to-security-breach.html

Newman L.H (2018), A New Google+ Blunder Exposed Data From 52.5 Million Users. Διαθέσιμο στην ιστοσελίδα: https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/

Nichols S. (2014), AOL confirms security breach from spam attack. Διαθέσιμο στην ιστοσελίδα: https://www.theregister.co.uk/2014/04/28/aol_confirms_security_breach_from_spam_attack/

NIST, Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication 800-53 Revision 4. Διαθέσιμο στην ιστοσελίδα: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NortonLifeLock employee, MyHeritage data breach exposes info of more than 92 million users. Διαθέσιμο στην ιστοσελίδα: https://us.norton.com/internetsecurity-emerging-threats-myheritage-data-breach-exposes-info-of-more-than-92-million-user.html

O' Flaherty K. (2019), Hackers have just put 620 million accounts up for sale on the dark web – Are you on the list? Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/kateoflahertyuk/2019/02/12/hackers-have-just-put-620-million-online-account-details-up-for-sale-is-yours-on-the-list/

O'Brien S.A. (2017), Giant Equifax data breach: 143 million people could be affected. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html

O'Flaherty K. (2018), Facebook data breach – what to do next. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/kateoflahertyuk/2018/09/29/facebook-data-breach-what-to-do-next/

O'Flaherty K. (2018), Google+ Security Bug - What Happened, Who Was Impacted And How To Delete Your Account. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/kateoflahertyuk/2018/10/09/google-plus-breach-what-happened-who-was-impacted-and-how-to-delete-your-account/

O'Kane J. (2017), Bell apologizes to customers after data breach hits 1.9 million e-mail addresses. Διαθέσιμο στην ιστοσελίδα: https://www.theglobeandmail.com/report-on-business/bell-apologizes-to-customers-after-data-breach-hits-19-million-e-mail-addresses/article35004027/

Ogden J. (2016), 7 Things to Know from Verizon's 2016 Data Breach Investigations Report. Διαθέσιμο στην ιστοσελίδα: https://www.cimcor.com/blog/7-things-to-know-from-verizons-2016-data-breach-investigations-report

Olano G. (2019), Data breach hits 800,000 Singaporean blood donors' personal data. Διαθέσιμο στην ιστοσελίδα: https://www.insurancebusinessmag.com/asia/news/breaking-news/data-breach-hits-800000-singaporean-blood-donors-personal-data-162635.aspx

Olenick D. (2018), Orbitz hit with data breach, info on 880,000 payment cards at risk. Διαθέσιμο στην ιστοσελίδα: https://www.scmagazine.com/home/security-news/data-breach/orbitz-hit-with-data-breach-info-on-880000-payment-cards-at-risk/

Opam K. (2015), Hackers dump data for 2.3 million Patreon users online. Διαθέσιμο στην ιστοσελίδα: https://www.theverge.com/2015/10/2/9439077/patreon-hack-user-database-2-million-users

OPM, Cybersecurity Resource Center. Διαθέσιμο στην ιστοσελίδα: https://www.opm.gov/cybersecurity/cybersecurity-incidents/

Osborne C. (2014), South Korean credit card firms suspended over data breach. Διαθέσιμο στην ιστοσελίδα: https://www.zdnet.com/article/south-korean-credit-card-firms-suspended-over-data-breach/

Osborne C. (2019), Massive Quest Diagnostics data breach impacts 12 million patients. Διαθέσιμο στην ιστοσελίδα: https://www.zdnet.com/article/massive-quest-diagnostics-data-breach-impacts-12-million-patients/

Padwal K, Thomas A, Howard T. and Carr M. (2019) 'Common Lessons from disparate Information Security Incidents', A White Paper Analysis, (ISC) National Capital Region Chapter

Padwal K, Thomas A, Howard T. and Carr M. (2019) 'Common Lessons from disparate Information Security Incidents', A White Paper Analysis, (ISC) National Capital Region Chapter

Paganini P. (2019), Secur Solutions Group data leak exposes 800,000 Singapore blood donors. Διαθέσιμο στην ιστοσελίδα: https://securityaffairs.co/wordpress/82452/data-breach/secur-solutions-group-data-leak.html

