Πανεπιστήμιο Πειραιά

Τμήμα Ψηφιακών Συστημάτων

Μεταπτυχιακό Πρόγραμμα Σπουδών

«ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

Θέμα: Προστασία Δεδομένων και Ιδιωτικότητας σε περιπτώσεις ανάθεσης έργων / υπηρεσιών πληροφορικής σε τρίτους φορείς (υπεργολάβους – outsourcing)

Γεωργιοπούλου Ζαφειρούλα

Δεκέμβριος 2011

Επιβλέπων: Επίκουρος καθηγητής

ΛΑΜΠΡΙΝΟΥΔΑΚΗΣ ΚΩΣΤΑΝΤΙΝΟΣ

Τμήμα Ψηφιακών Συστημάτων

Πανεπιστήμιο Πειραιά

Ευχαριστίες

Καθ' όλη την διάρκεια εκπόνησης της διπλωματικής εργασίας ο Δρ. Κωνσταντίνος Λαμπρινουδάκης υπήρξε σημαντικός αρωγός αυτής της προσπάθειας. Θα ήθελα να τον ευχαριστήσω για την συνεχή καθοδήγηση και για την άριστη συνεργασία που υπήρξε μεταξύ μας.

Περίληψη

Η ολοένα αυξανόμενη τάση των οργανισμών να αναθέτουν σε τρίτους έργα πληροφορικής τα οποία δεν αφορούν μόνο τις δομές (servers, δίκτυα κ.λπ.) αλλά και επιχειρησιακές λειτουργίες όπως η εισαγωγή, επεξεργασία και διατήρηση των δεδομένων που έχουν στη κατοχή τους, αναδεικνύεται μέσα από τις πρόσφατες έρευνες που διενεργήθηκαν σε οργανισμούς που δραστηριοποιούνται στο τομέα των πληροφοριακών συστημάτων. Κατά την ανάθεση της διαχείρισης δεδομένων σε τρίτους, προκύπτουν σημαντικά θέματα διασφάλισης της προστασίας και της ιδιωτικότητας των δεδομένων αυτών. Ιδιαίτερης σημασίας χρήζουν, οι περιπτώσεις όπου η ανάθεση αφορά επεξεργασία ευαίσθητων δεδομένων.

Στην παρούσα διπλωματική εργασία, παρουσιάζεται η σημερινή πραγματικότητα σε ότι αφορά την ανάθεση, ορίζοντας παράλληλα τους βασικότερους όρους και έννοιες που θα μας απασχολήσουν στην παρουσίαση του θέματος, βασιζόμενοι στη πρόσφατη βιβλιογραφία. Κατόπιν παρουσιάζεται αναλυτικά το Ελληνικό και Ευρωπαϊκό νομοθετικό καθεστώς που διέπει τους οργανισμούς που διαχειρίζονται προσωπικά δεδομένα και ειδικότερα στο νομοθετικό πλαίσιο που αφορά την ανάθεση της διαχείρισης σε τρίτους. Αναλύονται οι αδυναμίες – κίνδυνοι που μπορούν να προκύψουν. Τέλος με βάση τους κινδύνους ορίζονται οι απαιτήσεις της ασφάλειας και προτείνονται οι αντίστοιχες λύσεις που έχουν διατυπωθεί τόσο στον επιχειρηματικό όσο και στον ακαδημαϊκό χώρο. Στα πλαίσια της διπλωματικής εργασίας έχει αναπτυχθεί λογισμικό κρυπτογράφησης και αποκρυπτογράφησης ανταλλαγής δεδομένων ανάμεσα σε δύο ή περισσότερους οργανισμούς.

Η ανάθεση σε τρίτους έργων πληροφορικής και επικοινωνιών με την παράλληλη χρήση ευαίσθητων δεδομένων δεν έχει ως σήμερα αντιμετωπιστεί με την δέουσα σημασία. Ο χώρος της προστασίας της ιδιωτικότητας στις περιπτώσεις αυτές έχει ανάγκη από επιπλέον μελέτη και προσφέρεται για την ανάπτυξη τεχνολογιών που θα είναι ικανές να παρέχουν ένα ικανοποιητικό βαθμό προστασίας στην διαχείριση προσωπικών δεδομένων.

Πίνακας Περιεχομένων

1. Εισαγωγή

Κατά τη διάρκεια των τελευταίων δεκαετιών οι τεχνολογίες πληροφορικής και επικοινωνιών (ΤΠΕ) έχουν αναπτυχθεί ραγδαία. Οι επιχειρήσεις και οι οργανισμοί θέλοντας να ανταποκριθούν στις απαιτήσεις των νέων δεδομένων προσπαθούν να ενσωματώσουν τις νέες τεχνολογίες και τον τρόπο εργασίας που αυτές επιβάλλουν. Η σημαντικότερη αλλαγή στον τρόπο εργασίας που έχει παρατηρηθεί είναι η παραχώρηση εργασιών σε τρίτους. Στον κλάδο όμως των ΤΠΕ η συγκεκριμένη δραστηριότητα ενέχει σημαντικούς κινδύνους. Ο βασικότερος κίνδυνος στην παραχώρηση εργασιών σε τρίτους είναι η διαρροή πληροφοριών που αρκετές φορές εμπεριέχουν προσωπικά και ευαίσθητα δεδομένα.[1]

Η ανάθεση υπηρεσιών πληροφορικής σε τρίτους είναι η πρακτική της ανάθεσης μέρους ή όλων των λειτουργιών του τμήματος πληροφορικής σε εξωτερικούς παρόχους υπηρεσιών. (Grover and Cheon, 1996). Συνήθεις πρακτικές ανάθεσης αποτελούν οι δομές πληροφορικής (servers, δίκτυα κ.λπ.), επιχειρησιακές λειτουργίες πληροφορικής (εισαγωγή και επεξεργασία δεδομένων), ανάπτυξη εφαρμογών και άλλες παρόμοιες λειτουργίες.

Παρακάτω αναφέρονται οι σημαντικότεροι ορισμοί με βάση την βιβλιογραφία

- *"... turning over to a vendor some or all of the IS functions..." (Apte et al., 1997, p. 289)*
- *"...the contracting of various information systems' sub-functions by user firms to outside information systems vendors" (Chaudhury et al., 1995, p. 132)*
- *"...the organizational decision to turn over part or all of an organization's IS functions to external service provider(s) in order for an organization to be able to achieve its goals" (Cheon et al., 1995, p. 209)*

- *"... the commissioning of a third party (or a number of third parties) to manage a client organization's IT assets, people and/or activities (or part thereof) to required results" (Fitzgerald & Willcocks, 1994, p. 92)*
- *"...the third party provision of IT products and services" (Hancox & Hackney, 1999, p. 1)*
- *"...business practice in which a company contracts all or part of its information systems operations to one or more outside information service suppliers" (Hu et al., 1997, p. 288)*
- *"... a decision taken by an organization to contract-out or sell the organization's IT assets, people, and/or activities to a third party vendor, who in exchange provides and manages assets and services for monetary returns over an agreed time period" (Kern 1997, p. 37)*
- *"...the purchase of a good or service that was previously provided internally" (Lacity & Hirschheim, 1993b, p. 74).*
- "…the significant contribution by external vendors in the physical and/or human resources associated with the entire or specific components of the IT infrastructure in the user organization" (Loh & Venkatraman, 1992a, p. 9)
- "…the handing over to a third party management of IT/IS assets, resources, and/or activities for required results" (Willcocks & Kern, 1998, p. 2)

Τα βασικά χαρακτηριστικά της διαδικασίας ανάθεσης υπηρεσιών πληροφορικής σε τρίτους είναι τα κάτωθι :

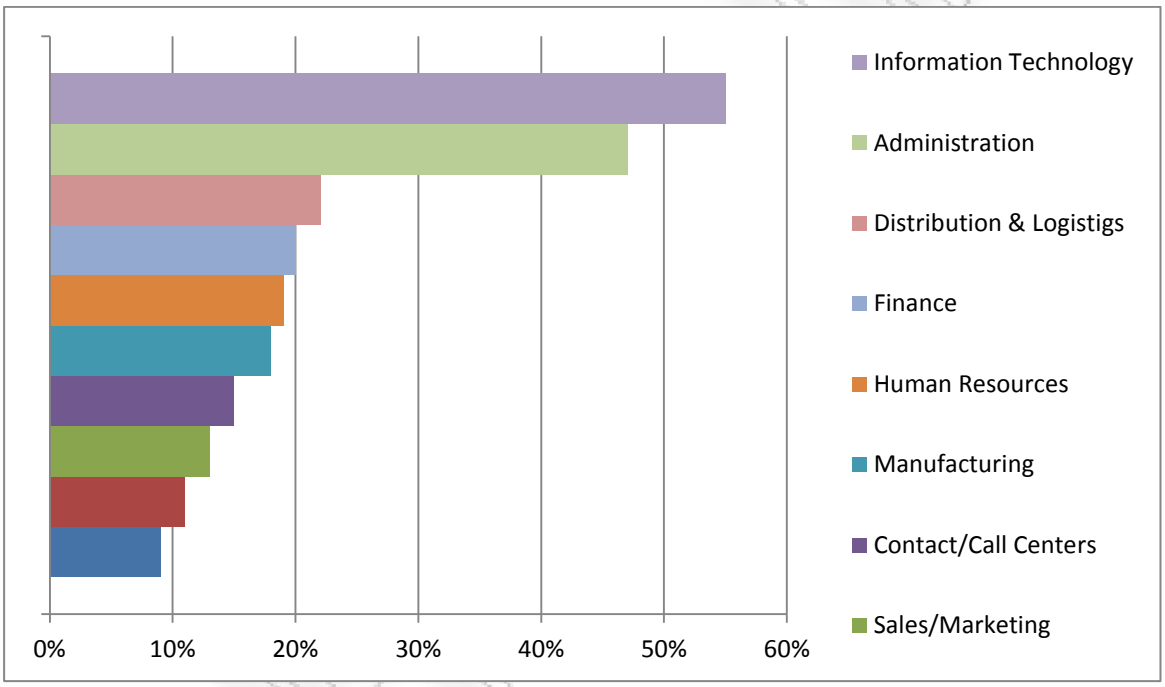
1. Ανάθεση σημαίνει ότι ο οργανισμός χρησιμοποιεί τρίτες οντότητες για να διαχειριστεί τα πληροφοριακά του συστήματα. Τα τελευταία αποτελούν και το αντικείμενο της ανάθεσης.

2. Τα πληροφοριακά συστήματα είναι συστήματα τα οποία χειρίζονται άνθρωποι και άρα δεν αναφερόμαστε μόνο σε τεχνολογίες πληροφορικής.

3. Οι υπηρεσίες που ανατίθενται είναι μέρος της κύριας λειτουργίας του οργανισμού και επομένως είναι απαραίτητο να εφαρμοστεί σχεδιασμός.

Οι βασικότεροι λόγοι επιλογής παραχώρησης μίας υπηρεσίας πληροφορικής σε τρίτους παρουσιάζονται παρακάτω:

1. μείωση του κόστους λειτουργίας
2. ελαχιστοποίηση του ρίσκου των νέων τεχνολογιών και υπηρεσιών
3. την εισαγωγή της καινοτομίας, ως συνεχούς παραμέτρου στον τρόπο λειτουργίας του οργανισμού.



Γραφ.1: Διαδικασίες προς ανάθεση

Πηγή:Outsourcing Institute- 5ο Ετήσιο Συνέδριο

Ο οργανισμός μέσω των υπηρεσιών που λαμβάνει και των σχέσεων Outsourcing που συνάπτει, κατορθώνει να βελτιώσει την ανταγωνιστικότητα του, να διαφοροποιήσει τα προϊόντα του απέναντι στο ανταγωνισμό και να ενισχύσει τη θέση του στην αγορά. Η χρήση νέων καινοτόμων τεχνολογιών και υπηρεσιών μέσω του Outsourcing, βοηθούν στη συνεχή

παραμονή της επιχείρησης στην αιχμή των γεγονότων και των εξελίξεων με μικρό κόστος επενδύσεων και ρίσκο.

Η αγορά του Outsourcing παγκόσμια γνωρίζει ιδιαίτερη ανάπτυξη και αναμένεται τα επόμενα χρόνια να αποτελέσει την πιο συνήθη πρακτική λήψης υπηρεσιών από τις επιχειρήσεις. Οι εξελίξεις στην τεχνολογία καθώς και η σύγκλιση των διαφορετικών πεδίων αυτής, βοηθούν ώστε να προσφέρονται από τους παρόχους νέες αρτιότερες υπηρεσίες καλύτερης ποιότητας σε συμφέρουσες τιμές.

2. Βιβλιογραφική Ανασκόπηση

Η διαθέσιμη βιβλιογραφία σχετικά με την ανάθεση σε υπεργολάβους είναι σημαντική και τα ζητήματα που αποτελούν αντικείμενο έρευνας είναι πολυάριθμα. Υπάρχουν τρία στάδια σε ένα έργο ανάθεσης υπηρεσιών πληροφορικής σε τρίτους με βάση τη χρονική αλληλουχία: πριν την υλοποίηση, η διαδικασία της υλοποίησης του έργου ανάθεσης και το αποτέλεσμα. Κατά αντιστοιχία, τα υπό έρευνα θέματα είναι: η απόφαση για ανάθεση υπηρεσιών, η εφαρμογή της ανάθεσης και το αποτέλεσμα της ανάθεσης. Επιπρόσθετα πολλά επιστημονικά άρθρα καλύπτουν περισσότερα από ένα στάδια της διαδικασία. Συνοψίζοντας, τα υπό έρευνα θέματα σχετικά με την ανάθεση, μπορούν να διαχωριστούν στις κάτωθι κατηγορίες:

- απόφαση
- υλοποίηση
- αποτέλεσμά
- ανάθεση υπηρεσιών πληροφορικής γενικά

Τα άρθρα που εντάσσονται στη κατηγορία «ανάθεση υπηρεσιών πληροφορικής γενικά» αναφέρονται στην ευρύτερη έννοια της ανάθεσης, συμπεριλαμβάνοντας ζητήματα όπως τη σημασία της ανάθεσης σε τρίτους, την κατηγοριοποίηση της ανάθεσης χωρίς να εμβαθύνουν την ανάλυση τους. Εν συνεχεία περιγράφεται συνοπτικά η κατηγοριοποίηση των τύπων και το εύρος των αναθέσεων σε ότι αφορά την υποστήριξη των παρόχων με βάση την σχετική βιβλιογραφία. Η υποστήριξη που παρέχεται είναι δυνατό να αφορά το υλικό (Hardware), το λογισμικό (Software) και άυλες υπηρεσίες με στόχο τη λήψη αποφάσεων σε θέματα τεχνολογίας, πληροφορικής και υπηρεσιών εκπαίδευσης των χρηστών. Αναφορικά με το υλικό, η υποστήριξη καλύπτει την παροχή όλης της απαραίτητης υλικοτεχνικής υποδομής για την παροχή υπηρεσιών σε μία επιχείρηση. Αντίστοιχα αναφορικά με το λογισμικό (Software) η υποστήριξη μπορεί να εκτείνεται από την απλή ανανέωση τυποποιημένων πακέτων λογισμικού, με στόχο την εύρυθμη λειτουργία των συστημάτων της επιχείρησης, έως την υποστήριξη σε επίπεδο ανάπτυξης και αποσφαλμάτωσης εφαρμογών οι οποίες έχουν αναπτυχθεί ειδικά για συγκριμένο πελάτη – επιχείρηση.

Η βιβλιογραφία που αναφέρεται στην έννοια της υλοποίησης μπορεί πολύ γρήγορα να γίνει κατανοητή με βάση τη φράση «πώς θα γίνει η εξωτερική ανάθεση;». Το προηγούμενο περιλαμβάνει τρία ζητήματα: επιλογή παρόχου, δόμηση σχέσης εμπιστοσύνης μεταξύ παρόχου και πελάτη (π.χ. διαπραγμάτευση συμβολαίου και χτίσιμο σχέσης) καθώς και διαχείριση και εφαρμογή της συμφωνίας που προκύπτει. Επομένως το «πώς» σχετίζεται με τις καλύτερες δυνατές επιλογές (best practices) , μεθόδους και τεχνικές που χρησιμοποιούνται για να επέλθει μια επιτυχής ανάθεση διασφαλίζοντας την ιδιωτικότητα. Παράδειγμα επιστημονικού άρθρου που εντάσσεται σε αυτή τη κατηγορία είναι του Klepper (1995). Αναλύει τον τρόπο δόμησης μιας μακροπρόθεσμης σχέσης μεταξύ παρόχου και πελατών χρησιμοποιώντας ένα ακολουθιακό μοντέλο ανάπτυξης σχέσεων συνεργασίας.

Σε ότι αφορά τη βιβλιογραφία που αναφέρεται στο αποτέλεσμα της ανάθεσης, θέμα της είναι η επίδραση που είχε στον οργανισμό, η επιτυχία ή η αποτυχία της συμφωνίας ,τα μαθήματα που πήραν οι άνθρωποι του οργανισμού μέσα από αυτή τη όλη διαδικασία και οι κίνδυνοι που προέκυψαν για την ιδιωτικότητα. Ουσιαστικά γίνεται αποτίμηση των πραγματικών αποτελεσμάτων της ανάθεσης απαντώντας σε ερωτήματα όπως:

- Ποιες ήταν οι εμπειρίες μέσα στον οργανισμό που προήλθαν μέσα από την ανάθεση των υπηρεσιών πληροφορικής τους σε τρίτους φορείς;
- Πώς μέσα από τις εμπειρίες θα οδηγηθούν στην επιτυχία του οργανισμού;
- Τι επιπτώσεις είχαν από την εφαρμογή της στην ευρύτερη λειτουργία του οργανισμού;

Από όλες αυτές τις ερωτήσεις και τα υπόλοιπα συμπεράσματα θα οδηγηθούν σε αποφάσεις σχετικά με την ανάθεση. Ένα επιστημονικό άρθρο το οποίο αναφέρεται στα αποτελέσματα της ανάθεσης είναι του Aubert et al (1998). Αναφέρεται σε πιθανά ή μη επιθυμητά αποτελέσματα που σχετίζονται άμεσα με την ανάθεση και τους παράγοντες του ρίσκου που μπορούν να οδηγήσουν σε αυτό το αποτέλεσμα. Επίσης ενδιαφέρον παρουσιάζουν τα επιστημονικά άρθρα σε αυτό το τομέα που εξετάζουν τη συμπεριφορά του εργαζομένου (Ang & Slaughter, 1998), τη συνέχιση των συμβολαίων μεταξύ οργανισμού και παρόχου (Fitzgerald & Willcocks, 1994), την ικανοποίηση των πελατών (Grover et al., 1996;

Lee & Kim, 1999; Saunders et al.,1997), ικανοποίηση παρόχου (Heckman & King, 1994), τα οικονομικά αποτελέσματα (Lacity et al., 1996) και τις αντιλήψεις της εξωτερικής ανάθεσης από διάφορους φορείς (Hirschheim & Lacity, 1998).[17]&[18]

3. Ελληνικό και Διεθνές νομικό πλαίσιο- Συμμόρφωση με ISO

3.1. Ιδιωτικότητα των δεδομένων.