Pagliery J. (2014), 5 million Gmail passwords leaked. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2014/09/10/technology/security/gmail-hack/index.html

Pagliery J. (2014), Hospital network hacked, 4.5 million records stolen. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2014/08/18/technology/security/hospital-chs-hack/index.html

Pagliery J. (2014), This is how your Gmail account got hacked. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2014/11/07/technology/security/gmail-account-stolen/index.html

Pagliery J. (2015), Scottrade hacked, customer data stolen. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2015/10/02/technology/scottrrade-hack/

Pagliery J. (2015), T-Mobile customers' info breached after Experian hack. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2015/10/01/technology/tmobile-experian-data-breach/

Pagliery J. (2015), UCLA Health hacked, 4.5 million victims. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2015/07/17/technology/ucla-health-hack/

Patreon (2015), Patreon had a security breach; here's what you need to know. Διαθέσιμο στην ιστοσελίδα: https://www.patreon.com/posts/patreon-had-what-3520192

Perez S. (2016), Recently confirmed MySpace hack could be the largest yet. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2016/05/31/recently-confirmed-myspace-hack-could-be-the-largest-yet/

Perez S. and Whittake Z. (2018), Everything you need to know about Facebook's data breach affecting 50M users. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/

Perlroth N. (2014), Michaels stores is investigating data breach. Διαθέσιμο στην ιστοσελίδα: https://www.nytimes.com/2014/01/26/technology/michaels-stores-is-investigating-data-breach.html

Pike S. (2016), Huge Tumbler and MySpace (yes, MySpace!) data breaches. Διαθέσιμο στην ιστοσελίδα: https://www.kaspersky.com/blog/myspace-tumbler-data-breach/12252/

Pramuk J. (2015), Scottrade data breach affects up to 4M customers. Διαθέσιμο στην ιστοσελίδα: https://www.cnbc.com/2015/10/02/scottrade-data-breach-affects-up-to-4m-customers.html

Price R. (2015), After the Hacking of Crowdfunding site Patreon, its users are now being blackmailed. Διαθέσιμος στην ιστοσελίδα: https://www.inc.com/business-insider/crowdfunding-site-patreon-hacked-users-blackmailed.html

Price R. (2015), Crowdfunding site Patreon has been hacked and a huge amount of data has been leaked online. Διαθέσιμο στην ιστοσελίδα: https://www.businessinsider.com/crowdfunding-site-patreon-hacked-user-data-leaked-online-2015-10

Quackenbush C. (2018), Cathay Pacific says data breach exposed personal information of 9.4 million passengers. Διαθέσιμο στην ιστοσελίδα: https://time.com/5434171/cathay-pacific-data-breach/

Quest Diagnostics (2019), Unauthorized Access to Database at AMCA containing personal information. Διαθέσιμο στην ιστοσελίδα: https://www.questdiagnostics.com/home/AMCA-data-breach-patients/

Rappler.com (2016), Comelec data leaked by hackers. Διαθέσιμο στην ιστοσελίδα: https://www.rappler.com/nation/politics/elections/2016/127315-comelec-data-hackers

Reading S. (2019), Earl Enterprises Restaurants Hit by Payment Card Data Breach. Διαθέσιμο στην ιστοσελίδα: https://securereading.com/earl-enterprises-restaurants-hit-by-payment-card-data-breach/

Regan S. (2014), Heartbleed to blame for Community Health Systems breach. Διαθέσιμο στην ιστοσελίδα: https://www.csoonline.com/article/2466726/data-protection-heartbleed-to-blame-for-community-health-systems-breach.html

Reuters (2014), Hackers steal Dominos Pizza customer data in Europe, ransom sought. Διαθέσιμο στην ιστοσελίδα: https://www.cnbc.com/2014/06/16/hackers-steal-dominos-pizza-customer-data-in-europe-ransom-sought.html

Reuters (2015), CareFirst says cyberattack stole data of 1.1 million users in U.S. Διαθέσιμο στην ιστοσελίδα: https://www.reuters.com/article/us-carefirst-cyberattack/carefirst-says-cyberattack-stole-data-of-1-1-million-users-in-u-s-idUSKBN0O52IF20150520

Reuters (2015), Premera BlueCross says data breach exposed medical data. Διαθέσιμο στην ιστοσελίδα: https://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html