Η ιδιωτικότητα αποτελεί ένα από τα πιο σημαντικά ζητήματα που συνδέονται με τις τεχνολογίες πληροφοριών. Κατά τη διάρκεια της συλλογής και ανταλλαγής δεδομένων προκύπτουν πολλά ερωτήματα τα οποία απαιτούν απαντήσεις. Τέτοιες ερωτήσεις είναι:

- Πώς μπορούν τα ευαίσθητα προσωπικά δεδομένα να αποθηκευτούν και να υποβληθούν σε επεξεργασία χωρίς να παραβιαστούν τα προσωπικά δικαιώματα και η ελευθερία των ατόμων;
- Πώς μπορούν τα προσωπικά δεδομένα να χρησιμοποιούνται αποκλειστικά από εξουσιοδοτημένες οντότητες με τέτοιο τρόπο ώστε να βοηθούν τα άτομα και όχι να τα βλάπτουν, παραδείγματος χάριν στιγματίζοντάς τα κοινωνικά;

Αυτά τα ερωτήματα στη περίπτωση της ανάθεσης είναι αναμφίβολο ότι θα τεθούν. Επίσης οποία απαιτούν απαντήσεις σε συνδυασμό τεχνικού, νομικού και κοινωνικού υπόβαθρου.

Στο κεφάλαιο αυτό θα εξετάσουμε το θέμα της ιδιωτικότητας των δεδομένων όπως αντιμετωπίζεται κυρίως από νομικής πλευράς. Συγκεκριμένα, στην παράγραφο 3.1.1 θα αναλύσουμε τα βασικότερα μοντέλα προστασίας της ιδιωτικότητας των δεδομένων. Στην παράγραφο 3.1.2 θα εξετάσουμε το βασικότερο από αυτά τα μοντέλα, τους νόμους και θα αναλύσουμε τη νομική προσέγγιση των Ευρωπαϊκών και μη Ευρωπαϊκών χωρών. Πιο συγκεκριμένα θα αναλύσουμε την Ελληνική νομοθεσία, τόσο για την προστασία των δεδομένων γενικότερα, όσο και για την προστασία των δεδομένων κατά την ανάθεση ειδικότερα. Μία αντίστοιχη ανάλυση θα κάνουμε για την Ευρωπαϊκή νομοθεσία περί προστασίας δεδομένων. Εν συνεχεία, στην παράγραφο θα ερευνήσουμε τη διεθνή νομική προσέγγιση για την προστασία των δεδομένων γενικότερα. Τέλος, θα εξετάσουμε τη

διασυνοριακή ροή δεδομένων, που αποτελεί έναν ανασταλτικό παράγοντα για την ιδιωτικότητα τους.

3.1.1. Μοντέλα Προστασίας της Ιδιωτικότητας Δεδομένων

Ένα από τα βασικότερα ερευνητικά ζητήματα στις μέρες μας, κυρίως λόγω της ραγδαίας ανάπτυξης της τεχνολογίας είναι η προσπάθεια για την προστασία της ιδιωτικότητας των δεδομένων. Οι περισσότερες χώρες του κόσμου αντιμετωπίζουν αυτό το καίριο ζήτημα θεσπίζοντας νέους νόμους ή ανανεώνοντας τους ήδη υπάρχοντες για την προστασία της ιδιωτικότητας των δεδομένων. Οι νόμοι αυτοί περιλαμβάνουν μέτρα για την διασφάλιση της ιδιωτικότητας. Συνήθως, υπάρχει ξεχωριστή νομοθετική μνεία για τέτοιου είδους δεδομένα, όπως συμβαίνει στην Ελλάδα και γενικότερα σε όλη την Ευρώπη.

Το πρώτο και βασικότερο μοντέλο για την προστασία δεδομένων είναι οι νόμοι που αφορούν τη συλλογή και την επεξεργασία των δεδομένων από δημόσιους ή ιδιωτικούς φορείς. Θεσπίζοντας νόμους οι χώρες δεν αφήνουν την προστασία δεδομένων στην κρίση του κάθε δημόσιου ή ιδιωτικού φορέα. Σε κάθε χώρα που έχει θεσπίσει νόμους για την προστασία δεδομένων υπάρχει συνήθως κάποια δημόσια Αρχή η οποία επιτηρεί την εφαρμογή τους.

Σε κάποιες περιπτώσεις, όμως, όπως συμβαίνει στην Αμερική, δεν υπάρχει κάποιος γενικός νόμος περί προστασίας ευαίσθητων ή προσωπικών δεδομένων. Αντίθετα, για κάθε τομέα, όπως για παράδειγμα προστασία οικονομικών ή ιατρικών δεδομένων, υπάρχει ξεχωριστή νομοθεσία. Το μειονέκτημα σε αυτήν την περίπτωση είναι ότι με κάθε ξεχωριστό τομέα της ανθρώπινης δραστηριότητας ή με κάθε καινούρια τεχνολογία θα πρέπει να θεσπίζεται ξεχωριστός νόμος.

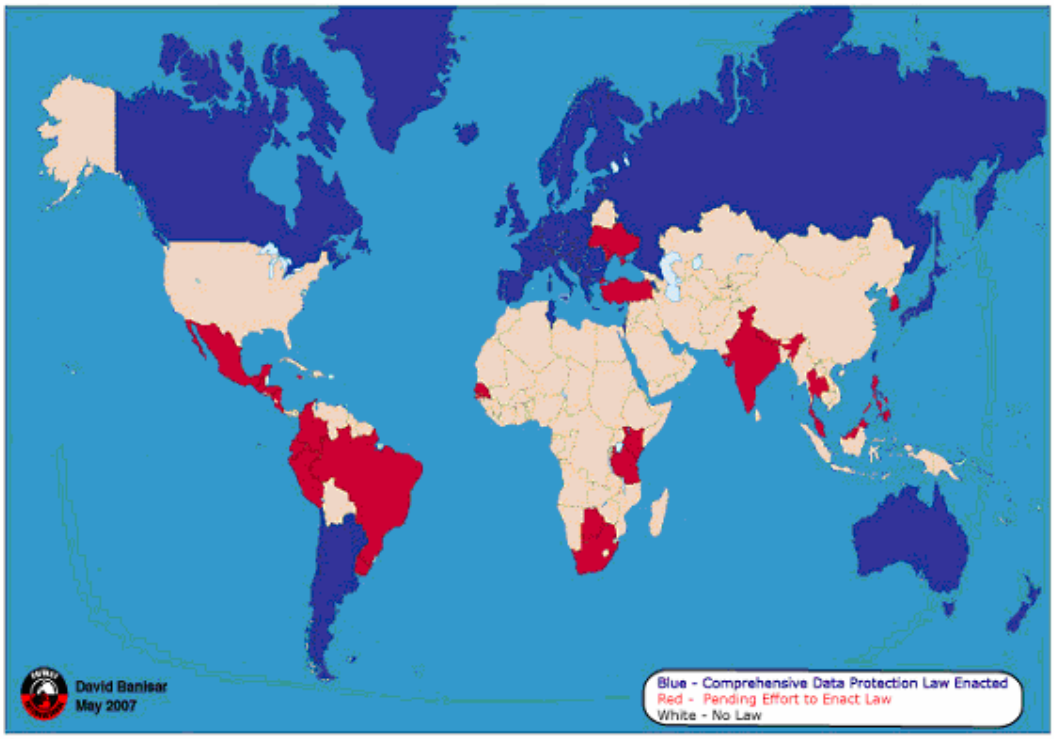
Σε πολλές περιπτώσεις, η προσπάθεια για προστασία των δεδομένων μπορεί να γίνει και από τους ίδιους τους φορείς, όπως οι εταιρίες, οι επιχειρήσεις και άλλα. Έτσι λοιπόν μπορούν να δημιουργήσουν ένα σύνολο από αρχές και οδηγίες που θα προσδιορίζουν τα δικαιώματα που έχει η κάθε συμμετέχουσα οντότητα πάνω στα προσωπικά δεδομένα. Το μοντέλο αυτό από μόνο του δεν μπορεί να προσφέρει σημαντική προστασία διότι συνήθως είναι ανεπαρκές και στερείται απόλυτου ελέγχου για την επιβολή του. Επιπρόσθετα, δεν

μπορεί να υπάρχει μία κοινή πολιτική προστασίας αφού οι οδηγίες και οι αρχές αυτές βρίσκονται στην ευχέρεια του κάθε φορέα.

Τέλος, με τη ραγδαία ανάπτυξη της τεχνολογίας, η προστασία δεδομένων μπορεί να καταλήξει στα χέρια του κάθε χρήστη. Για παράδειγμα, οι χρήστες του διαδικτύου μπορούν να εγκαταστήσουν στον προσωπικό τους υπολογιστή προγράμματα ή συστήματα προκειμένου να επιτύχουν το βαθμό ασφάλειας που επιθυμούν. Παραδείγματα αποτελούν οι τοίχοι προστασίας, οι *proxy servers* ή η κρυπτογράφηση.

Σε αυτό το σημείο θα πρέπει να σημειωθεί ότι τα παραπάνω μοντέλα δεν είναι απαραίτητο να χρησιμοποιούνται ανεξάρτητα. Αντιθέτως, μπορούν να χρησιμοποιηθούν παράλληλα (ακόμα και όλα) προκειμένου να παρέχεται η μέγιστη προστασία των ευαίσθητων/προσωπικών δεδομένων.

Στον παρακάτω χάρτη παρουσιάζεται η νομική αντιμετώπιση της προστασίας δεδομένων από όλες τις χώρες του κόσμου μέχρι το Μάιο του 2007. Ο χάρτης αυτός έχει αντληθεί από τον ιστοχώρο: *PrivacyInternational*[88].



Νομική αντιμετώπιση ανά τον κόσμο για την προστασία δεδομένων.

3.1.2. Ελληνική Νομοθεσία

Η Ελλάδα είναι μία από τις χώρες που έχουν ξεχωριστό νόμο για την προστασία δεδομένων προσωπικού χαρακτήρα γενικότερα (Νόμος 2472/1997) Στις ακόλουθες ενότητες θα αναλύσουμε τις βασικές αρχές των νόμου αυτού για την προστασία των δεδομένων και των κατόχων τους.

Ο νόμος 2472/1997 έχει ως βάση τις οδηγίες του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία φυσικών προσώπων σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ο νομοθέτης θεσπίζει τους βασικούς όρους και προϋποθέσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προκειμένου να προστατεύονται τα δικαιώματα και οι θεμελιώδεις ελευθερίες των φυσικών προσώπων, καθώς και η ιδιωτική τους ζωή. Ειδικότερα, κάνει διαχωρισμό των δεδομένων σε δεδομένα προσωπικού χαρακτήρα και σε ευαίσθητα δεδομένα. Τα δεδομένα «προσωπικού χαρακτήρα» σχετίζονται με το υποκείμενο των δεδομένων. Παραδείγματα τέτοιου είδους αποτελούν το όνομα, η

διεύθυνση ή γενικότερα κάποιο προσδιοριστικό της οικονομικής, πολιτιστικής ή κοινωνικής ταυτότητας του ατόμου. Από την άλλη, τα «ευαίσθητα δεδομένα» σχετίζονται και πάλι με το υποκείμενο αλλά χρήζουν μεγαλύτερης διαφύλαξης. Παραδείγματα τέτοιου είδους αποτελούν η φυλετική ή εθνική προέλευση, οι θρησκευτικές πεποιθήσεις και η υγεία.

Τα «ευαίσθητα δεδομένα», εξαιτίας της φύσης τους απαιτούν πιο αυστηρό τρόπο νομικής αντιμετώπισης σε σχέση με τα «προσωπικά δεδομένα». Βασικό ερώτημα που προκύπτει σε αυτό το σημείο είναι ποιες πρέπει να είναι οι προϋποθέσεις συλλογής των δεδομένων, ποιες οι συνθήκες επεξεργασίας τους και από ποιον θα χρησιμοποιηθούν. Ο νόμος 2472/1997 απαντά σε αυτά τα ερωτήματα. Η συλλογή δεδομένων πρέπει να είναι καθορισμένη, θεμιτή και νόμιμη, ενώ ο κάθε πολίτης θα πρέπει να είναι σε θέση να γνωρίζει ποιος, που, πότε, πώς και γιατί επεξεργάζεται τα «προσωπικά του δεδομένα». Η επεξεργασία προσωπικών δεδομένων θα πρέπει να τηρεί τις προϋποθέσεις τις οποίες αναφέρει ο νόμος. Έτσι, η συλλογή και επεξεργασία «ευαίσθητων δεδομένων» απαγορεύεται, εκτός αν συντρέχει λόγοι, όπως η διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, ή λόγοι εθνικής ασφάλειας, αναγκών εγκληματολογίας, προστασία δημόσιας υγείας και άλλοι. Τέλος, στο νόμο αναφέρονται τα δικαιώματα του υποκειμένου των δεδομένων, όπως το δικαίωμα ενημέρωσης, πρόσβασης, αντίρρησης, ή προσωρινής δικαστικής προστασίας του. [21]

3.1.3. Ευρωπαϊκή Νομοθεσία για την Προστασία Δεδομένων Προσωπικού

Στην Ευρώπη η Ευρωπαϊκή Επιτροπή είναι αρμόδια σχετικά με το ευρύτερο θεσμικό πλαίσιο για την ασφάλεια των δεδομένων με την έκδοση σχετικών Οδηγιών, Κανονισμών και Συστάσεων. Η Ευρωπαϊκή Ένωση έχει τους αυστηρότερους νόμους περί προστασίας δεδομένων και θεμελιωδών ελευθεριών των ανθρώπων. Η Ευρωπαϊκή νομοθεσία περιλαμβάνει ξεχωριστές Οδηγίες για την προστασία δεδομένων (Οδηγία 95/46/ΕΕ [22]) οι βασικές αρχές των οποίων θα παρουσιαστούν στην ακόλουθες ενότητες.

Το 1995, η Ευρωπαϊκή Ένωση θέσπισε την Οδηγία 95/46/ΕΕ [22], γνωστή και ως Οδηγία ιδιωτικότητας της ΕΕ. Μέσα από την Οδηγία αυτή η ΕΕ απαιτεί από όλα τα κράτη μέλη της να θεσπίσουν τους δικούς τους νόμους βασισμένους στους κανόνες της Οδηγίας περί προστασίας των θεμελιωδών δικαιωμάτων των ανθρώπων. Η βασικότερη αρχή της Οδηγίας είναι ότι κάθε άνθρωπος έχει το δικαίωμα της μυστικότητας της προσωπικής και οικογενειακής του ζωής καθώς και της αλληλογραφίας του. Επιπλέον, η Οδηγία κατοχυρώνει σε κάθε πολίτη το δικαίωμα να γνωρίζει το που αποθηκεύονται τα δεδομένα του, από ποιον επεξεργάζονται και για ποιο λόγο. Τα δεδομένα μπορούν να συλλέγονται μόνο για συγκεκριμένους και νόμιμους λόγους. Παράλληλα, δεν πρέπει να συλλέγονται περισσότερα δεδομένα από όσα είναι απαραίτητα για να επιτευχθεί ο σκοπός συλλογής τους ή να κρατούνται για μεγαλύτερο χρονικό διάστημα από τον αρχικό λόγο συλλογής τους. Επιπρόσθετα, η Οδηγία τονίζει ότι η επεξεργασία των δεδομένων, η οποία απέχει από τον αρχικό στόχο συλλογής τους, μπορεί να πραγματοποιηθεί μόνο με τη συγκατάθεση του ατόμου στο οποίο ανήκουν τα δεδομένα. Η συλλογή και επεξεργασία των δεδομένων θα πρέπει πάντα να γίνεται με γνώμονα την προσωπική ζωή του κάθε ατόμου, ακόμα και αν στα δεδομένα αυτά δεν περιέχονται ευαίσθητα δεδομένα. Ο μόνος λόγος για να μην ασκηθούν αυτά τα δικαιώματα είναι οι περιπτώσεις εθνικής προστασίας, δημόσιας ασφάλειας και υγείας, οικονομικής ευημερίας της κάθε χώρας ή για την πρόληψη εγκληματικών ή τρομοκρατικών ενεργειών.

Μια άλλη απαίτηση που προκύπτει μέσα από την Οδηγία για κάθε μέλος της Ευρωπαϊκής Ένωσης, είναι να έχει τη δική της δημόσια Αρχή (ή τις δικές της αρμόδιες Αρχές) η/οι οποία/ες θα ελέγχει/ουν το κατά πόσο τηρούνται οι νόμοι του κάθε κράτους. Βασικός όρος είναι οι Αρχές αυτές των κρατών μελών της ΕΕ θα πρέπει να βρίσκονται σε συνεργασία μεταξύ τους, ενώ οι υπάλληλοι μιας τέτοιας Αρχής δεσμεύονται από το επαγγελματικό απόρρητο για τις εμπιστευτικές πληροφορίες στις οποίες έχουν πρόσβαση στη διάρκεια της υπηρεσίας τους αλλά και μετά από το τέλος των καθηκόντων τους (άρθρο 28 της Οδηγίας 95/46/ΕΕ).

Τέλος, λόγω της ανησυχίας της Ευρώπης για τη νομοθεσία των μη Ευρωπαϊκών χωρών και ιδιαίτερα των ΗΠΑ, η Οδηγία προστατεύει τους Ευρωπαίους πολίτες της από τη μεταφορά των δεδομένων τους προς τις χώρες αυτές.

3.1.4. Διεθνής Νομοθεσία

Δεδομένου ότι μέσω του διαδικτύου γίνεται καθημερινή ανταλλαγή πληροφοριών (και ειδικά προσωπικών δεδομένων) σε όλο τον κόσμο, πολλές χώρες στρέφονται σε νομοθετικές προσπάθειες για την προστασία της προσωπικής μυστικότητας. Παραδείγματος χάριν, οι κυβερνήσεις της Ασίας, της Αυστραλίας και της Νέας Ζηλανδίας, της Ιαπωνίας, του Χονγκ Κονγκ, της Αμερικής και της Νότιας Αφρικής έχουν θεσπίσει νομοθεσία ώστε να προστατεύσουν τα προσωπικά δεδομένα και τη μυστικότητα. Στις ακόλουθες παραγράφους θα εξετάσουμε τις νομοθετικές προσεγγίσεις των μη Ευρωπαϊκών χωρών για την προστασία των δεδομένων.

Στην Ασία έχει θεσπιστεί νομοθεσία για το σεβασμό των ανθρωπίνων δικαιωμάτων και ελευθεριών, καθώς επίσης και για την ιδιωτικότητα των προσωπικών δεδομένων του ατόμου. Στην Αυστραλία, η ιδιωτικότητα των δεδομένων προστατεύεται από νόμο του 1998 που αναφέρεται στο δίκαιο χειρισμό των προσωπικών πληροφοριών των ατόμων . Αυτός ο νόμος παρέχει προστασία για τα προσωπικά δεδομένα που συλλέγονται είτε από δημόσιους είτε από ιδιωτικούς φορείς. Επίσης, η Νέα Ζηλανδία έχει θεσπίσει νομοθεσία για την προστασία των δικαιωμάτων των πολιτών της, παρόμοια με τη νομοθεσία της Αυστραλίας.

Το 2005, η Ιαπωνία θέσπισε πέντε νέους νόμους για την προστασία των δεδομένων. Συγκεκριμένα, οι νόμοι αυτοί αφορούν την προστασία της ιδιωτικότητας των προσωπικών δεδομένων τα οποία χρησιμοποιούνται όχι μόνο στο δημόσιο αλλά και στον ιδιωτικό τομέα και καθορίζουν τον τρόπο με τον οποίο οι δημόσιοι ή οι ιδιωτικοί φορείς συλλέγουν, διατηρούν και επεξεργάζονται τις προσωπικές πληροφορίες. Αυτοί οι νόμοι περιλαμβάνουν την προστασία των δεδομένων για τους ιατρικούς και οικονομικούς τομείς.

Το 1996 το Χονγκ Κονγκ πέρασε το διάταγμα περί προστασίας προσωπικών δεδομένων, το οποίο έχει επηρεαστεί από την Οδηγία της Ευρωπαϊκής Ένωσης. Το Χονγκ Κονγκ προστατεύει την ιδιωτικότητα των πολιτών του αποτρέποντας οποιονδήποτε συσχετισμό των δεδομένων άμεσα ή έμμεσα με κάποιο πρόσωπο και ισχύει για οποιονδήποτε χρήστη ο οποίος συλλέγει, διατηρεί, ή επεξεργάζεται τα προσωπικά δεδομένα. Οι ιδιοκτήτες των δεδομένων έχουν το δικαίωμα να επιβεβαιώνουν το που φυλάσσονται τα δεδομένα τους.

Θα πρέπει επίσης να αναφερθεί ότι από τις χώρες που μελετάμε, η Κίνα δεν έχει ιστορία στην προστασία των δικαιωμάτων ιδιωτικότητας των πολιτών της και παρέχει ακόμα λιγότερη προστασία μυστικότητας των δεδομένων. Όσον αφορά στους κανονισμούς που αφορούν την ασφάλεια διαδικτύου, η Κίνα παρέχει την πιο περιορισμένη προστασία των δικαιωμάτων.

Η Αμερική αποτελεί μία από τις χώρες οι οποίες έχουν θεσπίσει νόμους ανά τομέα. Δηλαδή, η νομοθεσία της δεν αποτελείται από έναν νόμο για την προστασία των προσωπικών δεδομένων γενικά, αλλά από ξεχωριστούς νόμους για κάθε είδους δεδομένων. Έτσι, για παράδειγμα, έχει ξεχωριστό νόμο για την προστασία των ιατρικών δεδομένων, ή των οικονομικών δεδομένων. Ένα πολύ σημαντικό μειονέκτημα της Αμερικάνικης νομοθεσίας σε σχέση με την Ευρωπαϊκή είναι η έλλειψη νόμου προστασίας μυστικότητας για τον ιδιωτικό τομέα. Σε αυτό το σημείο, είναι σημαντικό να αναφερθεί ότι εκτός της Ευρώπης, στην Αυστραλία, την Ιαπωνία και το Χονγκ Κονγκ, η νομοθεσία για την ιδιωτικότητα δεδομένων είναι πιο αυστηρή σε σχέση με τη νομοθεσία των ΗΠΑ.

Τέλος, στη Νότια Αφρική, η ιδιωτικότητα αντιμετωπίζεται ως θεμελιώδες ανθρώπινο δικαίωμα και ως εκ τούτου έχει θεσπιστεί νομοθεσία για την προστασία δεδομένων τόσο για το δημόσιο όσο και για τον ιδιωτικό τομέα. Οι νόμοι αυτοί αναγνωρίζουν τα δικαιώματα των πολιτών και προστατεύουν την ιδιωτικότητα του ατόμου σε πολλούς τομείς της καθημερινής ζωής, όπως ο ιατρικός τομέας, οι τραπεζικές συναλλαγές, το μάρκετινγκ και άλλα.

3.1.5. Διασυνοριακή Ροή Δεδομένων Προσωπικού Χαρακτήρα

Ένας πολύ σημαντικός παράγοντας στην ιδιωτικότητα δεδομένων είναι η γνώση του ποιος θα επεξεργαστεί τα δεδομένα καθώς είναι πολύ πιθανό στην εποχή του «cloud» να έχουμε και ανάθεση έργων πληροφορικής σε πάροχο άλλης χώρας. Μέχρι πριν λίγα χρόνια κάθε χώρα είχε τη δυνατότητα να έχει τη δική της νομοθεσία για την προστασία των ανθρώπινων δικαιωμάτων. Πλέον, με την εκρηκτική αύξηση της χρήσης των υπολογιστών και του διαδικτύου τα προβλήματα της προστασίας των δεδομένων δεν περιορίζονται μόνο σε μία περιοχή ή μόνο σε ένα κράτος. Στις ημέρες μας, στόχος είναι να εξασφαλιστεί ο διεθνής σεβασμός των δικαιωμάτων κάθε ανθρώπου. Η δυνατότητα όλοι οι υπολογιστές σε όλο τον κόσμο να συνδέονται μεταξύ τους μέσω του διαδικτύου αυξάνει αυτήν την ανησυχία, αφού συχνά οι χώρες που λαμβάνουν τα προσωπικά δεδομένα μπορεί να μην έχουν την ίδια, ή και καθόλου, νομοθεσία για την προστασία των ανθρώπινων δικαιωμάτων. Για το λόγο αυτό, αυτές οι χώρες προσελκύουν εκείνους που επιθυμούν να επεξεργαστούν δεδομένα με πιο επιεικείς νομικούς κανόνες. Κατά τη διασυνοριακή ροή δεδομένων πέρα από τη χώρα στην οποία έχουν συλλεχθεί δεν υπάρχει καμία δυνατότητα ελέγχου της μη επιθυμητής επεξεργασίας τους.

Για τους παραπάνω λόγους, ότι αφορά την πραγματοποίηση ή όχι της διασυνοριακής ροής δεδομένων και επομένως εξωτερικής ανάθεσης , στην Ελλάδα, αρμόδια αρχή που εξετάζει και αποφαίνεται είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Η Αρχή παρέχει άδεια για τη μεταφορά των δεδομένων σε κάποια άλλη χώρα εφόσον κρίνει ότι η χώρα αυτή, στην οποία θα πραγματοποιηθεί η επεξεργασία των δεδομένων, εξασφαλίζει ικανοποιητικό επίπεδο προστασίας τους. Βάση του ελέγχου είναι η φύση των δεδομένων, καθώς και οι σκοποί και η διάρκεια της επεξεργασίας τους. Το ίδιο, φυσικά, ισχύει και για όλες τις Ευρωπαϊκές χώρες. Στο νόμο περί προστασίας δεδομένων της Ευρωπαϊκής Ένωσης, και συγκεκριμένα στα άρθρα 25-26 , αναλύεται το ιδιαίτερα σημαντικό ζήτημα της διασυνοριακής ροής προσωπικών δεδομένων προς τρίτα κράτη εκτός της ΕΕ. Η ροή δεδομένων σε χώρες εντός της ΕΕ δεν απαιτεί ιδιαίτερη νομοθεσία αφού όλες οι χώρες-μέλη ακολουθούν το νομοθετικό πλαίσιο που προτείνει η ΕΕ. Για το λόγο αυτό τα δεδομένα μπορούν να μεταφέρονται ελεύθερα από το ένα κράτος-μέλος στο άλλο. Στις υπόλοιπες

χώρες, όμως, η νομοθεσία για την ιδιωτικότητα δεδομένων μπορεί να είναι κατώτερη ή ακόμη και ανεπαρκής. Για το λόγο αυτό, η Οδηγία απαιτεί να μη διαβιβάζονται τα δεδομένα σε χώρες οι οποίες δεν εξασφαλίζουν την επαρκή προστασία τους. Τα κράτη μέλη οφείλουν να ελέγξουν και να μην επιτρέψουν τη ροή των προσωπικών πληροφοριών σε τρίτα κράτη που δεν εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας, λαμβάνοντας υπόψη όλες τις σχετικές περιστάσεις και τους όρους της επεξεργασίας τους στο άλλο κράτος.

Μερικά κράτη, όπως οι ΗΠΑ, δεν έχουν επεκτείνει τη νομοθεσία τους για την προστασία δεδομένων στον ιδιωτικό τομέα, με αποτέλεσμα η ΕΕ να απαγορεύει σε πολλές περιπτώσεις τη διαβίβαση δεδομένων στις ΗΠΑ. Πριν την ηλεκτρονική εποχή, οι διαφορές στις πολιτικές μυστικότητας των δεδομένων μεταξύ της Ευρώπης και των ΗΠΑ ήταν ελάχιστες. Στη σημερινή εποχή, όπου το ηλεκτρονικό εμπόριο και οι ηλεκτρονικές υπηρεσίες αποτελούν κομμάτι της καθημερινής μας ζωής, η διαφορά στις πολιτικές αυτές είναι πολύ μεγάλη. Παρόλο που σήμερα η Ευρώπη βρίσκεται πολύ πιο πίσω στη χρήση υπολογιστών και διαδικτύου σε σχέση με τις ΗΠΑ, οι νόμοι της περί προστασίας ιδιωτικότητας των δεδομένων είναι οι πιο περιεκτικοί σε όλο τον κόσμο. Για το λόγο αυτό η ΕΕ παροτρύνει τους αγοραστές μέσω διαδικτύου να αποφεύγουν τις ηλεκτρονικές αγορές από αμερικάνικες επιχειρήσεις λόγω των ανησυχιών

Παράλληλα, η ΕΕ έχει το δικαίωμα να ελέγξει και να αποφανθεί για το εάν τα τρίτα κράτη εξασφαλίζουν το απαραίτητο επίπεδο προστασίας της ιδιωτικής ζωής και των θεμελιωδών ελευθεριών και δικαιωμάτων του ατόμου. Η διασυνοριακή ροή δεδομένων προς τρίτες χώρες, οι οποίες μπορεί να μην παρέχουν το απαραίτητο επίπεδο προστασίας τους, επιτρέπεται μόνο στις περιπτώσεις όπου ο ιδιοκτήτης των δεδομένων δώσει την συγκατάθεσή του ή σε περιπτώσεις έκτακτης ανάγκης, όπως η διασφάλιση εθνικής προστασίας ή η ανίχνευση τρομοκρατικών και εγκληματικών επιθέσεων. Επιπλέον, υπάρχει η δυνατότητα διασυνοριακής ροής δεδομένων προς χώρες με ανεπαρκές επίπεδο προστασίας, από τη στιγμή που η αρμόδια Αρχή παρέχει ικανοποιητική εγγύηση για την προστασία της ιδιωτικής ζωής και των δικαιωμάτων του ατόμου. [21]

3.2. Νομικό πλαίσιο για την προστασία των δεδομένων κατά την εξωτερική ανάθεση

Αφού αναφέραμε την ισχύουσα νομοθεσία για την προστασία των προσωπικών δεδομένων στο επόμενο κεφάλαιο θα αναφέρουμε τι ορίζει σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο για τη προστασία της ιδιωτικότητα και επομένως και των προσωπικών δεδομένων κατά την ανάθεση σε εξωτερικούς παρόχους υπηρεσιών.

3.2.1. Ελληνική Νομοθεσία

Στα πλαίσια του νόμου 2472/97 για τα προσωπικά δεδομένα ο νομοθέτης, λαμβάνοντας υπόψη την ευρέως διαδεδομένη πρακτική του outsourcing προβλέπει ώστε η σχετική ανάθεση μεταξύ του υπεύθυνου και του εκτελούντος την επεξεργασία να γίνεται πάντα εγγράφως και με την υποχρέωση του πρώτου ώστε ο εκτελών την επεξεργασία να δεσμεύεται από τις σχετικές υποχρεώσεις (Άρθρο 10 παρ. 4 Ν. 2472/97). Ο νόμος (άρθρο 10 § 3) επιτάσσει τη λήψη μέτρων τα οποία "πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας". [21]

Επιπλέον, άλλοι νόμοι που διέπουν την προστασία των δεδομένων κατά την ανάθεση σε τρίτους σε εθνικό επίπεδο είναι :

- Ν. 2819/2000 α.8. Τροποποίηση του Ν. 2472/1997.
- Ν. 2774/1999 Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.
- Απόφαση 408/1998 Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Ενημέρωση υποκειμένων επεξεργασίας δεδομένων προσωπικού χαρακτήρα δια του τύπου Κωδικοποίηση σε ενιαίο κείμενο του
- Ν.3057/2002 (ΦΕΚ 239 Α΄/10 Οκτωβρίου 2002) - άρθρο 81 - Εναρμόνιση με την Οδηγία 2001/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 29ης Μαΐου 2001 για την εναρμόνιση ορισμένων πτυχών του δικαιώματος

του δημιουργού και των συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας και άλλες διατάξεις"

- Ν. 2819/2000 α.8. Τροποποίηση του Ν. 2472/1997.
- Ν. 2774/1999 Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.
- Απόφαση 408/1998 Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Ενημέρωση υποκειμένων επεξεργασίας δεδομένων προσωπικού χαρακτήρα δια του τύπου Κωδικοποίηση σε ενιαίο κείμενο του
- Ν. 2819/2000 Άρθρο 7 . Εναρμόνιση με την Οδηγία 96/9/ΕΟΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Μαρτίου 1996 σχετικά με τη νομική προστασία των βάσεων δεδομένων. (Τροποποίηση του Ν. 2121/93).
- Ν 2557/1997/Α-271 Θεσμοί μέτρα και δράσεις πολιτιστικής ανάπτυξης (Τροποποίηση του Ν. 2121/93)
- Ν 2435/1996 (Τροποποίηση του Ν. 2121/93)
- Ν. 2121/1993 Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα.[23]

3.2.2. Ευρωπαϊκή Νομοθεσία

Οι πάροχοι υπηρεσιών και οι υπεύθυνοι ασφάλειας που εδρεύουν στην Ευρωπαϊκή κοινότητα πρέπει να λάβουν σοβαρά υπόψη τις νομικές υποχρεώσεις και τους περιορισμούς που προκύπτουν από τα συμβόλαια ανάθεσης. Η εμπιστευτικότητα, η προστασία της πνευματικής ιδιοκτησίας, η υπευθυνότητα και η ασφάλεια είναι ζητήματα πρώτης προτεραιότητας κατά την ανάθεση. Το νομικό και κανονιστικό πλαίσιο παρόλα αυτά δεν παρέχει μόνο περιορισμούς στην τρίτη οντότητα αλλά αποτελεί και μέσο για την επιλογή αξιόπιστου παρόχου και διαμόρφωση κατάλληλου συμβολαίου.

Τα τελευταία χρόνια νομικά και κανονιστικά πλαίσια. που ρυθμίζουν τις απαιτήσεις από έναν πάροχο υπηρεσιών αυξάνονται ραγδαία . Παραδείγματα αυτών είναι το Sarbanes Oxley Act (2002), οι απαιτήσεις που ορίζει η Βασιλεία ΙΙ (Basel II, 2005) [13], η Ευρωπαϊκή

οδηγία για την προστασία των δεδομένων και ρυθμίσεις πιο εξιδεικεύμενες για τις τηλεπικοινωνίες και το ηλεκτρονικό εμπόριο (EUEC, 2000).

Στη συνέχεια θα αναλύσουμε τις απαιτήσεις που θέτει η Ευρωπαϊκή κοινότητα για την ανάθεση σε εξωτερικούς φορείς. Η ιδιωτικότητα και η προστασία των προσωπικών δεδομένων αποτέλεσε όπως αναλύσαμε σε προηγούμενη ενότητα επίκεντρό συζητήσεων για πολλές δεκαετίες στη πλειονότητα των Ευρωπαϊκών χωρών. Η εφαρμογή λοιπόν της ευρωπαϊκής οδηγίας για τη προστασία των προσωπικών δεδομένων δεν επέβαλλε μόνο την υποχρέωση αλλά ενθάρρυνε και τους χρήστες να ελέγχουν και να σκέφτονται κριτικά για την διαχείριση των προσωπικών τους δεδομένων (European Commission, 1998).[25]

Στο βαθμό που η εξωτερική ανάθεση σχετίζεται ή περιλαμβάνει επεξεργασία προσωπικών δεδομένων, ο «Διαχειριστής» των δεδομένων, δηλαδή το φυσικό ή νομικό πρόσωπο που ορίζει τον σκοπό και τα μέσα της επεξεργασίας (Αρ. 2d) , πρέπει να συμμορφώνεται με τις απαιτήσεις των οδηγιών όπως αυτές έχουν ενταχθεί στο νομικό πλαίσιο της χώρας του η οποία είναι μέλος της Κοινότητας. Η οδηγία για τα προσωπικά δεδομένα καλύπτει την επεξεργασία προσωπικών δεδομένων με αυτοματοποιημένες ή μη διαδικασίες (Αρ. 3), επομένως είναι αδιαμφισβήτητο ότι όλες οι μορφές επεξεργασίας κατά την ανάθεση σε εξωτερικούς φορείς θα πρέπει να είναι σύμφωνη με τις απαιτήσεις της.

Βασικό ζήτημα που ορίζει η νομοθεσία της Ε.Ε. με κατάλληλες οδηγίες είναι οι υποχρεώσεις του Διαχειριστή και αυτού που επεξεργάζεται τα δεδομένα εκ μέρους του διαχειριστή (Αρ. 2e). Ο τελευταίος είναι αρμόδιος για τη διασφάλιση των αρχών της προστασίας προσωπικών δεδομένων (αναλογικότητα, σκοπό, ακρίβεια, διάρκεια κ.λπ.). Ο διαχειριστής είναι αρμόδιος να διασφαλίσει ότι τηρείται ο σκοπός της νόμιμης επεξεργασίας προσωπικών δεδομένων (Αρ. 7) και ότι τηρούνται οι συνθήκες για την επεξεργασία ευαίσθητων δεδομένων (Αρ. 8).