Reuters (2015), VTech hack: Data of 6.4M kids exposed. Διαθέσιμο στην ιστοσελίδα: https://www.cnbc.com/2015/12/02/vtech-hack-data-of-64m-kids-exposed.html

Reuters (2016), *Hackers attack 20 mln accounts on Alibaba's Taobao shopping site*. Διαθέσιμο στην ιστοσελίδα: https://www.reuters.com/article/alibaba-cyber/hackers-attack-20-mln-accounts-on-alibabas-taobao-shopping-site-idUSL3N15J1P2

Reuters (2016), *Hackers in China attack 20M accounts on Alibaba's Taobao shopping site.* Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/business/2016/feb/04/hackers-in-china-attack-20m-accounts-on-alibaba-taobao-shopping-site

Reuters (2017), Anthem to pay record $115M to settle lawsuits over data breach. Διαθέσιμο στην ιστοσελίδα: https://www.nbcnews.com/news/us-news/anthem-pay-record-115m-settle-lawsuits-over-data-breach-n776246

Reuters (2018), Cathay Pacific revealed a major data breach affecting 9.4 million passengers that leaked passport numbers, credit card numbers and email address. Διαθέσιμο στην ιστοσελίδα: https://www.businessinsider.com/r-cathay-pacific-flags-data-breach-affecting-94-million-passengers-2018-10

Reuters (2018), Panera Bread's website hit by data breach. Διαθέσιμο στην ιστοσελίδα: https://nypost.com/2018/04/03/panera-breads-website-hit-by-data-breach/

Reuters (2019), Quest Diagnostics says data breach could have hit nearly 12 million patients. Διαθέσιμο στην ιστοσελίδα: https://nypost.com/2019/06/04/quest-diagnostics-says-data-breach-could-have-hit-nearly-12-million-patients/

Riley C. (2015), Insurance giant Anthem hit by massive data breach. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/

Risen T. (2015), VTech hack shows kids at risk with WiFi toys. Διαθέσιμο στην ιστοσελίδα: https://www.usnews.com/news/articles/2015/12/01/vtech-hack-shows-kids-at-risk-with-wifi-toys

Roberts J.J. (2017), Home Depot to pay banks $25 million in data breach settlement. Διαθέσιμο στην ιστοσελίδα: https://fortune.com/2017/03/09/home-depot-data-breach-banks/

Roberts P. (2015), Doctors still in the dark after electronics records hack exposes data on 4 million. Διαθέσιμο στην ιστοσελίδα: https://securityledger.com/2015/07/doctors-still-in-the-dark-after-electronics-records-hack-exposes-data-on-4-million/

Rodriguez M. (2018), Reddit suffers 'serious' security breach. Διαθέσιμο στην ιστοσελίδα: https://fortune.com/2018/08/01/reddit-security-breach/

Roman J. (2014), AOL investigating data breach. Διαθέσιμο στην ιστοσελίδα: https://www.inforisktoday.com/aol-investigating-data-breach-a-6797

Roman J. (2014), Michaels confirms data breach. Διαθέσιμο στην ιστοσελίδα: https://www.bankinfosecurity.com/michaels-a-6763

Romanosky S, Telang R. and Acquisti A. (2011) 'Do Data Breach Disclosure Laws Reduce Identity Theft?', Journal of Policy Analysis and Management, Vol. 30, No. 2, pp. 256–286

Romanosky S, Telang R. and Acquisti A. (2011) 'Do Data Breach Disclosure Laws Reduce Identity Theft?', Journal of Policy Analysis and Management, Vol. 30, No. 2, pp. 256–286

Rowan L. (2019), StockX reveals details about data breach. Διαθέσιμο στην ιστοσελίδα: https://www.retaildive.com/news/stockx-reveals-details-about-data-breach/560896/

Rowland C. (2019), Quest Diagnostics discloses breach of patient records. Διαθέσιμο στην ιστοσελίδα: https://www.washingtonpost.com/business/economy/quest-diagnostics-discloses-breach-of-patient-records/2019/06/03/aa37b556-860a-11e9-a870-b9c411dc4312_story.html

Rushe D. (2014), JP Morgan Chase reveals massive data breach affecting 76M households. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach

Rushe D. (2015), OPM hack: China blamed for massive breach of US government data. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances

Russell J. (2016), Snapchat employee data leaks out following phishing attack. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2016/02/29/snapchat-employee-data-leaks-out-following-phishing-attack/

Santillan M. (2016), Weebly to notify 43 million customers of data breach. Διαθέσιμο στην ιστοσελίδα: https://www.tripwire.com/state-of-security/latest-security-news/weebly-notify-43-million-customers-data-breach/

Schuman E. (2017), Neiman Marcus data breach settlement tells us plenty about the ROI of security. Διαθέσιμο στην ιστοσελίδα: https://www.computerworld.com/article/3186285/neiman-marcus-data-breach-settlement-tells-us-plenty-about-the-roi-of-security.html

Schwartz M.J (2016), A Look at Breach Notification Laws Around the World. Διαθέσιμο στην ιστοσελίδα: https://www.databreachtoday.eu/blogs/look-at-breach-notification-laws-around-world-p-2140

Sciutto J. (2015), OPM government data breach impacted 21.5 million. Διαθέσιμο στην ιστοσελίδα: https://edition.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/index.html

Seals T. (2016), 21st Century Oncology Breach: A Sign of Things to Come. Διαθέσιμο στην ιστοσελίδα: https://www.infosecurity-magazine.com/news/21st-century-oncology-a-sign-of/

Security Magazine (2019), Desjardins group to offer data protection to customers affected by breach. Διαθέσιμο στην ιστοσελίδα: https://www.securitymagazine.com/articles/90557-desjardins-group-to-offer-data-protection-to-customers-affected-by-breach

Sen R. and Borle S. (2015) 'Estimating the Contextual Risk of Data Breach: An Empirical Approach', Journal of Management Information Systems 2015, Vol. 32, No. 2, pp. 314–341.

Shaikh R. (2016), More mega breaches! Weebly confirms hack affecting 43 million users – Foursquare also exposed. Διαθέσιμο στην ιστοσελίδα: https://wccftech.com/weebly-foursquare-data-breaches/

Sheldon E. (2019), What is a data breach, how does one happen and what should you do next? Διαθέσιμο στην ιστοσελίδα: https://www.british-assessment.co.uk/insights/what-is-data-breach-how-does-one-happen-and-what-should-you-do-next/

Sherstobitoff R. (2008) 'Anatomy of a Data Breach', Information Security Journal: A Global Perspective, USA, pp. 247-252

Shingler B. (2019), What you need to know about the Desjardins data breach. Διαθέσιμο στην ιστοσελίδα: https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-explain-1.5185163

Siew A. (2019), HSA blood donor data leak: When 'sorry' may not be enough. Διαθέσιμο στην ιστοσελίδα: https://www.todayonline.com/commentary/hsa-blood-donor-data-leak-when-sorry-may-not-be-enough

Silversmith W. (2016), Security: data breach & old password expiration. Διαθέσιμο στην ιστοσελίδα: https://blog.eyewire.org/security-data-breach-partial-password-expiration-2016-02-23/

Simon M. (2018), After another massive Google+ data breach, you should probably delete your profile right now. Διαθέσιμο στην ιστοσελίδα: https://www.pcworld.com/article/3326821/google-plus-data-breach-delete-profile.html

Simon M. (2018), T-Mobile data breach FAQ: What happened, how it affects you, and what you should do now. Διαθέσιμο στην ιστοσελίδα: https://www.pcworld.com/article/3300160/t-mobile-data-hack-faq.html

SingHealth, Cyberattack on SingHealth IT system – information for SingHealth patients. Διαθέσιμο στην ιστοσελίδα: https://www.singhealth.com.sg/about-singhealth/data-security-check

Smith B. (2014), 'Information Security Incident Management', Information Security Fundamentals, 2nd edition, CRC Press, pp.257-280

Smith J.F (2015), Cyberattack Exposes I.R.S. Tax Returns. Διαθέσιμο στην ιστοσελίδα: https://www.nytimes.com/2015/05/27/business/breach-exposes-irs-tax-returns.html

Snell E. (2015), Excellus BCBS data breach affects 7M individuals. Διαθέσιμο στην ιστοσελίδα: https://healthitsecurity.com/news/excellus-bcbs-data-breach-affects-7m-individuals