Αναμφίβολα, συμφώνα με την ευρωπαϊκή οδηγία υπόχρεός να συμμορφώνεται νομικά είναι ο κάτοχος των δεδομένων, ανεξάρτητα αν η επεξεργασία τους έχει ανατεθεί σε εξωτερικό φορέα. Οι κάτοχοι επομένως είναι υποχρεωμένοι να λάβουν όλα τα απαραίτητα μέτρα που σχετίζονται με τις πληροφορίες και τα δικαιώματα πρόσβασης των δεδομένων

(Αρ. 10,11,12), όπως επίσης και για το δικαίωμα του υποκειμένου των δεδομένων να αρνηθούν την επεξεργασία (Αρ. 14). Παρόλα αυτά και ο κάτοχος και ο εξωτερικός φορέας υπόκεινται στις ανεξάρτητές αρχές για τη προστασία των δεδομένων και σε περίπτωση μη νόμιμης επεξεργασίας προσωπικών δεδομένων και οι δύο αντιμετωπίζουν κυρώσεις [24]

Οι πλέον σημαντικές απαιτήσεις για μια συμφωνία ανάθεσης αναφέρονται στην εμπιστευτικότητα (Αρ. 16) και στην ασφάλεια (Αρ. 17) της επεξεργασίας των δεδομένων. Το άρθρο 16 αναφέρει ότι οποιοσδήποτε δρα εκ μέρους του Διαχειριστή καθώς και ο ίδιος δεν πρέπει να επεξεργάζεται δεδομένα τα οποία παραβιάζουν τους κανόνες που έχει θέσει ο διαχειριστής με μοναδική εξαίρεση τη περίπτωση επιβολής από το νόμο. Σε περίπτωση λοιπόν εξωτερικής ανάθεσης οι διαχειριστές θα πρέπει με γραπτό συμβόλαιο να ορίσουν τις προϋποθέσεις και τα όρια επεξεργασίας. Οι εξωτερικοί φορείς λοιπόν θα πρέπει να λάβουν όλα τα τεχνικά και διαδικαστικά μέτρα ασφάλειας ώστε να εξασφαλίσουν την εμπιστευτικότητα μέσα από τον κατάλληλο έλεγχο πρόσβασης και την καταγραφή κάθε πρόσβασης στα προσωπικά δεδομένα. Επίσης τα συμβόλαια μεταξύ εξωτερικού φορέα και νόμιμου ιδιοκτήτη των δεδομένων θα πρέπει να ορίζουν σαφώς την ανεξάρτητη αρχή στην οποία υπόκειται ο πάροχος των υπηρεσιών. Σε περίπτωση απουσίας μη επίσημης, ασαφούς και μη γραπτής οδηγίας από τον νόμιμο ιδιοκτήτη για την επεξεργασία το δεδομένων ο εξωτερικός φορέας μπορεί να απαιτήσει επιπλέον αποζημίωση για να καλύψει την ανάληψη της ευθύνης [25].

Στο άρθρο 17 η Ευρωπαϊκή οδηγία ορίζει τις απαιτήσεις ασφάλειας για μια συμφωνία εξωτερικής ανάθεσης. Επομένως αναφέρει τις υποχρεώσεις των νόμιμων ιδιοκτήτων των δεδομένων σχετικά με την μη καταπάτηση των προσωπικών δεδομένων (μη νόμιμη καταστροφή, απώλεια δεδομένων, τροποποίηση, μη εξουσιοδοτημένη δημοσιοποίηση και πρόσβαση ή οποιαδήποτε άλλη μορφή παράνομης επεξεργασίας). Οι ίδιες υποχρεώσεις ανατίθενται και στον εξωτερικό φορέα (Αρ.17 § 3), ο οποίος είναι υπόχρεος να δρα με βάση τις οδηγίες του νόμιμου ιδιοκτήτη. Τέλος τα μέτρα ασφάλειας που λαμβάνει ο εξωτερικός φορέας θα πρέπει να ορίζονται σε γραπτή ή άλλη ισότιμη μορφή.

3.2.3. Νομικό πλαίσιο εξωτερικής ανάθεσης σε διαφορετική χώρα

Όταν ένας οργανισμός αποφασίζει να αναθέσει σε εξωτερικούς φορείς ο πλέον πιθανός στόχος είναι να μειώσει το κόστος επεξεργασίας των δεδομένων κάτι που οδηγεί στην επιλογή φορέων που εδρεύουν σε χώρες χαμηλού βιοτικού επιπέδου. Η οδηγία της ευρωπαϊκής ένωσης όμως συχνά αποτελεί εμπόδιο για την ανάθεση σε χώρες εκτός κοινότητας καθώς είναι δύσκολο να εφαρμοστεί η ισχύουσα νομοθεσία.

Το νομικό πλαίσιο της Ε.Ε. που διέπει τη μεταφορά προσωπικών δεδομένων σε τρίτες χώρες όταν γίνεται ανάθεση σε εξωτερικούς φορείς είναι τα άρθρα 25 και 26 της οδηγίας. Στο άρθρο 25 αναφέρεται ότι η ανάθεση μπορεί να γίνει αν η χώρα παρέχει ένα ισότιμο επίπεδο προστασίας παραθέτοντας στη § 2 μια λίστα με κριτήρια για το επίπεδο προστασίας (συνθήκες, περιβάλλον, φύση των δεδομένων, σκοπός, διάρκεια, κανόνες ανά τομέα, επαγγελματικούς κανόνες, μέτρα ασφάλειας, κλπ).

Το επίπεδο της ασφάλειας σύμφωνα με το άρθρο 26 κρίνεται από την εκάστοτε ανεξάρτητη αρχή προστασίας των προσωπικών δεδομένων. Σε περίπτωση που το επίπεδο δεν είναι ικανοποιητικό το άρθρο προβλέπει μια περιορισμένη λίστα παρεκκλίσεων, οι οποίες ουσιαστικά δεν είναι εφαρμόσιμες σε συμβόλαια ανάθεσης σε τρίτους.

3.3. Απαιτήσεις συμμόρφωσης με το ISO

Ο Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization, διακριτική ονομασία: ISO), δημιουργεί και εκδίδει πρότυπα. Αποτελείται από αντιπροσώπους των εθνικών οργανισμών τυποποίησης. Ο οργανισμός ιδρύθηκε στις 23 Φεβρουαρίου του 1947 και παράγει τα παγκόσμια βιομηχανικά και εμπορικά πρότυπα, τα επονομαζόμενα πρότυπα ISO. Ο ISO έχει εκδώσει ειδική οδηγία για την περίπτωση ανάθεσης διαδικασιών του οργανισμού σε εξωτερικούς φορείς με βάση το πρότυπο 27001 για τα πληροφοριακά συστήματα ενός οργανισμού.

Ως ανάθεση σε εξωτερικούς φορείς ο οργανισμός θεώρει ότι ο όρος περιλαμβάνει τη μεταβίβαση της ευθύνης για τη διεξαγωγή μιας δραστηριότητας (η οποία πριν γινόταν εσωτερικά) σε τρίτο φορέα επί προσυμφωνημένης αποζημίωσης. Ο εξωτερικός φορέας παρέχει υπηρεσίες στους πελάτες του σε ένα κοινά αποδεκτό επίπεδο υπηρεσιών, που συνήθως ορίζεται με συμβόλαιο. Τα πλεονεκτήματα με βάση την ISO από την ανάθεση είναι η μείωση του κόστους, η δυνατότητα του οργανισμού να ασχοληθεί πιο έντονα με πιο βασικές για τον οργανισμό λειτουργίες και να έχει πιο εξειδικευμένα άτομα. Τα μειονεκτήματα όμως είναι τα περιστατικά ανασφάλειας που μπορεί να προκύψουν όπως η μη νόμιμη πρόσβαση και αποκάλυψη ευαίσθητων πληροφοριών, η απώλεια της προστασίας της πνευματικής ιδιοκτησίας και η ανικανότητα του εξωτερικού φορέα να διατηρήσει τα απαιτούμενα επίπεδα παροχής υπηρεσιών.

Ως παρόχους υπηρεσιών θεωρεί τις εταιρείες παροχής υπηρεσιών υποστήριξης υλικούς και λογισμικού, εξωτερικούς συμβούλους, εταιρείες που αναλαμβάνουν υπηρεσίες πληροφορικής ή άλλου είδους, εποχιακό προσωπικό.

Βάση που ορίζει η ISO είναι να ισορροπήσει τα εμπορικά πλεονεκτήματα από την ανάθεση σε τρίτους και τους κινδύνους οι οποίοι πρέπει να διαχειριστούν με την εφαρμογή κατάλληλων ελέγχων. Οι έλεγχοι αυτοί πρέπει να αποτελούν συνδυασμό νομικών, φυσικών, διαδικαστικών και διαχειριστικών ελέγχων.

Μέσα στη πολιτική για τη συμμόρφωση με το ISO 27001 αναφέρεται, τι πρέπει να λάβει υπόψη ένας οργανισμός για να θέσει τα κριτήρια επιλογής εξωτερικού φορέα τα οποία θα πρέπει για να υπάρχει συμμόρφωση να είναι τεκμηριωμένα και καταγεγραμμένα. Βασικοί παράγοντες για τον ορισμό των κριτηρίων είναι η φήμη και η ιστορία του παρόχου, η ποιότητα υπηρεσιών σε άλλους πελάτες της, ο αριθμός και η ικανότητα του προσωπικού της, η οικονομική της σταθερότητα, τεκμηρίωση της ποιότητας και υπάρχουσες πιστοποιήσεις από διεθνείς οργανισμούς.

Η ISO με βάση το πρότυπο θεωρεί αναγκαίο πριν την ανάθεση να γίνει αποτίμηση των κινδύνων. Για να γίνει αυτό θα πρέπει η διοίκηση να ορίσει ένα «ιδιοκτήτη» κάθε λειτουργίας/διαδικασίας που θα ανατεθεί, ο οποίος θα συνεισφέρει στην αποτίμηση του ρίσκου μαζί με την Ομάδα Αποτίμησης Ρίσκου. Ζητήματα τα οποία θα πρέπει να ληφθούν σοβαρά υπόψη είναι τα εξής:

- Οι ανάγκες που προκύπτουν για φυσική και λογική πρόσβαση στις πληροφορίες και στον εξοπλισμό του οργανισμού ώστε να μπορεί ο πάροχος να ικανοποιήσει τις απαιτήσεις του συμβολαίου.
- Η ευαισθησία, ο όγκος και η αξία των πληροφοριών στις οποίες θα έχει πρόσβαση ο πάροχος.
- Εμπορικούς κινδύνους που προκύπτουν. Κίνδυνοι μπορεί να είναι, να μην είναι σε θέσει ο εξωτερικός φορέας να παρέχει καθόλου υπηρεσίες ή στο επίπεδο που έχει συμφωνηθεί στη συμφωνία για τη ποιότητα υπηρεσιών (SLA- Service Level Agreement) ή να παρέχει υπηρεσίες σε ανταγωνιστικό οργανισμό.
- Μέτρα ασφάλειας που έχει ήδη λάβει ο οργανισμός ή ο φορέας.

Η ISO απαιτεί τα αποτελέσματα της αποτίμησης κινδύνων να παρουσιαστούν στη διοίκηση για έγκριση πριν την υπογραφή του συμβολαίου ανάθεσης ώστε να αποφασίσει αν η ανάθεση θα ωφελήσει τον οργανισμό λαμβάνοντας υπόψη την ασφάλεια από πλευράς πληροφοριών και εμπορικά.

Μέσα στη πολιτική ανάθεσης η ISO θέτει απαιτήσεις για το συμβόλαιο και το σύμφωνο εμπιστευτικότητας ανάμεσα στον οργανισμό και τον εξωτερικό πάροχο. Το συμβόλαιο λοιπόν απαιτείται για να προστατέψει και τις δύο πλευρές και θα πρέπει να ορίζει ξεκάθαρα το είδος και το τρόπο των πληροφοριών που ανταλλάσσονται. Ως αποτέλεσμα αυτού σε περίπτωση που οι πληροφορίες που ανταλλάσσονται είναι ευαίσθητες απαιτείται σύμφωνο εμπιστευτικότητας ανάμεσα στον οργανισμό και τον εξωτερικό φορέα είτε ως μέρος του συμβολαίου είτε ως ξεχωριστή συμφωνία καθώς είναι πιθανό να απαιτείται

χωριστά πριν την έναρξη οποιασδήποτε συζήτησης. Επίσης το σύμφωνο εμπιστευτικότητας είναι πιθανό να χρειάζεται ακόμα και μετά τη λήξη του συμβολαίου μεταξύ παρόχου και οργανισμού. Τα συμβόλαια θα πρέπει να ορίζουν ξεκάθαρα τις υποχρεώσεις και των δύο μερών, ημερομηνία έναρξης ισχύος, λειτουργίες για τις οποίες παρέχονται υπηρεσίες, εταιρική ευθύνη, περιορισμοί που τίθενται σχετικά με τη χρήση υπεργολάβων και άλλα εμπορικά ή νομικά ζητήματα. Επίσης με βάση την αποτίμηση κινδύνου που απαιτεί το ISO για συμμόρφωση διάφοροι πρόσθετοι έλεγχοι είναι δυνατόν να συμπεριλαμβάνονται στο συμβόλαιο όπως:

- Νομικές κανονιστικές και άλλες υποχρεώσεις των εξωτερικών φορέων όπως η τήρηση του νόμου για την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας, το ξέπλυμα χρήματος κλπ.*
- Υποχρεώσεις και μέτρα ασφάλειας πληροφοριών όπως:
    - Πολιτικές ασφάλειας πληροφοριών, διαδικασίες, πρότυπα και οδηγίες που απαιτούνται στα πλαίσια της διαχείρισης ασφάλειας πληροφοριακών συστημάτων (ISMS – InformationSecurityManagementSystem) όπως αυτό που ορίζεται στο πρότυπο ISO/IEC 27001.
    - Έλεγχοι στους εργαζομένους που θα δουλεύουν στο πάροχο.
    - Έλεγχοι πρόσβασης που θα περιορίζουν την μη εξουσιοδοτημένη αποκάλυψη, τροποποίηση ή καταστροφή των πληροφοριών, συμπεριλαμβάνοντας ελέγχους φυσικής και λογικής πρόσβασης, διαδικασίες εξουσιοδότησης, αναθεώρησης, ενημέρωσης και ανάκλησης πρόσβασης στο σύστημα, στα δεδομένα, στις εγκαταστάσεις κ.λπ.
    - Διαδικασίες διαχείρισης περιστατικών ανασφάλειας.
    - Επιστροφή ή καταστροφή όλων των δεδομένων από τον εξωτερικό πάροχο μετά την ολοκλήρωση της συνεργασίας ή όταν οι πληροφορίες δεν είναι πλέον απαραίτητες.

*σε περίπτωση ανάθεσης σε άλλη χώρα πρέπει να γίνει ιδιαίτερη αναφορά στις επιπτώσεις της μεταφοράς των πληροφοριών μεταξύ των χωρών και σε πιθανές διαφορές ανάμεσα στα νομικά πλαίσια λαμβάνοντας και τη βοήθεια ενός νομικού.

- Ζητήματα δικαιωμάτων αντιγραφής, πατέντες και γενικά ζητήματα πνευματικής ιδιοκτησίας που μπορεί να σχετίζονται με το πάροχο πρέπει να ορίζονται στο συμβόλαιο.
- Έλεγχοι για προστασία από κακόβουλο λογισμικό.

- Το δικαίωμα του οργανισμού να καταγράφει τη πρόσβαση και τη χρήση του εξοπλισμού, των δικτύων, και των συστημάτων και να ελέγχει τη συμμόρφωση του εξωτερικού παρόχου με το συμβόλαιο ή να προσληφθεί ανεξάρτητος τρίτος φορέας για αυτό το σκοπό.
- Συμφωνίες για σχέδιο συνέχεια και ανάκαμψης από καταστροφή.

Για συμμόρφωση με το πρότυπο η ISO απαιτεί την εκπαίδευση και τον έλεγχο του προσωπικού του παρόχου όπως αυτοί που γίνονται στο προσωπικό του οργανισμού. Αυτοί οι έλεγχοι θα πρέπει να λάβουν υπόψη το επίπεδο εμπιστοσύνης και την ευθύνη που έχει η θέση του καθενός. Ειδικότερα:

- Αποδείξεις για τη ταυτότητα του κάθε εργαζόμενου (π.χ. ταυτότητα)
- Αποδείξεις για τις πανεπιστημιακές σπουδές (π.χ. πιστοποιητικά)
- Αποδείξεις για την επαγγελματική εμπειρία (π.χ. βιογραφικό και συστατικές επιστολές)

Ένα κατάλληλο πρόγραμμα για ευαισθητοποίηση σε ζητήματα ασφάλειας πληροφοριών θα πρέπει να γίνει σε όλους του εργαζόμενους του οργανισμού και του παρόχου μέσα από το οποίο θα αναδεικνύονται οι αρμοδιότητες που σχετίζονται με τις πολιτικές ασφάλειας, τα πρότυπα, τις διαδικασίες και οδηγίες και όλες τις σχετικές πληροφορίες που ορίζονται μέσα στο συμβόλαιο.

Σε ότι αφορά τον έλεγχο πρόσβασης η ISO απαιτεί για να είναι σε θέση ο οργανισμός να αποτρέψει τη μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες από τον εξωτερικό πάροχο

την χρήση κατάλληλων ελέγχων ασφάλειας όπως αυτές που θα παρουσιάσουμε παρακάτω. Οι λεπτομέρειες εξαρτώνται από το είδος των πληροφοριών και τους συσχετιζόμενους κινδύνους, κάνοντας σαφές ότι είναι αναγκαία η αποτίμηση κινδύνων και ο σχεδιασμός των κατάλληλων ελέγχων.

Η πολιτική προτείνει μια λίστα για το τι πρέπει να περιλαμβάνει από τεχνικής πλευράς τα μέτρα για τον έλεγχο πρόσβασης:

- Ταυτοποίηση και αυθεντικοποίηση του χρήστη.
- Εξουσιοδοτημένη πρόσβαση, μέσα από τη συσχέτιση των χρηστών με ρόλους οι οποίοι θα έχουν τα κατάλληλα δικαιώματα και ελέγχους.
- Κρυπτογράφηση των δεδομένων με βάση τις πολιτικές κρυπτογράφησης του οργανισμού και τα πρότυπα μέσα από τα οποί ορίζονται οι αλγόριθμοι, το μήκος του κλειδιού και η διαχείριση κλειδιών κ.λπ.
- Παρακολούθηση των προσβάσεων και εισαγωγή μηχανισμών προειδοποίησης για πιθανή προσπάθεια μη εξουσιοδοτημένης πρόσβασης.

Οτιδήποτε αφορά τον έλεγχο πρόσβαση για να υπάρχει συμμόρφωσης\ με το πρότυπο πρέπει να τεκμηριωθεί μέσα από διαδικασίες, οδηγίες και σχετικά έγγραφα και μέσα από εκπαίδευση και εκπαιδευτικές δραστηριότητες. Αυτό περιλαμβάνει:

- Επιλογή σωστών συνθηματικών.
- Προσδιορισμός και εφαρμογή σωστών δικαιωμάτων πρόσβασης.
- Αναθεώρηση των μέτρων ελέγχου πρόσβασης για να διατηρούν τη συμμόρφωση με τις απαιτήσεις του προτύπου.

Η πολιτική προτείνει μια λίστα για το τι πρέπει να περιλαμβάνουν τα φυσικά μέτρα ασφάλειας για τον έλεγχο πρόσβασης:

- Έλεγχοι που να περιλαμβάνουν το εξωτερικό και το εσωτερικό του κτιρίου.
- Καλά κατασκευασμένες εγκαταστάσεις.
- Κατάλληλα μέτρα ασφάλειας φυσικής πρόσβασης.
- Καταγραφή πρόσβασης με χρήση καρτών, καταγραφή επισκεπτών κ.λπ.
- Συναγερμούς και διαδικασίες απόκρισης.

Στη περίπτωση που κάποιος από τον υλικό εξοπλισμό θα φιλοξενηθεί στο κέντρο πληροφοριών (Datacenter) του εξωτερικού παρόχου οι διαχειριστές θα πρέπει να βεβαιωθούν ότι είναι απομονωμένο φυσικά και λογικά από άλλα συστήματα.

Η ISO απαιτεί στη περίπτωση που κάποια λειτουργία του οργανισμού έχει ανατεθεί σε εξωτερικό φορέα που έχει ως έδρα διαφορετική από αυτή του οργανισμού θα πρέπει περιοδικά να ελέγχει τις εγκαταστάσεις του παρόχου σχετικά με τη συμμόρφωση στις πολιτικές ασφάλειας του οργανισμού και με βάση τις απαιτήσεις που έχουν οριστεί στο συμβόλαιο. Σε ότι αφορά το συμβόλαιο κατά τον έλεγχο θα πρέπει να ληφθεί υπόψη το επίπεδο υπηρεσιών. Η συχνότητα των ελέγχων πρέπει να οριστεί από τη διοίκηση.

Μέσα στις απαιτήσεις για συμμόρφωση με το πρότυπο, ορίζονται και οι αρμοδιότητες των εμπλεκόμενων μερών. Η διοίκηση είναι υπεύθυνη να ορίσει τους κατάλληλους ιδιοκτήτες των υπηρεσιακών λειτουργιών που ανατίθενται, ώστε να παρακολουθούν τις δραστηριότητες και να επιβεβαιώνουν ότι η πολιτική ακολουθείται. Επίσης η διοίκηση είναι υπεύθυνη για να επιβάλλει μέτρα για την διαχείριση των εμπορικών κινδύνων και των κινδύνων ασφάλειας που προκύπτουν από την ανάθεση. Ο εξωτερικός φορέας είναι υπεύθυνος για την αποτίμηση και τη διαχείριση των κινδύνων που αφορούν την ασφάλεια των πληροφοριών και των εμπορικών σκοπών του οργανισμού καθώς και ότι αφορά τις

νομικές υποχρεώσεις. Η ασφάλεια πληροφοριών σε συνδυασμό με τις νομικές υποχρεώσεις, τη συμμόρφωση με πρότυπα, και τη διαχείριση κίνδυνων είναι υπεύθυνη να βοηθήσει των εξωτερικό φορέα να αναλύσει τους συσχετιζόμενους κινδύνους και να υιοθετήσει κατάλληλες διαδικασίες που να περιλαμβάνουν τεχνικούς, φυσικούς και νομικούς ελέγχους. Τέλος για να υπάρχει συμμόρφωση θα πρέπει η ομάδα εσωτερικών ελέγχων που είναι εξουσιοδοτημένη από τη διοίκηση να υπάρχει συμμόρφωση με τις πολιτικές του οργανισμού, θα πρέπει να βοηθήσει στους ελέγχους του εξωτερικού φορέα.[26]

4. Τομείς ασφαλούς IT outsourcing και παραδείγματα.

Η πρόσληψη υπηρεσιών από μια επιχείρηση μέσω Outsourcing μπορεί να λάβει διαφορετικές μορφές και εκτάσεις. Έτσι το Outsourcing μπορεί να λάβει τις ακόλουθες μορφές:

- Ως προς τις υπηρεσίες και το αντικείμενό τους ενδεικτικές κατηγορίες είναι: οι υπηρεσίες τεχνικής υποστήριξης (technical support), δικτύωσης (networking), παροχής υποδομής (systems infrastructure), παροχής περιβάλλοντος ανάπτυξης (development environment), εφαρμογών (applications), περιεχόμενου (content), υποστήριξης διαδικασιών (process support) καθώς και ανάληψης διαδικασιών (process execution).
- Ως προς το χρόνο αντίδρασης του παρόχου, κατηγορίες υπηρεσιών Outsourcing είναι: συνεχούς παροχής υπηρεσιών (performance), με συγκεκριμένα επίπεδα ποιότητας. Τυπικά παραδείγματα τέτοιων υπηρεσιών είναι η παροχή λειτουργιών εξυπηρετητών ηλεκτρονικού ταχυδρομείου, αρχείων κ.λπ., η παροχή υπηρεσιών back-office, η παροχή υπηρεσιών call center κ.ο.κ.. Απόκρισης σε συμβάντα (reactive), όπου ο πάροχος αντιδρά στην περίπτωση κάποιου γεγονότος ή/και αιτήματος από την επιχείρηση. Τυπικό παράδειγμα τέτοιων υπηρεσιών είναι η υποστήριξη των σταθμών εργασίας. Πρόληψης (proactive), όπου ο πάροχος παρέχει συγκεκριμένες υπηρεσίες στοχεύοντας στην πρόληψη προβλημάτων. Τυπικά παραδείγματα τέτοιων υπηρεσιών είναι η λήψη αντιγράφων ασφαλείας, ο τακτικός έλεγχος ασφάλειας των πληροφοριακών συστημάτων κ.ο.κ.
- Ως προς το βαθμό εμπλοκής της επιχείρησης, οι υπηρεσίες Outsourcing κατηγοριοποιούνται σε αυτές που απαιτείται μερική δραστηριοποίηση κάποιου τμήματος της επιχείρησης για την παροχή των υπηρεσιών (Partial Outsourcing). Οι υπηρεσίες παρέχονται με συνεργασία μεταξύ του παρόχου και του τμήματος της επιχείρησης το οποίο είναι αρμόδιο. Και στις υπηρεσίες που η παροχή των υπηρεσιών γίνεται πλήρως από τον πάροχο (Full Outsourcing). Από την πλευρά της επιχείρησης πραγματοποιείται μόνο η διαχείριση της σύμβασης.

- Ως προς τον αριθμό των παρόχων οι οποίοι εμπλέκονται για την παροχή των υπηρεσιών Outsourcing κατηγοριοποιούνται σε αυτές που η παροχή πραγματοποιείται από έναν πάροχο (Single Outsourcing). Και σε αυτές στις οποίες η παροχή πραγματοποιείται από πολλαπλούς παρόχους σε συνεργασία (Multiple Outsourcing).

4.1. Επαγγελματικοί και κοινωνικοί τομείς που γίνεται ανάθεση.

Η διεθνής εμπειρία έχει δείξει ότι το πλήθος και το είδος των υπηρεσιών τις οποίες μπορεί μία επιχείρηση να εκχωρήσει σε τρίτους είναι απεριόριστο. Από την απλή συντήρηση ενός εξυπηρετητή αρχείων, έως την πλήρη εκχώρηση των υπηρεσιών σε τρίτες εταιρείες. Χαρακτηριστικό είναι το παράδειγμα γνωστής μάρκας αναψυκτικών η οποία διατηρεί εντός της εταιρείας μόνο το τμήμα προώθησης και διαφήμισης. Όλες οι υπόλοιπες φάσεις παραγωγής και διακίνησης των εμπορευμάτων της έχουν εκχωρηθεί σε τρίτους μέσω σχέσεων ανάθεσης. Στην περίπτωση, πιο συγκεκριμένα, των υπηρεσιών πληροφορικής (Information Technology – IT), οι υπηρεσίες οι οποίες συνηθίζεται να εκχωρούνται αφορούν τις ακόλουθες περιπτώσεις. Την Τεχνική Υποστήριξη όλης της υλικοτεχνικής υποδομής μίας επιχείρησης. Η υποστήριξη που παρέχεται είναι δυνατό να αφορά το υλικό (Hardware) το λογισμικό (Software) καθώς και άυλες υπηρεσίες με στόχο τη λήψη αποφάσεων σε θέματα τεχνολογίας και πληροφορικής καθώς και υπηρεσιών εκπαίδευσης των χρηστών. Αναφορικά με το λογισμικό (Software) η υποστήριξη μπορεί να εκτείνεται από την απλή ανανέωση τυποποιημένων πακέτων λογισμικού με στόχο την εύρυθμη λειτουργία των συστημάτων τις επιχείρησης, έως την υποστήριξη σε επίπεδο ανάπτυξης και αποσφαλμάτωσης εφαρμογών οι οποίες έχουν αναπτυχθεί ειδικά για λογαριασμό του πελάτη – επιχείρηση. Τη Δικτύωση, καλύπτοντας την παροχή όλης της απαραίτητης υλικοτεχνικής υποδομής για την παροχή δικτυακών υπηρεσιών σε μία επιχείρηση. Οι δικτυακές υπηρεσίες δεν αφορούν μόνο τη συνδεσιμότητα αλλά επεκτείνονται και σε υπηρεσίες δεδομένων (όπως είναι το ηλεκτρονικό ταχυδρομείο, η πρόσβαση στον παγκόσμιο ιστό – World Wide Web, η παρουσία και προβολή στον παγκόσμιο ιστό μέσω εταιρικής σελίδας κ.λπ.) καθώς και φωνής.

Επιπρόσθετα η παροχή υλικοτεχνικής υποδομής μπορεί να αφορά τόσο τη σύνδεση των γραφείων – παραρτημάτων μίας επιχείρησης μεταξύ τους και το παγκόσμιο διαδίκτυο, όσο και την παροχή της κατάλληλης υποδομής για την εξυπηρέτηση των αναγκών για δικτύωση u949 εντός των γραφείων της επιχείρησης (εσωτερικό δίκτυο). Η υποδομή για τη Δικτύωση ανήκει είτε στον πάροχο της υπηρεσίας, οπότε και με τη λήξη της σύμβασης η υποδομή επιστρέφει σε αυτόν, είτε στην επιχείρηση (κυρίως στην περίπτωση της εσωτερικής δικτύωσης) οπότε ο πάροχος ουσιαστικά προσφέρει υπηρεσίες διαχείρισης. Στην πρώτη περίπτωση με τη λήξη της σύμβαση συνεργασίας η υποδομή επιστρέφει στον πάροχο και είναι ευθύνη του νέου παρόχου, αν αυτός υπάρχει, να εγκαταστήσει την απαραίτητη υποδομή για την παροχή των υπηρεσιών. Την παροχή Υποδομής Εφαρμογών, η οποία και αφορά την προμήθεια υπηρεσιών εξυπηρετητών ή σταθμών εργασίας και των απαραίτητων εφαρμογών για τη λειτουργία των διαδικασιών τους. Οι υποδομές στη πλειοψηφία τους αφορούν την παροχή υπηρεσιών εξυπηρετητών προς τις επιχειρήσεις. Οι εξυπηρετητές αυτοί βρίσκονται συγκεντρωμένοι σε κάποιο Data Center, μέσω του οποίου παρέχονται υπηρεσίες σε μεγάλο αριθμό επιχειρήσεων. Οι εφαρμογές οι οποίες παρέχονται πάνω από αυτούς τους εξυπηρετητές αφορούν εφαρμογές ηλεκτρονικού επιχειρείν, λογιστικές εφαρμογές, διαχείρισης αποθήκης, προγραμματισμού συναντήσεων, επικοινωνίας και μηνυμάτων, διαχείρισης βάσεων δεδομένων καθώς και λήψης αντιγράφων ασφαλείας.

Οι υπηρεσίες Περιεχομένου αναφέρονται στην πρόσβαση σε δεδομένα απαραίτητα για την αποδοτική λειτουργία μιας επιχείρησης. Τα δεδομένα αυτά είναι δυνατό να αφορούν πολύ διαφορετικά αντικείμενα όπως πληροφορίες τεχνικής και τεχνολογικής φύσης (όπως κείμενα τεχνικών προδιαγραφών, προτύπων κ.λπ.), νομικών κειμένων (πρόσβαση σε βιβλιοθήκες με νομοθεσία του Ελληνικού κράτους ή της Κοινότητας) ή και πληροφορίες για τμήμα της αγοράς (πληροφορίες ζήτησης, προσφοράς, προκηρύξεων, αγοράς εργασίας κ.λπ.). Τα δεδομένα αυτά είναι δυνατό να έχουν επεξεργαστεί ή όχι.

Το outsourcing μπορεί να φτάσει μέχρι την πλήρη Ανάληψη και Υποστήριξη Διαδικασιών εντός της επιχείρησης. Οι διαδικασίες αυτές παρέχονται είτε στους χώρους της επιχείρησης είτε απομακρυσμένα ανάλογα με το είδος τους και τη σχετική συμφωνία μεταξύ

της επιχείρησης και του παρόχου. Τέτοιες υπηρεσίες συνήθως είναι οι υπηρεσίες διαχείρισης ανθρώπινων πόρων, τηλεφωνικής επαφής με τους πελάτες (call center), λογιστικής υποστήριξης καθώς και τεχνικής –τεχνολογικής υποστήριξης. Σε αυτή την περίπτωση η επιχείρηση δεν απασχολεί καθόλου πόρους για τις υπηρεσίες αυτές, μόνο την ομάδα παρακολούθησης και ελέγχου της σχετικής σύμβασης με τον πάροχο. Με αυτό τον τρόπο οι πόροι της επιχείρησης κατευθύνονται και επικεντρώνονται στις διαδικασίες και υπηρεσίες εκείνες οι οποίες αποτελούν τον πυρήνα της επιχειρηματικής δραστηριότητάς της.[20],[11],[13]

5. Κίνδυνοι & Απαιτήσεις ασφάλειας

5.1. Κίνδυνοι

Οι δημόσιοι οργανισμοί και οι ιδιωτικές εταιρείες που αναθέτουν τη διαχείριση των δεδομένων τους σε τρίτους αποθηκεύουν τα δεδομένα τους σε εξυπηρετητές-παρόχους οι οποίο πάντα ενέχουν τον κίνδυνο διαρροής της πληροφορίας. Αυτό έχει ως συνέπεια πέρα από τους γνωστούς κινδύνους για την ιδιωτικότητα και την εμπιστευτικότητα στους οποίους υπόκεινται όλα τα δεδομένα, να προσθέτονται και άλλοι. Αυτοί είναι:

- Μη νόμιμη χρήση δεδομένων: Ένας από τους κυριότερους κινδύνους είναι ότι μπορεί να γίνει μη νόμιμη χρήση των δεδομένων της ανατεθείσας βάσης. Σε αυτές τις περιπτώσεις η βάση μπορεί να αποσπασθεί και να πουληθεί ή τμήματα της βάσης με δεδομένα που έχουν συλλεχθεί από το νόμιμο ιδιοκτήτη να χρησιμοποιηθούν για εμπορικούς σκοπούς. Άμεσο αποτέλεσμα μιας τέτοιας μη νόμιμης χρήσης είναι να βλάπτεται η αγορά η οποία απευθύνεται ο νόμιμος ιδιοκτήτης για όλες τις υπηρεσίες και προϊόντα που αναφέρονται μέσα και σε άλλες περιπτώσεις θίγονται ευαίσθητα προσωπικά δεδομένα προσώπων τα οποία αναφέρονται.
- Μη-εξουσιοδοτημένη τροποποίηση των δεδομένων: Ο τρίτος μη έμπιστος φορέας που αναλαμβάνει την παροχή υπηρεσιών πληροφορικής μπορεί να προσθέσει νέα δεδομένα, να τροποποιήσει ή να διαγράψει δεδομένα από το σύστημα.
- Κίνδυνος από το απασχολούμενο προσωπικό και φυσική ανασφάλεια: Είναι πιθανό μεγάλο μέρος του προσωπικού του παρόχου των υπηρεσιών να υποκλέψουν χρήσιμες πληροφορίες για παράνομη χρήση. Παράλληλα επειδή οι τρίτοι φορείς διαχειρίζονται πολλές βάσεις, είναι δύσκολο αρκετές φορές οι υπηρεσίες που παρέχουν να προέρχονται από απόλυτα ασφαλές περιβάλλον.
- Απειλές λόγω πλαστοπροσωπίας: Η απάντηση σε ένα ερώτημα (query) που τίθεται στη βάση μπορεί και να μην είναι τα πλέον πρόσφατα, ή να μην να προέρχονται από τον εξυπηρετητή αλλά κάποια διαφορετική κακόβουλη πηγή.


Κατηγοριοποίηση Κινδύνων
1. Στρατηγικής Θέση Εταιρίας
2. Προϊόντα
3. Λεπτομέρειες για τη λειτουργία των προϊόντων
4. Δεδομένα Τρίτων
5. Νομικές Παραβάσεις
6. Επιθέσεις Υπεργολάβου
7. Εσωτερικές Επιθέσεις

Εικόνα 1

5.2. Απαιτήσεις ασφάλειας

Στο προηγούμενο κεφάλαιο παρουσιάσαμε τους κινδύνους που μπορεί να προκύψουν κατά την εμπλοκή τρίτων φορέων στην αξιοποίηση και διαχείριση δεδομένων. Κατόπιν λοιπόν της μελέτης των σημείων ευπάθειας (vulnerabilities) που παρουσιάζουν τα αγαθά–δεδομένα (assets), αποτιμώντας τους υφιστάμενους κινδύνους θα ορίσουμε τις απαιτήσεις ασφάλειας ώστε να οδηγηθούμε στο τι χρειάζεται να προστατευθεί και στη συνέχεια στο ποια είναι τα κατάλληλα τεχνικά και διαδικαστικά μέτρα ασφάλειας.

ΑΠΑΙΤΗΣΕΙΣ	
Εμπιστευτικότητα (Confidentiality)	Διαφύλαξη των προσωπικών ή ευαίσθητων δεδομένων ώστε οποιοσδήποτε μη εξουσιοδοτημένος χρήστης να μη μπορεί να έχει πρόσβαση σε έμπιστες πληροφορίες που περιλαμβάνουν τα δεδομένα που βρίσκονται στον εξυπηρετητή της τρίτης οντότητας.
Ακεραιότητα (Integrity)	Προστασία από την μη εξουσιοδοτημένη τροποποίηση των δεδομένων και λαθροχειρίας (tampering). Τα αποτελέσματα των ερωτημάτων που στέλνονται από τη τρίτη οντότητα θα πρέπει να είναι: α) σωστά (authenticity): τα δεδομένα δεν έχουν αλλαχθεί και β) πλήρη (completeness): δεν έχουν αφαιρεθεί έγκυρες πλειάδες από τα αποτελέσματα.
Ενημερωσιμότητα (Freshness)	Τα δεδομένα που διατίθενται στους νόμιμους χρήστες είναι τα πλέον ενημερωμένα.
Μη αποποίηση (non repudiation)	Καλύπτοντας ζητήματα απόδειξης μη – αποποίησης προέλευσης (origin) και αποστολής (submission), περιεχομένων (contents) που αποστέλλονται.