Snell E. (2015), PHI exposed in Medical Informatics Engineering data breach. Διαθέσιμο στην ιστοσελίδα: https://healthitsecurity.com/news/phi-exposed-in-medical-informatics-engineering-data-breach

Snider M. (2018), Q&A site Quora says data breach may affect 100 million users. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/tech/news/2018/12/04/quora-says-data-breach-may-affect-100-million-its-q-site/2200175002/

Soergel A. (2014), 53 million email addresses stolen in Home Depot hack. Διαθέσιμο στην ιστοσελίδα: https://www.usnews.com/news/newsgram/articles/2014/11/07/53-million-customer-email-addresses-leaked-in-home-depot-hack

Solomon H. (2018), Bell acknowledges data breach. Διαθέσιμο στην ιστοσελίδα: https://www.itworldcanada.com/article/bell-acknowledges-data-breach/401010

Sosa K. (2018), We had a security incident. Here's what you need to know. Διαθέσιμο στην ιστοσελίδα: https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/

Spadafora A. (2019), Data leak reveals how Russia uses telecoms for surveillance. Διαθέσιμο στην ιστοσελίδα: https://www.techradar.com/news/data-leak-reveals-how-russia-uses-telecoms-for-surveillance

Spiekermann S, Acquisti A, Böhme R. and Hui K. (2015) 'The challenges of personal data markets and privacy', Springer, Electron Markets (2015), pp.161–167

Spring T. (2016), Home Depot agrees to $19.5 million settlement to end 2014 breach nightmare. Διαθέσιμο στην ιστοσελίδα: https://threatpost.com/home-depot-agrees-to-19-5-million-settlement-to-end-2014-breach-nightmare/116884/

Spring T. (2018), Under Armour reports massive breach of 150 million MyFitnessPal accounts. Διαθέσιμο στην ιστοσελίδα: https://threatpost.com/under-armour-reports-massive-breach-of-150-million-myfitnesspal-accounts/130863/

SrockX (2019), Update on data security issue. Διαθέσιμο στην ιστοσελίδα: https://stockx.com/news/update-on-data-security-issue/

Stanley J. (2019), StockX faces class action lawsuit after data breach left users' information exposed. Διαθέσιμο στην ιστοσελίδα: https://hypebeast.com/2019/8/stockx-password-reset-suspicious-activity

Statt N. (2018), Google hid major Google+ security flaw that exposed users' personal information. Διαθέσιμο στην ιστοσελίδα: https://www.theverge.com/2018/10/8/17951914/google-plus-data-breach-exposed-user-profile-information-privacy-not-disclosed

Sweney M. (2019), Marriot to be fined nearly £100M over GDPR breach. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/business/2019/jul/09/marriott-fined-over-gdpr-breach-ico

Szoldra P. (2014), Hackers Possibly Stole Credit Card Data From Neiman Marcus. Διαθέσιμο στην ιστοσελίδα: https://www.businessinsider.com/neiman-marcus-data-breach-2014-1

Taylor K. (2018), Panera reportedly ignored a breach that exposed thousands of customers' information for 8 months. Διαθέσιμο στην ιστοσελίδα: https://www.businessinsider.com/panera-data-breach-reportedly-remained-unsolved-for-months-2018-4

Temperton J. (2016), The Philippines election hack is 'freaking huge'. Διαθέσιμο στην ιστοσελίδα: https://www.wired.co.uk/article/philippines-data-breach-fingerprint-data

Terhune C. (2015), UCLA Health system data breach affects 4.5 million patients. Διαθέσιμο στην ιστοσελίδα: https://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html

TF Attendee Support (2018), Ticketfly cyber incident information. Διαθέσιμο στην ιστοσελίδα: https://support.ticketfly.com/s/article/41507

The Ganadian Press (2017), Bell Canada says customer information compromised in hack. Διαθέσιμο στην ιστοσελίδα: https://globalnews.ca/news/3453577/bell-canada-says-customer-information-compromised-in-hack/

Thielman S. (2015), Experian hack exposes 15 million people's personal information. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/business/2015/oct/01/experian-hack-t-mobile-credit-checks-personal-information