5.3. Ζητήματα που χρειάζονται προάσπιση

Τα βασικά ζητήματα για τα οποία θα πρέπει να λάβει κάποιος διαδικαστικά και τεχνικά μέτρα ασφάλειας, όπως προκύπτουν με βάση τις παραπάνω απαιτήσεις, ώστε να είναι σε θέση να εγγυάται την ασφάλεια των δεδομένων του κατά την ανάθεση σε τρίτους είναι:

Προστασία δεδομένων: Τα δεδομένα αποθηκεύονται σε εξωτερικούς εξυπηρετητές και υπόκεινται στον έλεγχο ατόμων τα οποία δεν είναι οι νόμιμοι ιδιοκτήτες τους. Εφόσον αυτά τα δεδομένα είναι ευαίσθητα κρίνεται απαραίτητη η κατάλληλη προστασία τους. Η προστασία αναφέρεται σε απειλές που προκύπτουν από τον εξυπηρετητή τον ίδιο καθώς όταν διαχειρίζεται και αποθηκεύει τη βάση δεν θα πρέπει να εξουσιοδοτείται να έχει πρόσβαση στα πραγματικά δεδομένα.

Εκτέλεση ερωτημάτων: Εφόσον τα ανατεθειμένα δεδομένα προστατεύονται και από τον ίδιο τον εξυπηρετητή θα πρέπει και για τα ερωτήματα των χρηστών να προστατεύονται δημιουργώντας ζητήματα όπως το πώς θα εκτελεσθούν ερωτήματα σε κρυπτογραφημένα ή κατακερματισμένα δεδομένα. Για παράδειγμα ας υποθέσουμε ότι ένας χρήστης έχει τη δυνατότητα εκτέλεσης ερωτημάτων σε ιατρικές βάσεις. Η πληροφορία ότι ένας χρήστης ενδιαφέρεται για μια συγκεκριμένη ασθένεια είναι αρκετό για να βγάλει κάποιος συμπεράσματα για ένα χρήστη ότι είτε αυτός είτε κάποιο κοντινό του πρόσωπο πάσχει από την ασθένεια.

Ιδιωτικότητας πρόσβασης: Η προστασία των δεδομένων που αναφέρθηκε παραπάνω δημιουργεί παράλληλα την ανάγκη προστασίας της εμπιστευτικότητας. Αύτο μπορεί να γίνει αποτρέποντας μη εξουσιοδοτημένη πρόσβαση στα προσωπικά δεδομένα.

Ακεραιότητα των δεδομένων και ορθότητα: Απαραίτητη κρίνεται η χρήση τεχνικών που θα επιβεβαιώνεται ότι τα δεδομένα που επιστρέφονται ως απάντηση σε αντίστοιχα ερωτήματα είναι ορθά και ακέραια δηλαδή να μην είναι δυνατή η μη νόμιμη τροποποίηση των δεδομένων.

Έλεγχος πρόσβασης: Στις περισσότερες βάσεις δεδομένων η πρόσβαση ανά χρήστη στα δεδομένα είναι διαφορετική ανάλογα με τα δικαιώματα του. Στη περίπτωση ανάθεσης όμως σε υπεργολάβους δημιουργούνται συγκεκριμένα προβλήματα και περιορισμοί. Υπάρχουν διαφορετικές επιλογές για την εφαρμογή των περιορισμών. Η πρώτη είναι να επιβάλλονται οι περιορισμοί από τον νόμιμο ιδιοκτήτη των δεδομένων, κάτι που όμως θα έκρινε απαραίτητη την μόνιμη παρουσία του ώστε να παρεμβαίνει σε κάθε ερώτημα και να ορίσει τα δικαιώματα σε κάθε χρήστη. Η άλλη είναι να ανατεθεί στον υπεργολάβο η εφαρμογή της πολιτικής εξουσιοδότησης κάτι το οποίο για λόγους ασφάλειας είναι αδύνατο καθώς θα απαιτούσε τη δημοσιοποίηση της πολιτικής εξουσιοδότησης στον πάροχο των υπηρεσιών. Η δημοσιοποίηση είναι αδύνατη καθώς εφόσον θεωρούμε ότι τα δεδομένα είναι ευαίσθητα το ίδιο ισχύει και για τη πολιτική που εφαρμόζεται. Επίσης είναι πολύ πιθανό οι περιορισμοί πρόσβασης να εφαρμόζονται ανάλογα με το περιεχόμενο των πραγματικών δεδομένων στα οποία ο υπεργολάβος δεν έχει εξορισμού πρόσβαση και τέλος αν ακόμα και αν ξεπεράσουμε τα προηγούμενα θα πρέπει ο υπεργολάβος να θεωρηθεί έμπιστος. Επομένως κρίνεται απαραίτητη η ανάπτυξη τεχνικών με αξιόπιστες διαδικασίες μέσα από τις οποίες να αποφευχθεί η συμμετοχή του νόμιμου ιδιοκτήτη των δεδομένων.

Δυνατότητα δικαιωμάτων εγγραφής: Είναι πιθανό ένας χρήστης να έχει δικαιώματα εγγραφής μόνο στα δεδομένα και όχι πρόσβασης στα υπόλοιπα δεδομένα.

Δημοσίευση και χρηστικότητα των δεδομένων: Η προστασία των δεδομένων είναι απαραίτητη και σε περιπτώσεις που τα δεδομένα δημοσιεύονται με διάφορους σκοπούς καθώς πρέπει να προστατευθούν τα ευαίσθητα δεδομένα. Επομένως στη προκειμένη περίπτωση της δημοσιοποίησης είναι απαραίτητο να ληφθούν υπόψη οι συσχετισμοί μεταξύ των δημοσιευθέντων δεδομένων και παράλληλα να διατηρείται η χρηστικότητα των δημοσιευθέντων δεδομένων. Ο όρος χρηστικότητα δεδομένων διαφοροποιείται ανάλογα με το είδος των δεδομένων ή την εφαρμογή. Δηλαδή ως χρηστικότητα μπορούμε να ορίσουμε ότι ορισμένοι συσχετισμοί μεταξύ των δεδομένων θα πρέπει να είναι διαθέσιμοι ώστε να είναι δυνατή η εκτέλεση ερωτημάτων στη βάση. Ας λάβουμε υπόψη το παράδειγμα της βάσης με τα ιατρικά

δεδομένα. Αν θεωρήσουμε ως δημοσιοποιήσιμα τα δεδομένα που αφορούν τη σχέση ασθενειών και εργασίας των ασθενών είναι προφανώς απαραίτητο αυτή η συσχέτιση να είναι δημοσίως διαθέσιμη. Αντίστοιχα σε περίπτωση που θεωρούμε δημοσιοποιήσιμα τα δεδομένα που αφορούν συσχετίσεις μεταξύ πόλεων και ασθενειών είναι απαραίτητο να δημοσιοποιήσουμε αυτή τη συσχέτιση και πιθανότατα να αποφύγουμε τη δημοσιοποίηση της προηγούμενης καθώς θα είναι εύκολη η παραβίαση της ιδιωτικότητας με όλη αυτή τη πληροφορία διαθέσιμη σε ένα επιτιθέμενο.[10]

6. Λύσεις

6.1. Φυσική και Λογική Ασφάλεια

Από τον πάροχο που θα αναλάβει τη διαχείριση των δεδομένων του οργανισμού θα απαιτήσουμε να λάβει μέτρα που αφορούν τη λογική και φυσική ασφάλεια. Αναφέροντας τον όρο φυσική ασφάλεια εννοούμε όλα τα τεχνικά και διαδικαστικά μέτρα που θα πρέπει να λάβει ο πάροχος ώστε να προστατευθούν τα συστήματα και οι υποδομές που διαχειρίζονται και διατηρούν τα δεδομένα, από κίνδυνους που προέρχονται από το περιβάλλον. Ως βασική προϋπόθεση για τη λήψη μέτρων ασφάλειας τίθεται η υλοποίηση ανάλυσης κινδύνων επειδή οι απαιτήσεις φυσικής ασφάλειας δε μπορεί να είναι ίδιες για όλες τις περιοχές και τούς χώρους που στεγάζουν συστήματα οι πάροχοι, ούτε και η κρισιμότητα των συστημάτων είναι η ίδια μέσα σε μια συγκεκριμένη περιοχή ή χώρο. Αναφέροντας τον όρο λογική ασφάλεια εννοούμε όλα τα τεχνικά και διαδικαστικά μέτρα που πρέπει να λαμβάνονται από τον πάροχο για τον περιορισμό της πρόσβασης στους πόρους των συστημάτων (system resources). Ως πόροι των συστημάτων θεωρούνται ο μηχανογραφικός εξοπλισμός, τα δίκτυα, το λογισμικό και τα δεδομένα που αναθέτει ο οργανισμός στον πάροχο ή αυτά τα οποία χρησιμοποιεί ο πάροχος ώστε να παρέχει τις ανατεθείσες υπηρεσίες. Τα μέτρα που θα ληφθούν ώστε να διασφαλιστεί η λογική ασφάλεια καθορίζουν όχι μόνον το «ποιος» ή «τι» (π.χ. πρόγραμμα) θα έχει πρόσβαση σε συγκεκριμένους πόρους του συστήματος, αλλά και το είδος της πρόσβασης που επιτρέπεται να έχει. Τα μέτρα αυτά μπορεί να είναι ενσωματωμένα στα λειτουργικά συστήματα, να υλοποιούνται σε προγράμματα εφαρμογών, σε συστήματα διαχείρισης βάσεων δεδομένων, σε συστήματα επικοινωνιών ή ακόμη να υλοποιούνται μέσω πρόσθετων αυτόνομων πακέτων ασφάλειας.

6.1.1. Βασικά μέτρα φυσικής ασφάλειας

Για να εξασφαλιστεί η φυσική ασφάλεια απαιτούνται τουλάχιστον:

- Μηχανισμοί ελέγχου φυσικής πρόσβασης (Physical Access Controls). Οι μηχανισμοί ελέγχου φυσικής πρόσβασης χρησιμοποιούνται ώστε να περιορίζουν, να ελέγχουν, να καταγράφουν την είσοδο και την έξοδο του προσωπικού και των επισκεπτών καθώς και τη διακίνησης μηχανογραφικού εξοπλισμού και αποθηκευτικών μέσων. Παράλληλα σε χώρους που στεγάζουν μηχανογραφικό εξοπλισμό, αλλά και οπουδήποτε υπάρχουν καλωδιώσεις που συνδέουν κρίσιμα συστήματα, υποστηρικτικές συσκευές (π.χ. μονάδες παροχής αδιάλειπτης τάσης, γεννήτριες), μαγνητικά μέσα στα οποία φυλάσσονται αρχεία, κλπ θα πρέπει να υπάρχουν μηχανισμοί ελέγχου φυσικής πρόσβασης. Το είδος των μηχανισμών ελέγχου που θα πρέπει να επιλέγονται από τον τρίτο πάροχο θα πρέπει να προσδιορίζονται ανάλογα από την κρισιμότητα των συστημάτων και την ευαισθησία των δεδομένων που καλούνται να προστατεύσουν.
- Μηχανισμοί πρόληψης και αντιμετώπισης καταστροφών από φυσικά αίτια (φωτιά, σεισμός ,πλημμύρα, κλπ). Τέτοιου είδους κίνδυνοι μπορεί να προκαλέσουν ολοσχερή καταστροφή των συστημάτων και των δικτύων.
- Μηχανισμοί πρόληψης και αντιμετώπισης κακόβουλων ενεργειών (διάρρηξη / κλοπή, βανδαλισμός, τρομοκρατική ενέργεια, κλπ). Τέτοιου είδους κίνδυνοι μπορεί να προκαλέσουν ολοσχερή καταστροφή των συστημάτων και των δικτύων.
- Μηχανισμοί πρόληψης και αντιμετώπισης προβλημάτων από διακοπή λειτουργίας και παροχής υπηρεσιών ή βλάβη υποστηρικτικών συσκευών. Για να παρέχετε η διαθεσιμότητα (availability) από τον τρίτο πάροχο τα συστήματα είναι απαραίτητο να λειτουργούν σε ένα αποτελεσματικά υποστηριζόμενο τεχνικά στο νόμιμο ιδιοκτήτη των δεδομένων.
- Αποτελεσματική διαχείριση της τηλεπικοινωνιακής και δικτυακής καλωδίωσης για την αντιμετώπιση θεμάτων φθοράς, παρεμβολών και έλλειψης κατάλληλης σήμανσης.
- Μηχανισμοί ασφάλειας φορητών συστημάτων. Η χρήση των φορητών υπολογιστών και οποιωνδήποτε άλλων φορητών συστημάτων θα πρέπει να λαμβάνεται σοβαρά υπόψη στην ανάλυση κινδύνων. Φορητοί υπολογιστές που αποθηκεύουν ευαίσθητα εταιρικά δεδομένα θα πρέπει, αφενός μεν να φυλάσσονται σε ασφαλή σημεία όταν δεν είναι σε χρήση, αφετέρου δε να αποθηκεύουν τα ευαίσθητα δεδομένα σε κρυπτογραφημένη μορφή.

- Η ασφαλής μεταφορά και αποθήκευση των ευαίσθητων εγγράφων και μαγνητικών μέσων. Ως ευαίσθητα έγγραφα μπορούμε να θεωρήσουμε: διαβαθμισμένες αναφορές, εφεδρικοί κωδικοί εισόδου των διαχειριστών συστημάτων, συνθηματικά των πελατών μέχρι να τους αποσταλούν, τεκμηρίωση των συστημάτων και εφαρμογών, Σχέδια Συνέχειας Εργασιών και Ανάκαμψης από Καταστροφή, κα. Στα μαγνητικά μέσα ανήκουν τα εφεδρικά αντίγραφα αρχείων, το πλαστικό υλικό των καρτών συναλλαγών κλπ

Με στόχο την ελαχιστοποίηση των προαναφερθέντων κινδύνων, η επιλογή και κατάλληλη διαμόρφωση των χώρων εξαρτώνται και προσδιορίζονται πάντοτε με τη χρήση για την οποία προορίζονται και την κρισιμότητα των συστημάτων που στεγάζουν.

6.1.2. Βασικά μέτρα λογικής ασφάλειας

Θέλοντας να ορίσουμε ένα αποδεκτό επίπεδο λογικής ασφαλείας, θα παραθέσουμε μια λίστα από βασικές οδηγίες ανά βασικές κατηγορίες ενός συστήματος. Σε ότι αφορά την ασφάλεια των προσβάσεων στα συστήματα που φυλάσσονται τα δεδομένα του οργανισμού απαιτούνται:

- Όλοι οι χρήστες να έχουν ένα μοναδικό ατομικό λογαριασμό πρόσβασης σε κάθε σύστημα και να έχουν πρόσβαση μόνο για τους πόρους που δικαιούνται πρόσβαση, ώστε κάθε ενέργεια των χρηστών να μπορεί να χρεωθεί μονοσήμαντα. Το προφανές συμπέρασμα του προηγούμενου είναι πως κοινοί – ομαδικοί λογαριασμοί πρόσβασης δεν θα πρέπει να χρησιμοποιούνται, και όπου αυτό δεν είναι εφικτό, θα πρέπει οι ενέργειες των κατόχων των λογαριασμών αυτών να καταγράφονται και να ελέγχονται σχολαστικά.
- Μέσα στον πάροχο των υπηρεσιών θα πρέπει να υπάρχουν καταγεγραμμένες και εγκεκριμένες διαδικασίες για τη διαχείριση των λογαριασμών πρόσβασης, τον καθορισμό και την αναθεώρηση των δικαιωμάτων που παρέχονται στον κάθε λογαριασμό για όλα τα στάδια της εργασιακής πορείας του ιδιοκτήτη του λογαριασμού (πρόσληψη, μετακίνηση, αλλαγή αντικειμένου εργασίας, αποχώρηση

κλπ). Να υπάρχει διαχωρισμός αρμοδιοτήτων στην έγκριση, υλοποίηση και έλεγχο των προσβάσεων.

- Θα πρέπει να πραγματοποιείται συστηματικός έλεγχος και καταγραφή των ενεργειών που γίνονται με χρήση λογαριασμών πρόσβασης που γίνονται με προνομιακά δικαιώματα όπως αυτά που έχουν οι διαχειριστές συστημάτων και άλλοι χρήστες με παρόμοια.
- Όταν ένας λογαριασμός δεν είναι πλέον απαραίτητος ή σε περίπτωση σημαντικής παραβίασης των κανόνων που έχει ορίσει ο πάροχος με το νόμιμο ιδιοκτήτη θα πρέπει να απενεργοποιείται άμεσα.
- Ο πάροχος θα πρέπει να ορίσει και να καταγράψει συγκεκριμένη διαδικασία που να δίνει τη δυνατότητα δημιουργίας προσωρινών λογαριασμών πρόσβασης, με καθορισμένο επίπεδο εξουσιοδοτήσεων, για συγκριμένες εργασίες ή για περιπτώσεις ανάγκης. Η χρήση των λογαριασμών αυτών θα πρέπει να ελέγχεται σχολαστικά, και μόλις εκλείψει η ανάγκη για την οποία δημιουργήθηκαν θα πρέπει να απενεργοποιούνται.
- Να πιστοποιείται ο ιδιοκτήτης ενός λογαριασμού πρόσβασης, κατά τη διαδικασία εισόδου του στο σύστημα μέσω μιας διαδικασίας υψηλής ασφάλειας (όπως π.χ. κωδικός εισόδου, χρήση «έξυπνης» κάρτας, ψηφιακού πιστοποιητικού κλπ) .
- Να αλλάζονται άμεσα οι κωδικοί πρόσβασης που έχουν τεθεί από τις κατασκευάστριες εταιρίες σε κάθε νέο τεχνολογικό εξοπλισμό μετά την παραλαβή του.
- Οι κωδικοί πρόσβασης:
  να δημιουργούνται και να γίνεται η διαχείρισή τους βάσει προτύπων και διαδικασιών
  να είναι δύσκολα προβλέψιμοι
  να διατηρούνται μυστικοί με ευθύνη των κατόχων τους
  να αλλάζουν σε τακτική βάση και οπωσδήποτε την πρώτη φορά εισόδου του κατόχου τους στο σύστημα. Η αλλαγή των κωδικών να επιβάλλεται από το σύστημα, και να κρατείται ιστορικό αλλαγών για την αποφυγή επανάληψης των ίδιων κωδικών, εφόσον αυτό είναι εφικτό.

- Οι εφεδρικοί κωδικοί των διαχειριστών συστημάτων ή λογαριασμών ειδικών προνομίων θα πρέπει να βρίσκονται αποθηκευμένοι σε ασφαλές σημείο, ώστε να

μπορούν να χρησιμοποιηθούν βάσει ειδικής διαδικασίας σε περίπτωση έκτακτης ανάγκης.

Όπου κρίνεται αναγκαίο, οι κωδικοί πρόσβασης λογαριασμών ειδικών προνομίων θα πρέπει να μη φυλάσσονται ενιαίοι, αλλά σε τμήματα με ευθύνη διαφορετικών ατόμων. Να χρησιμοποιείται – όπου είναι εφικτό – ειδικό λογισμικό διαχείρισης και ελέγχου των προσβάσεων.

Σε ότι αφορά την προστασία των δεδομένων κρίνονται απαραίτητα τα ακόλουθα:

- Να υπάρχουν επαρκείς ενσωματωμένοι μηχανισμοί ελέγχου (controls) των δεδομένων στα διάφορα συστήματα, και ειδικότερα, στην προετοιμασία, εισαγωγή, και επεξεργασία τους.
- Να υπάρχει καταγεγραμμένη και εγκεκριμένη διαβάθμιση των δεδομένων σύμφωνα με το βαθμό ευαισθησίας τους και να προβλέπονται επιπλέον διαδικασίες ασφάλειας των ευαίσθητων δεδομένων μέσω τεχνικών κρυπτογράφησης ή άλλων μεθόδων προστασίας.

Ότι αφορά τη κρυπτογράφηση απαραίτητο κρίνεται:

- Να καθορίζεται σαφώς το πότε και σε ποιο επίπεδο γίνεται κρυπτογράφηση.
- Να χρησιμοποιείται ικανοποιητικό μήκος κλειδιού σε όλο το λογισμικό.
- Να αναπτύσσεται στρατηγική υποδομής Δημόσιου Κλειδιού P.K.I. (public key infrastructure) για τη διαχείριση των ψηφιακών πιστοποιητικών, κυρίως για την επικοινωνία του ΠΙ με τους πελάτες του για παροχή υπηρεσιών ηλεκτρονικής τραπεζικής.
- Να επιδιώκεται η συμμόρφωση με τους εθνικούς και διεθνείς κανονισμούς και πρακτικές κρυπτογράφησης.
- Να γίνονται οι απαραίτητες ενέργειες για τη συμμόρφωση με τη σχετική νομοθεσία και τους κανονισμούς Προστασίας Δεδομένων.

Σε ότι αφορά τις βάσεις δεδομένων:

- Να υπάρχει ολοκληρωμένη και ακριβής τεκμηρίωση της βάσης που να περιλαμβάνει τουλάχιστον τον λογικό σχεδιασμό, τον φυσικό σχεδιασμό και το λεξικό δεδομένων.
- Να γίνεται αναδιοργάνωση της βάσης σε τακτά χρονικά διαστήματα.
- Να εξασφαλίζεται η καταχώρηση μόνο ολοκληρωμένων συναλλαγών (commit / rollback)

Σε ότι αφορά την προστασία των συστημάτων:

- Να υπάρχει εγκαταστημένο κατ' ελάχιστο στα κρίσιμα συστήματα, και όπου αλλού είναι αναγκαίο ειδικό λογισμικό προστασίας από ιούς ή άλλο «κακόβουλο» λογισμικό. Το λογισμικό προστασίας θα πρέπει να ενημερώνεται σε συνεχή βάση και να είναι εγκαταστημένο με τέτοιο τρόπο ώστε να ενεργοποιείται αυτόματα και να μην μπορεί να απενεργοποιηθεί από τους χρήστες των συστημάτων, παρά μόνο από τον αρμόδιο διαχειριστή.
- Να παρέχεται αποτελεσματική προστασία σε ευαίσθητους πόρους των συστημάτων, όπως τα αρχεία συστήματος και εφαρμογών.
- Να συντηρείται αρχείο με το εγκεκριμένο από το ΠΙ λογισμικό.
- Να απεγκαθίσταται ή να απενεργοποιείται σε κάθε σύστημα, κάθε λογισμικό ή λειτουργία που δεν κρίνεται απαραίτητη.
- Να ενεργοποιούνται τουλάχιστον οι βασικές λειτουργίες ελέγχου και καταγραφής (auditing & logging functions) σε κάθε σύστημα και να παραγοντοποιούνται κατάλληλα σε συνεργασία με τον εσωτερικό έλεγχο.
- Να εξασφαλίζεται όπου αυτό είναι αναγκαίο, κατόπιν σχετικής εγκριτικής διαδικασίας, η συνεχής ενημέρωση των συστημάτων με τις τελευταίες ενημερώσεις σε θέματα ασφάλειας, ώστε να ελαχιστοποιούνται οι αδυναμίες και τα τρωτά τους σημεία.
- Να υπάρχουν καταγεγραμμένες διαδικασίες αποκατάστασης της ασφαλούς λειτουργίας ενός συστήματος σε περίπτωση που παραβιαστεί η ασφάλειά του.

- Να υπάρχουν περιορισμοί στις ενέργειες των χρηστών του Διαδικτύου (π.χ. στις προσβάσεις σε συγκεκριμένους διαδικτυακούς τόπους, στη διακίνηση αρχείων κλπ).

- Να γίνεται συνεχής εκπαίδευση και ενημέρωση των χρηστών σε θέματα ασφαλούς λειτουργίας των συστημάτων.
- Να προστατεύονται αποτελεσματικά τα κρίσιμα συστήματα από κακόβουλες ενέργειες εξωτερικών ή εσωτερικών χρηστών. Προς αυτή την κατεύθυνση οφείλουν να υλοποιούνται διάφορες τεχνικές, όπως :

  Η χρήση ειδικών συστημάτων (firewalls, filtering routers κλπ), τα οποία, ως σημεία ελέγχου των προσβάσεων, θα ρυθμίζουν και θα ελέγχουν την επικοινωνία από και προς περιοχές του δικτύου οι οποίες είναι συνήθως εκτεθειμένες σε αυξημένους κινδύνους

  Η δημιουργία στο δίκτυο ειδικών περιοχών (Demilitarized Zones – DMZ), ανάμεσα σε σημεία ελέγχου προσβάσεων, οι οποίες να λειτουργούν σαν απομονωμένο δίκτυο για τα προσβάσιμα από εσωτερικούς ή εξωτερικούς χρήστες συστήματα του ΠΙ, προστατεύοντας έτσι αποτελεσματικά το υπόλοιπο δίκτυο από κακόβουλες ενέργειες

Σε ότι αφορά τη δικτυακή δομή των επικοινωνιών:

- Να είναι σαφώς καθορισμένες, καταγεγραμμένες και ελεγχόμενες οι δίοδοι επικοινωνίας (gateways) με εξωτερικά δίκτυα.
- Να εκτιμάται η δυνατότητα κατάτμησης (segmentation) του δικτύου σε ελεγχόμενα επί μέρους υποδίκτυα για τον καλύτερο έλεγχο των προσβάσεων.
- Να μην παραμένουν ανοιχτές λογικές θύρες επικοινωνίας (ports) σε κάθε συσκευή του δικτύου, επιπλέον όσων έχουν καθοριστεί σαφώς ως αναγκαίες για τις υπηρεσίες που υποστηρίζουν και αφού έχει συνεκτιμηθεί ο συνεπαγόμενος κίνδυνος από τη λειτουργία τους.
- Να περιορίζεται και να ελέγχεται επαρκώς η πρόσβαση στις ειδικές λειτουργίες διαχείρισης και ελέγχου του δικτύου.
- Να υπάρχει αποτελεσματική διαχείριση των παραμετροποιήσεων των συσκευών του δικτύου.
- Να υπάρχει η δυνατότητα εντοπισμού από το διαχειριστή του δικτύου λειτουργίας μη εξουσιοδοτημένων συσκευών.

- Να περιορίζονται στα απολύτως απαραίτητα τα σημεία πρόσβασης στο δίκτυο τα οποία βρίσκονται σε χώρους μη ελεγχόμενης φυσικής πρόσβασης, και εφόσον δε χρησιμοποιούνται να είναι ανενεργά.
- Να περιορίζεται και να ελέγχεται συστηματικά η δυνατότητα ασύρματης σύνδεσης χρηστών στο δίκτυο, ώστε να αποτρέπεται η παρείσφρηση μη εξουσιοδοτημένων χρηστών σε αυτό.
- Να μην παρέχεται η δυνατότητα απομακρυσμένης πρόσβασης στο δίκτυο, και όπου κρίνεται αναγκαία τέτοια πρόσβαση, να καταγράφεται και να ελέγχεται συστηματικά. Ειδικότερα, σε περίπτωση πρόσβασης στο δίκτυο χρηστών μέσω τηλεφωνικής σύνδεσης (dialup), αυτή να πραγματοποιείται κατόπιν διαδικασίας επιστροφής κλήσης (callback) ή άλλης κατάλληλης μεθόδου επαλήθευσης του καλούντος.
- Να χρησιμοποιούνται τα κατάλληλα πρωτόκολλα επικοινωνίας ανάλογα με το είδος των δεδομένων που μεταδίδονται, αντιμετωπίζοντας αποτελεσματικά θέματα διαχείρισης και ασφάλειάς τους.
- Να εξασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων που μεταδίδονται μέσω του δικτύου καθ’ όλη τη διαδρομή τους σε αυτό.
- Να γίνεται χρήση ειδικών εργαλείων λογισμικού για τον εντοπισμό κενών ασφαλείας ή σημείων μειωμένης ασφάλειας στο δίκτυο (vulnerability tests).
- Να υπάρχουν διαδικασίες και συστήματα παρακολούθησης, αποτροπής και αντιμετώπισης προσπαθειών παρείσφρησης στο δίκτυο ή γενικότερα προσπαθειών παραβίασης της ασφάλειας του δικτύου (intrusion detection/prevention systems).
- Να διενεργούνται σε τακτική βάση, από ειδικευμένες εταιρίες, δοκιμαστικές απόπειρες παραβίασης της ασφάλειας του δικτύου (penetration tests), βάσει καθορισμένων σεναρίων, με στόχο την αξιολόγηση της επάρκειας της ασφάλειας του δικτύου.
- Να υπάρχει μίσθωση γραμμής όπου αυτό κρίνεται αναγκαίο.

[27]

6.2. Ασφάλεια βάσης δεδομένων.

6.2.1. Βάση σαν υπηρεσία

Η πληροφορία είναι στην εποχή μας ο πιο σημαντικός και πολύτιμος πόρος. Ιδιωτικοί και δημόσιοι οργανισμοί συγκεντρώνουν μεγάλα ποσά δεδομένων τα οποία συλλέγονται και συντηρούνται, περιλαμβάνοντας συχνά ευαίσθητα προσωπικά δεδομένα. Σε τέτοιες περιπτώσεις όπως αναφέραμε σε προηγούμενα κεφάλαια η προστασία της ιδιωτικότητας των δεδομένων όταν αυτά αποθηκεύονται ή στέλνονται σε τρίτους μεταβάλλεται σε πρωτίστης σημασίας απαίτηση. Στη συνέχεια λοιπόν παρουσιάζουμε μια προτυποποίηση της όλης διαδικασίας της ανάθεσης της διαχείρισης των δεδομένων ενός οργανισμού σε τρίτους παρόχους.

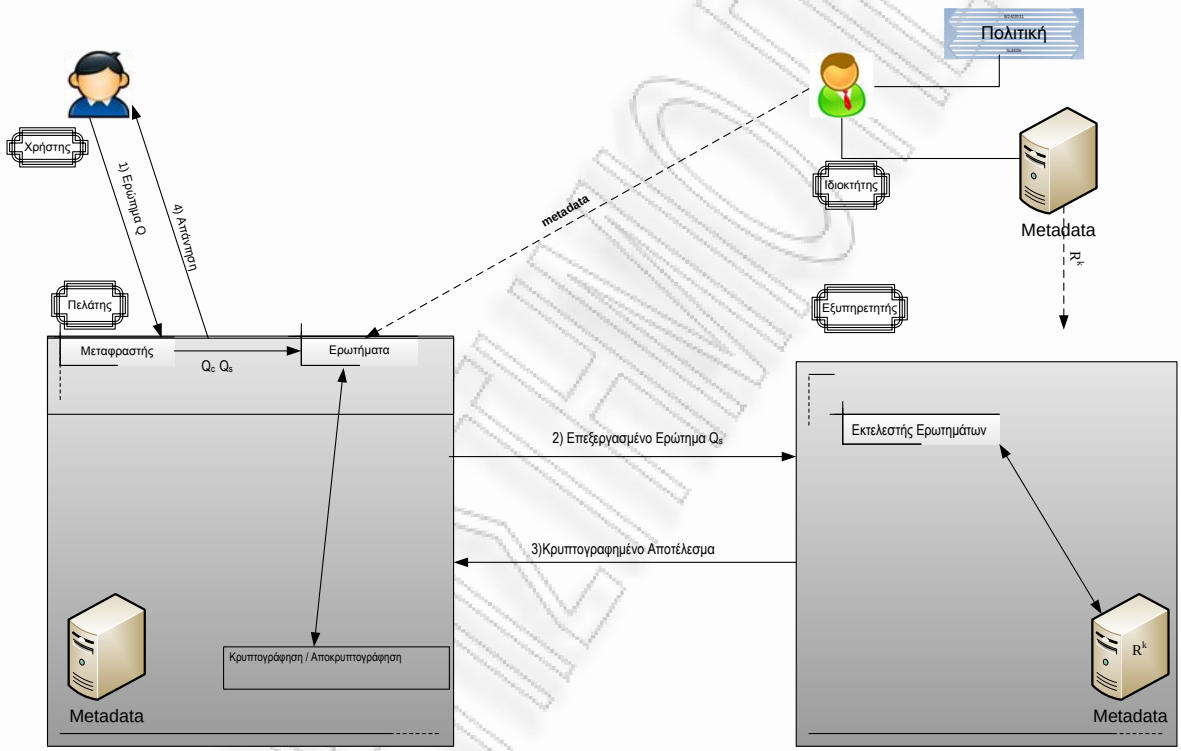
Το πρότυπο σενάριο που είναι εφαρμόσιμο σε όλους τους οργανισμούς οι οποίοι επιθυμούν έναν ασφαλή τρόπο για την ανάθεση των δεδομένων ονομάζεται Βάση Δεδομένων σαν Υπηρεσία (Database As A service – DAS). Η βασική ιδέα είναι ότι μια κρυπτογραφημένη βάση αποθηκεύεται σε έναν εξωτερικό εξυπηρετητή όπου κάθε πλειάδα συσχετίζεται με ένα δείκτη που αποτελεί μέσο αναγνώρισης.

Σε αυτή την ενότητα θα περιγράψουμε το βασικό πρότυπο σενάριο ξεκινώντας από τις βασικές οντότητες που συμμετέχουν, τις σχέσεις μεταξύ τους και στη συνέχεια περιγράφοντας τη χρήση των δεικτών στην όλη διαδικασία.

Το σενάριο της Βάσης Δεδομένων ως υπηρεσίας περιλαμβάνει τέσσερεις βασικές οντότητες:

- Χρήστης: Στέλνει ερωτήματα στον εξυπηρετητή. Ως χρήστες μπορούμε να θεωρήσουμε τους πελάτες του οργανισμού που χρησιμοποιούν δικτυακές υπηρεσίες και τους εργαζόμενους του οργανισμού που κάνει την ανάθεση στο πάροχο.

- Ιδιοκτήτης των Δεδομένων: Παράγει και αναθέτει πόρους σε τρίτους για να τα κάνει μερικώς διαθέσιμα.
- Πελάτης: Μετατρέπει τα ερωτήματα που στέλνονται από τους χρήστες σε ερωτήματα που αντιστοιχούν στη κρυπτογραφημένη βάση και αποκρυπτογραφεί τα αποτελέσματα.
- Εξυπηρετητής: Λαμβάνει κρυπτογραφημένα από τον ιδιοκτήτη των δεδομένων και τα διαθέτει στους χρήστες. (Υπεργολάβος-πάροχος υπηρεσιών)



Εικόνα 2-Μελέτη Περίπτωσης

Θέλοντας να δούμε πώς οργανώνονται τα δεδομένα ας υποθέσουμε από εδώ και πέρα ότι έχουμε μια σχεσιακή βάση δεδομένων όπου τα δεδομένα οργανώνονται σε πίνακες. Στη βάση αυτή σύμφωνα με το σενάριο θα εφαρμοσθεί συμμετρική ή ασύμμετρη κρυπτογραφία

ώστε τα δεδομένα να μην είναι διαθέσιμα στους υπεργολάβους. (η συμμετρική να είναι πιο δημοφιλής καθώς είναι οικονομικότερη). Η κρυπτογράφηση μπορεί να γίνει σε διάφορα επίπεδα διακριτότητας ανάλογα με τον τρόπο που συνηθίζουν οι χρήστες να προσπελαύνουν τα δεδομένα (οι χρηστές ζητούν πάντα ολόκληρη τη μισθοδοσία ενός οργανισμού και όχι ανά εργαζόμενο). Έτσι έχουμε:

- Σχέσης: κάθε σχέση κρυπτογραφείται με μια τιμή και έτσι ένας χρήστης δε μπορεί να θέσει ερωτήματα για πλειάδες και γνωρίσματα αλλά πάντα θα του επιστρέφεται ολόκληρος ο πίνακας.
- Γνωρίσματος: κάθε στήλη του πίνακα κρυπτογραφείται σα μία τιμή και για το χρήστη που θέτει ερωτήματα ισχύει ότι και παραπάνω, δηλαδή δε μπορεί να θέσει ερώτημα που να του επιστρέφει υποσύνολο της σχέσης αλλά μόνο στήλες του πίνακα.
- Πλειάδας: κάθε γραμμή ενός πίνακα κρυπτογραφείται χωριστά. Η πιο διαδεδομένη επιλογή και αυτή που θεωρούμε ότι εφαρμόζεται στο σενάριο.
- Στοιχείου: κάθε κελί κρυπτογραφείται. Επιφέρει μεγάλο φόρτο στη βάση.

Το προφανές συμπέρασμα των παραπάνω είναι ότι είναι απαραίτητος ο σχεδιασμός ενός μηχανισμού που να δίνει τη δυνατότητα στους χρήστες να στέλνουν ερωτήματα απευθείας στη κρυπτογραφημένη βάση. Το προηγούμενο ζήτημα έχει αποτελέσει επίκεντρο έρευνας για αρκετούς και οι περισσότερες λύσεις περιλαμβάνουν τη χρήση δεικτών.

Οι δείκτες χρησιμοποιούνται από τον εξυπηρετητή για να επιλέξει τα δεδομένα που θα στείλει ως απάντηση στο ερώτημα. Με άλλα λόγια , ας υποθέσουμε ότι έχουμε έναν εξυπηρετητή ο οποίος αποθηκεύει πίνακα με κρυπτογραφημένα δεδομένα καθώς και ένα δείκτη για κάθε γνώρισμα, όπου χρησιμοποιώντας τον μπορεί ο χρήστης να εκτελέσει ερωτήματα που περιλαμβάνουν συνθήκες. Κάθε σχέση στον μη κρυπτογραφημένο πίνακα αναπαρίσταται στην κρυπτογραφημένη βάση σα μια σχέση με ένα γνώρισμα που καθεμία αναπαριστά κρυπτογραφημένη πλειάδα με τόσους δείκτες όσα και τα γνωρίσματα (στήλες).