Thielman S. (2016), Yahoo hack: 1bn accounts compromised by biggest data breach in history. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached

Thomsen S. (2015), Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online. Διαθέσιμο στην ιστοσελίδα: https://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7

TimeHop (2018), TimeHop security incident, July 4th, 2018. Διαθέσιμο στην ιστοσελίδα: https://www.timehop.com/security

Tobin B. (2018), Google to shut down Google+ early due to bug that leaked data of 52.5 million users. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/tech/2018/12/11/google-plus-leak-social-network-shut-down-sooner-after-security-bug/2274296002/

Tomesco F. (2019), Desjardins: Rogue employee caused data breach for 2.9 million members. Διαθέσιμο στην ιστοσελίδα: https://montrealgazette.com/business/desjardins-rogue-employee-caused-data-breach-for-2-9-million-members

Topa I. and Karyda M. (2018), 'From theory to practice: guidelines for enhancing information security management', Information & Computer Security, vol. 27, no. 3, 2019, pp. 326-342

Truong A. (2015), Hackers breached Slack's database containing users' contact information and passwords. Διαθέσιμο στην ιστοσελίδα: https://qz.com/371676/hackers-breached-slacks-database-containing-users-contact-information-and-passwords/

Tsohou A, Karyda M, Kokalakis S. and Kiountouzis E. (2010), 'Aligning Security Awareness with Information System Security Management', ReachGate 2010

Tsohou A., Kokolakis S., Karyda M. and Kiountouzis E. (2008), 'Investing Information Security Awareness: Research and Practice Gaps', Greece: Information Security Journal A Global Perspective, December 2008

UpGuard (2019), Telecommunications breakdown: how Russian telco infrastructure was exposed. Διαθέσιμο στην ιστοσελίδα: https://www.upguard.com/breaches/mts-nokia-telecom-inventory-data-exposure

USA TODAY (2015), Cyber breach hits 10 million Excellus healthcare customers. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-blue-shield/72018150/

Utermohlen K. (2019), Facebook data breach 2019: 540 million user's records exposed. Διαθέσιμο στην ιστοσελίδα: https://finance.yahoo.com/news/facebook-data-breach-2019-540-202405997.html?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJt6eLd4y9tTRZYX7xy8XuTZeZyoa0Hj4t12dqLkvQQHKH7oXEu0IVgXSLj59Ck928MNIoffHgdHxFzz6UHlsHlTeB6zAJtv5mMlR3geSoKHo99evjq9_zoiKtK1okxJNiejYQDOKPgvcWD9q2SnFta39SiH9WYZP-HVnkcIckIn&guccounter=2

Uzair A. (2019), Slack data breach: Company resets thousands of passwords. Διαθέσιμο στην ιστοσελίδα: https://www.hackread.com/slack-data-breach-company-resets-thousands-of-passwords/

Vaas L. (2019), Desjardins' employee from hell spills 2.9m records. Διαθέσιμο στην ιστοσελίδα: https://nakedsecurity.sophos.com/2019/06/24/desjardins-employee-from-hell-spills-2-9m-records/

Valinsky J. (2019), Quest Diagnostics says 12 million patients may have had their personal information exposed. Διαθέσιμο στην ιστοσελίδα: https://edition.cnn.com/2019/06/03/business/quest-diagnostics-breach/index.html

Victor D. (2015), Security breach at Toy maker VTech includes data on children. Διαθέσιμο στην ιστοσελίδα: https://www.nytimes.com/2015/12/01/business/security-breach-at-toy-maker-vtech-includes-data-on-children.html

Vinton K. (2014), With 56 million cards compromised, Home Depot's breach is bigger that Target's. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/katevinton/2014/09/18/with-56-million-cards-compromised-home-depots-breach-is-bigger-than-targets/

Vinton K. (2015), Data Belonging To 1.1 Million CareFirst Customers Stolen In Cyber Attack. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/katevinton/2015/05/20/data-belonging-to-1-1-million-carefirst-customers-stolen-in-cyber-attack/

Vinton K. (2015), Premera BlueCross breach may have exposed 11 million customers' medical and financial data. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach/

Volodzko D. (2018), Marriott breach exposes far more than just data. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/davidvolodzko/2018/12/04/marriott-breach-exposes-far-more-than-just-data/

Volz D. (2016), Yahoo says hackers stole data from 500 million accounts in 2014. Διαθέσιμο στην ιστοσελίδα: https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-hackers-stole-data-from-500-million-accounts-in-2014-idUSKCN11S16P

Voss W.G (2017), 'European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting', Business Lawyer, Vol. 72, No. 1, pp. 221-233

VTech press release (2015), Data breach on VTech learning lodge. Διαθέσιμο στην ιστοσελίδα: https://www.vtech.com/en/press_release/2015/statement/

Wagenseil P. (2018), 27 million Ticketfly accounts hacked: what you should do. Διαθέσιμο στην ιστοσελίδα: https://www.tomsguide.com/us/ticketfly-data-breach,news-27374.html

Wagenseil P. (2019), 139 million user hit in Canva data breach. Διαθέσιμο στην ιστοσελίδα: https://www.tomsguide.com/us/canva-data-breach,news-30165.html

Wakabayashi D. (2018), Google Plus Will Be Shut Down After User Information Was Exposed. Διαθέσιμο στην ιστοσελίδα: https://www.nytimes.com/2018/10/08/technology/google-plus-security-disclosure.html

Wakefield J. (2014), eBay faces investigations over massive data breach. Διαθέσιμο στην ιστοσελίδα: https://www.bbc.com/news/technology-27539799

Warwick A. (2015), US health insurer Excellus BlueCross BlueShield hit by data breach. Διαθέσιμο στην ιστοσελίδα: https://www.computerweekly.com/news/4500253229/US-health-insurer-Excellus-BlueCross-BlueShield-hit-by-data-breach

Waugh R. (2014), 'Milions' of users at risk after AOL email breach. Διαθέσιμο στην ιστοσελίδα: https://www.welivesecurity.com/2014/05/01/millions-of-users-at-risk-aol-email-breach/

Weber J. (2019), More than 12M people may be affected by latest medical data breach. Why those patients are now vulnerable. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/news/nation/2019/06/06/quest-diagnostics-data-breach-leaves-patients-vulnerable-fraud/1356069001/

Weise E. (2014), JP Morgan reveals data breach affected 76 million households. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/tech/2014/10/02/jp-morgan-security-breach/16590689/

Weise E. (2015), 4.6mln Scottrade clients possibly exposed in hack. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/tech/2015/10/02/scottrade-broker-hacker-breach-46-million/73233356/

Weise E. (2015), Hack at UCLA Health could involve 4.5M people. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/tech/2015/07/17/ucla-health-hack-45-million-patients-medical/30304977/

Weise E. (2016), 360 million MySpace accounts breached. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/tech/2016/05/31/360-million-myspace-accounts-breached/85183200/

Weise E. (2016), 412 million FriendFinder hook-up accounts possibly hacked. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/tech/news/2016/11/14/412-million-adult-meeting-accounts-possibly-hacked/93818404/

Weise E. (2018), Orbitz breach: Expedia says 800,000 Orbitz.com customers may have been breached. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/tech/2018/03/20/800-000-orbitz-cards-compromised-breached/442277002/

Whittaker Z. (2016), Adult FriendFinder Network hack exposes 412 million accounts. Διαθέσιμο στην ιστοσελίδα: https://www.zdnet.com/article/adultfriendfinder-network-hack-exposes-secrets-of-412-million-users/

Whittaker Z. (2016), Weebly confirms hack; millions of Foursquare accounts also exposed. Διαθέσιμο στην ιστοσελίδα: https://www.zdnet.com/article/millions-of-accounts-stolen-in-weebly-foursquare-breaches/

Whittaker Z. (2019), A huge database of Facebook user's phone numbers found online. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/

Whittaker Z. (2019), Capital One replaces security chief after data breach. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2019/11/07/capital-one-security-chief-shuffle/

Whittaker Z. (2019), Documents reveal how Russia taps phone companies for surveillance. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/

Whittaker Z. (2019), Quest Diagnostics says 11.9 million patients affected by data breach. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2019/06/03/quest-diagnostics-breach/

Whittaker Z. (2019), StockX was hacked, exposing millions of customers' data. Διαθέσιμο στην ιστοσελίδα: https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/?guccounter=2

Wiliams K.B (2015), CareFirst BlueCross BlueShield breach impacts 1.1M. Διαθέσιμο στην ιστοσελίδα: https://www.healthcaredive.com/news/carefirst-bluecross-blueshield-breach-impacts-11m/399558/

Williams C. (2019), 620 million accounts stolen from 36 hacked websites now for sale in dark web, seller boasts. Διαθέσιμο στην ιστοσελίδα: https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/

Wilson M. and Hash J. (2003, October), 'Building an Information Technology Security Awareness and Training Program', Computer Security Division Information Technology Laboratory , National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8933

Winder D. (2018), Quora hacked: what happened, what data was stolen and what do 100 millions users need to do next? Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/daveywinder/2018/12/04/quora-hacked-what-happened-what-data-was-stolen-and-what-do-100-million-users-need-to-do-next/

Winder D. (2019), Slack Hack Prompts 100,000 Account Password Reset. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/daveywinder/2019/07/19/slack-hack-prompts-100000-account-password-reset/

Winder D. (2019), Unsecured Facebook databases leak data of 419 million users. Διαθέσιμο στην ιστοσελίδα: https://www.forbes.com/sites/daveywinder/2019/09/05/facebook-security-snafu-exposes-419-million-user-phone-numbers/

Winter M. (2014), Home Depot hackers used vendor log-on to steal data, e-mails. Διαθέσιμο στην ιστοσελίδα: https://eu.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/

Wong J.C and Solon O. (2018), Google to shut down Google+ after failing to disclose user data leak. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/technology/2018/oct/08/google-plus-security-breach-wall-street-journal

Wong J.C. (2017), Uber concealed massive hack that exposed data of 57M users and drivers. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

Wong J.C. (2018), Facebook says nearly 50M users compromised in huge security breach. Διαθέσιμο στην ιστοσελίδα: https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach

Writer S. (2018), Dubai's Careem reports data breach affecting millions of customers. Διαθέσιμο στην ιστοσελίδα: https://gulfbusiness.com/dubais-careem-reports-data-breach-affecting-millions-customers/

Yan S. and Kwon K.J (2014), Massinve data theft hits 40% of South Koreans. Διαθέσιμο στην ιστοσελίδα: https://money.cnn.com/2014/01/21/technology/korea-data-hack/index.html

Yu E. (2018), SingHealth data breach reveals several 'inadequate' security measures. Διαθέσιμο στην ιστοσελίδα: https://www.zdnet.com/article/singhealth-data-breach-reveals-several-inadequate-security-measures/

Zach Miners Z. (2015), Slack hacked, compromising users' profile data. Διαθέσιμο στην ιστοσελίδα: https://www.pcworld.com/article/2903272/slack-hacked-compromising-users-profile-data.html

Zetter K. (2015), Hackers finally post stolen Ashley Madison data. Διαθέσιμο στην ιστοσελίδα: https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/

Zetter K. (2015), Scottrade alerts 4.6 million brokerage customers of breach. Διαθέσιμο στην ιστοσελίδα: https://www.wired.com/2015/10/scottrade-alerts-4-6-million-brokerage-customers-breach/

Zhong R. (2018), Cathay Pacific data breach exposes 9.4 million passengers. Διαθέσιμο στην ιστοσελίδα: https://www.nytimes.com/2018/10/25/business/cathay-pacific-hack.html

Zorabedian J. (2014), AOL mail accounts breached, users advised to change passwords. Διαθέσιμο στην ιστοσελίδα: https://nakedsecurity.sophos.com/2014/04/29/aol-mail-accounts-breached-users-advised-to-change-passwords/

Zurkus K. (2019), Slack Resets 1% of Passwords After 2015 Data Breach. Διαθέσιμο στην ιστοσελίδα: https://www.infosecurity-magazine.com/news/slack-resets-1-of-passwords-after/

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2016), Γνωστοποίηση περιστατικών παραβίασης δεδομένων. Διαθέσιμο στην ιστοσελίδα: https://www.dpa.gr/portal/page?_pageid=33,211125&_dad=portal&_schema=PORTAL

Κάτσικας Σ. Κ. (2014), Διαχείριση της ασφάλειας πληροφοριών, Αθήνα, Εκδόσεις Πεδίο