Τυπικά κάθε σχέση r_i σε πίνακα Ri(Ai1, Ai2, *: : :*, Ain) της μη κρυπτογραφημένης βάσης δεδομένων, μετατρέπεται σε σχέση $r_ι^κ$ σε πίνακα R_i^k (Count, Etuple, I1, I2, *: : :*, In) στη κρυπτογραφημένη βάση όπου:

- Count είναι το πρωτεύον κλειδί.
- Etuple είναι γνώρισμα για την κρυπτογραφημένη πλειάδα όπου οι τιμές του προκύπτουν με χρήση κρυπτογραφικής συνάρτησης Ek *(k*είναι το κλειδί κρυπτογράφησης).
- Ii είναι ο δείκτης που συσχετίζεται με το i_iγνώρισμα.

Για να γίνει κατανοητή η παραπάνω περιγραφή σας παραθέτω το ακόλουθο παράδειγμα: Ας θεωρήσουμε πως έχουμε ένα πίνακα ΜΑΘΗΤΩΝ όπως φαίνεται στην εικόνα 3α και αντίστοιχα τον κρυπτογραφημένο πίνακα ΜΑΘΗΤΩΝ^κ στην εικόνα 3β. Εύκολα παρατηρούμε ότι και οι δύο πίνακες έχουν τον ίδιο αριθμό γραμμών και ότι για κάθε γνώρισμα έχουμε ένα δείκτη. Επίσης διατηρείτε η ίδια σειρά μεταξύ των πινάκων όπως και το γνωρισμάτων. Για λόγους ασφάλειας σε πραγματικά παραδείγματα αυτή η σειρά δεν διατηρείται.

Id	**Όνομα**	**Τάξη**	**Μ.Ο. Βαθμολ.**
Α1	Ελένη	Α	13
Β1	Μαρία	Β	19
Α2	Κώστας	Α	17
Γ3	Σοφία	Γ	16

Εικόνα 3α

Counter	Etuple	I_1	I_2	I_3	I_4
1	Dfhgdfhgfdtrfdsghdgsasdzxcv9*7	π	A	γ	E
2	Hfgjdfhhjoqwi9uvknkmfdnro94uip?$(%	λ	ρ	γ	E
3	509tijotfijgjbiul43jer'kdhjvoutrhl	φ	γ	α	Π
4	Rk3[5i60ypijrfm9t54ik	β	δ	σ	A

Εικόνα 4β

Αφού εξηγήσαμε τη χρήση των δεικτών είμαστε σε θέση να εξηγήσουμε πλήρως τη διαδικασία με την οποία τίθεται ένα ερώτημα στη κρυπτογραφημένη βάση (όπως φαίνεται στην εικόνα 2).

1) Ο χρήστης θέτει το ερώτημα του αναφερόμενος στη μη κρυπτογραφημένη βάση R και το μεταφέρει στο πελάτη.

2) Ο πελάτης μετατρέπει το ερώτημα του χρήστη σε ισότιμο ερώτημα *Qs*, που σχετίζεται με τις συσχετίσεις της κρυπτογραφημένης βάσης όπως προκύπτουν από τους δείκτες και σε ένα ακόμα ερώτημα *Qc* που σχετίζεται με τα αποτελέσματα του *Qs*. Στη συνέχεια το ερώτημα *Qs* στέλνετε στον εξυπηρετητή.

3) Ο εξυπηρετητής εκτελεί το μετασχηματισμένο ερώτημα *Qs* στη κρυπτογραφημένη βάση και επιστρέφει το σύνολο των κρυπτογραφημένων πλειάδων στον πελάτη.

4) Ο πελάτης αποκρυπτογραφεί τις πλειάδες που του επέστρεψε ο εξυπηρετητής. Η μη κρυπτογραφημένη απάντηση επιστρέφεται στο χρήστη.[28]

6.2.2 Κατακερματισμός και κρυπτογραφία για προάσπιση της ιδιωτικότητας

Από τη σκοπιά της πρόσβασης των δεδομένων το DAS δεν είναι αποτελεσματικό καθώς η κρυπτογραφία δεν είναι αποτελεσματική πάντα στην εκτέλεση ερωτημάτων πάνω στα δεδομένα. Στη προσέγγιση που παρουσιάσαμε πριν όλα τα δεδομένα θεωρούνται ευαίσθητα και κρυπτογραφούνται. Αυτό όμως δεν ισχύει για όλα τα δεδομένα ενώ συνήθως οι συσχετισμοί μεταξύ τους είναι ευαίσθητοι. Για παράδειγμα σε ένα νοσοκομείο η λίστα με τις ασθένειες που θεραπεύτηκαν ή η λίστα με τους ασθενείς θα μπορούσε να είναι δημόσια διαθέσιμες ενώ ο συσχετισμός μεταξύ τους δε θα έπρεπε να είναι. Επομένως δεν κρίνεται αναγκαίο να κρυπτογραφηθούν και οι ασθένειες και οι ασθενείς αν υπάρχει ένας άλλος τρόπος να προστατευθεί ο συσχετισμός μεταξύ τους.

Μια προσέγγιση που θα μπορούσε να παρέχει προστασία στα ευαίσθητα δεδομένα ή σε ευαίσθητους συσχετισμούς είναι η χρήση κατακερματισμού (fragmentation) και κρυπτογραφίας. Η χρήση κατακερματισμού και κρυπτογραφίας σε συνδυασμό διαφυλάσσουν τη μη νόμιμη αποκάλυψη πληροφορίας.

Με την εφαρμογή αυτής της προσέγγισης τα δεδομένα μπορούν να ανατεθούν και να αποθηκευτούν σε μη έμπιστους εξυπηρετητές επιτυγχάνοντας χαμηλότερα κόστη, μεγαλύτερη διαθεσιμότητα και πιο αποτελεσματική κατανεμημένη πρόσβαση.

Η συνδυαστική χρήση της κρυπτογραφίας και της κατακερματισμού είχε προταθεί αρχικά στο [29] με τον περιορισμό ότι τα δεδομένα αποθηκεύονται σε δύο διαφορετικούς μη – επικοινωνούντες εξυπηρετητές

Σε αυτή τη προσέγγιση με βάση ισχύουσες προτάσεις θεωρούμε ότι τα δεδομένα που προστατεύονται αναπαριστούνται με μια σχέση r σε σχεσιακό σχήμα R(a1,. . . ,an), που περιλαμβάνουν όλες τις πληροφορίες που χρειάζονται προστασία. Θέλοντας να ορίσουμε

ορισμένες απαιτήσεις που πρέπει να εκπληρώνει η προσέγγιση για την εμπιστευτικότητα ορίζουμε:

- *A*: σύνολο γνωρισμάτων
- *c*: περιορισμός εμπιστευτικότητας πάνω στο *A* είναι
  - ένα υποσύνολο α $\subset A$, που περιλαμβάνει όλες τις πληροφορίες που είναι ευαίσθητες.
  - ένα υποσύνολό των γνωρισμάτων του *A*, που οι συσχετίσεις ανάμεσα στις τιμές είναι ευαίσθητες.

Στη συνέχεια παραθέτουμε ένα παράδειγμα τέτοιων περιορισμών

Αρ.Ταυτότητας	**Όνομα**	**Επάγγελμα**	**Ασθένεια**	**Τ.Κ.**
Φ049861	Ελένη Κωτσαντακάτου	Νοσοκόμα	Ίωση	12354
ΑΒ123876	Μαρία Γεωργίου	Νοσοκόμα	Καρκίνος	18743
Z5671093	Κώστας Παπαδόπουλος	Υπάλληλος	Τροφική Δηλητηρίαση	14378
Κ3791204	Σοφία Λεονταρίδου	Δικηγόρος	Πνευμονία	19032
Γ27102363	Σάββας Κώνστας	Αρχιτέκτονας	HIV	14323

Πίνακας 1

Οι περιορισμοί που μπορούμε να ορίσουμε είναι

1. c0=Αρ.Ταυτότητας
2. c1= Όνομα, Επάγγελμα
3. c2= Όνομα, Ασθένεια
4. c3= Επάγγελμα, Ασθένεια, Τ.Κ.

Τις απαιτήσεις εμπιστευτικότητας που μπορεί να οριστούν σε κάθε σχεσιακή βάση τις καλύπτουν πλήρως ο συνδυασμός της κρυπτογραφίας και του κατακερματισμού. Η κρυπτογραφία εφαρμόζεται σε επίπεδο γνωρίσματος. Το προηγούμενο σημαίνει ότι

κρυπτογραφούνται ανά πλειάδα όλες οι τιμές, προστατευόμενοι παράλληλα από επιθέσεις συχνότητας. Από την άλλη πλευρά ο κατακερματισμός εφαρμόζεται σε σύνολα γνωρισμάτων ώστε να μην είναι ορατά μαζί για να μην είναι διαθέσιμοι οι συσχετισμοί με τα κλειδιά κρυπτογράφησης.

Ουσιαστικά οι περιορισμοί που αφορούν τα γνωρίσματα μπορούν να επιλυθούν μόνο με κρυπτογραφία. Από την άλλη πλευρά οι περιορισμοί που αφορούν τις σχέσεις μεταξύ των γνωρισμάτων μπορούν να επιτευχθούν είτε με: 1)κρυπτογράφηση των γνωρισμάτων που περιλαμβάνονται μέσα στη σχέση είτε με 2) κατακερματισμός των γνωρισμάτων που περιλαμβάνονται στο περιορισμό ώστε να μην είναι ορατά μαζί.

Δοθείσας σχέσης r σε σχήμα R και ενός συνόλου περιορισμών C πάνω σε αυτί, στόχος μας είναι να διασπάσουμε την R παρέχοντας εγγυήσεις για την ικανοποίηση των περιορισμών. Επίσης θα πρέπει να παρέχονται εγγυήσεις ότι κανένας περιορισμός δεν πρέπει να παραβιάζεται αν επανασυνδυαστούν δύο ή περισσότερα τμήματα. Εφόσον η κρυπτογραφία διαφοροποιείται με τη χρήση των επιπλέον χαρακτήρων προκύπτει ότι τα τμήματα προστατεύονται από επιθέσεις επανασύνδεσης αν πληρούν την προϋπόθεση να εμφανίζονται μια μόνο φορά σε καθαρό κείμενο σε όλα τα διασπασμένη τμήματα.

Ορισμός: Κατακερματισμός σε σχεσιακό σχήμα R είναι ένα σύνολο τμημάτων F = {F1, . . . ,Fm},όπου Fi⊆*R*, για i = 1, . . . ,m

- Κάθε τμήμα ***F*** πάνω στο R επιβάλλει σωστά ένα σύνολο περιορισμών εμπιστευτικότητας C αν ικανοποιούνται οι ακόλουθες συνθήκες:
  - ∀ F∈*F*, ∀*c*∈C⊆*F*(κάθε διάσπαση ικανοποιεί έναν ή περισσότερους περιορισμούς)
  - ∀ *Fi*,*Fj*∈*F*, *i*≠*j*: *Fi*∩*Fj*= 0(οι διασπάσεις δεν έχουν κοινά γνωρίσματα)

- Κάθε τμήμα ***F*** σχετίζεται με μια «φυσική» διάσπαση που περιλαμβάνει
  - όλα τα γνωρίσματα του F σε ακρυπτογράφητο κείμενο

◦ όλα τα άλλα γνωρίσματα του R κρυπτογραφημένα (μια σειρά τυχαίων χαρακτήρων προστίθεται σε κάθε κρυπτογράφημα-salt)[28]

Ας δούμε για παράδειγμά ποια θα ήταν τα τμήματα που θα ορίζαμε στο πίνακα που παρουσιάσαμε παραπάνω (Πίνακας 1) λαμβάνοντας υπόψη τους περιορισμούς που ορίσαμε.

Salt	enc	Όνομα
s1	**α**	Ελένη Κωτσαντακάτου
s2	**β**	Μαρία Γεωργίου
s3	**γ**	Κώστας Παπαδόπουλος
s4	**δ**	Σοφία Λεονταρίδου
s5	**ε**	Σάββας Κώνστας

f1

Πίνακας 2α

salt	enc	Επάγγελμα
s6	**ζ**	Νοσοκόμα
η	**η**	Νοσοκόμα
s8	**θ**	Υπάλληλος
s9	**ι**	Δικηγόρος
s10	**κ**	Αρχιτέκτονας

f2

Πίνακας 2β

salt	enc	Ασθένεια	Τ.Κ.
s1	**α**	Ίωση	12354
s2	**β**	Καρκίνος	18743
s3	**γ**	Τροφική Δηλητηρίαση	14378

s4	**δ**	Πνευμονία	19032
s5	**Ε**	HIV	14323

f3

Πίνακας 3γ

6.3 Λύση για την μη αποποίηση και εγκυρότητα.

Για την αποτροπή της αποποίησης ευθύνης κατά την διάρκεια ανταλλαγής ηλεκτρονικών μηνυμάτων έχει προταθεί κυρίως η χρήση των ψηφιακών πιστοποιητικών. Με την χρήση των ψηφιακών υπογραφών ο κάτοχος του ιδιωτικού κλειδιού δεν μπορεί να αρνηθεί την αποστολή ή παραλαβή ενός μηνύματος δεδομένο ότι είναι ο μοναδικός χρήστης και κάτοχος του πιστοποιητικού. Εκτός από την γενικά αποδεκτή λύση της χρήσης των ψηφιακών υπογραφών στη βιβλιογραφία συναντάμε και άλλες προτάσεις. Συγκεκριμένα η χρήση μισθωμένων γραμμών και οι διαδικασίες καταγραφής αποστολής και παραλαβής μηνυμάτων από συγκεκριμένο τερματικό με παράλληλα την φυσική προστασία αυτού.

Επιπλέον στα πλαίσια των ευρωπαϊκών ερευνητικών προγραμμάτων με την συμμετοχή και Ελληνικών Πανεπιστήμιων (Πανεπιστήμιο Πειραιά) έχουν αναπτυχθεί αντίστοιχες διαδικασίες μη αποποίησης με την χρήση τεχνολογιών που βασίζονται στην XML.(π.χ. ηλεκτρονική τιμολόγηση). Παράλληλα με την υλοποίηση λογισμικού ως τρόπου αντιμετώπισης της μη αποποίησης, έχουμε αρκετές φορές συναντήσει και πολύ αξιόλογες προτάσεις hardware, οι οποίες είναι αποτελεσματικές και συχνά αποτελούν τελικές λύσεις σε περιπτώσεις που οι εμπλεκόμενοι είναι ένας περιορισμένος αριθμός χρηστών.

Για είναι σίγουρο πώς τα δεδομένα δεν έχουν τροποποιηθεί και είναι τα πλέον έγκυρα θα μπορούσε να χρησιμοποιήσουμε τη λύση της HashFunction.. Η συνάρτηση αυτή κρυπτογραφεί κάποιο απλό κείμενο οποιουδήποτε μεγέθους εφαρμόζοντας σε αυτό ένα μαθηματικό μετασχηματισμό και προκύπτει το κρυπτογραφημένο μήνυμα το οποίο έχει

σταθερό μέγεθος, hashvalue. Το κρυπτογράφημα θεωρείται ως μια σύντομη και περιεκτική αναπαράσταση του απλού κειμένου από το οποίο παράχθηκε. Το κρυπτογράφημα συνοδεύει το μήνυμα από το οποίο παράχθηκε και χρησιμοποιείται για επιβεβαίωση της αυθεντικότητας και της εγκυρότητας του μηνύματος που συνοδεύει και την μη αλλοίωσή του κατά τη μεταφορά του.

7. Συμπεράσματα

Η επιλογή της ανάθεσης μέρος των εργασιών σε τρίτους από επιχειρήσεις ή οργανισμούς στο τομέα των πληροφορικών συστημάτων αναμένεται να αυξηθεί σημαντικά στα επόμενα χρόνια. Οι βασικότερο λόγοι είναι δύο. Ο πρώτος είναι η ανάπτυξη συστημάτων και τεχνολογιών που πλέον κάνουν σαφώς ευκολότερη τη διαδικασία της ανάθεσης και δεύτερον γιατί η εξειδίκευση σε όλους τους τομείς, που μια εξωτερική οντότητα μπορεί να παρέχει σε κάθε οργανισμό, κερδίζει ολοένα και περισσότερο έδαφος. Επιπλέον η ανάγκη για συνεχή αναβάθμιση και εκσυγχρονισμό τόσο των υπηρεσιών όσο και του εξοπλισμού των εταιριών αποτελούν ένα επιπλέον παράγοντα για την ανάθεση εργασιών σε τρίτους. Ο προφανής λόγος είναι η εξοικονόμηση πόρων και η ελαχιστοποίηση του κόστους με παράλληλη αύξηση της απόδοσης και των παρεχόμενων υπηρεσιών.

Αρκετά ζητήματα που χρήζουν προσοχής και ενέχουν κινδύνους που προκύπτουν από την εξωτερική ανάθεση, δεν έχουν αντιμετωπιστεί και σε αρκετές περιπτώσεις δεν έχουν καν εντοπιστεί ως αδυναμίες. Ένα από τα σημαντικότερα ζητήματα είναι και το θέμα που πραγματεύεται η συγκεκριμένη εργασία. Η ασφάλειας των πληροφοριών και ειδικότερα ο τομέας της ιδιωτικότητας των δεδομένων είναι ένα από τα παραπάνω ζητήματα. Ο τομέας της ιδιωτικότητας των δεδομένων στην περίπτωση της ανάθεσης σε τρίτους μέρος εργασιών που συμπεριλαμβάνει και την διαχείριση δεδομένων δεν είναι όμοια με την πλειοψηφία των περιπτώσεων ασφάλειας πληροφορικών συστημάτων και απαιτεί ιδιαίτερη μελέτη. Η επιστημονική βιβλιογραφία έχει εντοπίσει το μέγεθος του προβλήματος και αρκετές μελέτες έχουν υλοποιηθεί για την ανάδειξη του ζητήματος. Οι προτεινόμενες λύσεις όμως ως τώρα βασίζονται είτε σε εξειδικευμένες περιπτώσεις είτε σε μία γενική άποψη με βάση την ευρύτερη περιοχή της ασφάλεια των πληροφορικών και επικοινωνιακών συστημάτων.

Σε αντίθεση με το νομικό πλαίσιο που έχει αναπτυχθεί για την προστασία των προσωπικών δεδομένων τόσο από την Ευρωπαϊκή Ένωση όσο και από την Ελληνική

νομοθεσία το οποίο περιγράφει αναλυτικά τις υποχρεώσεις των οργανισμών που διαχειρίζονται προσωπικά δεδομένα, το αντίστοιχο τεχνολογικό πλαίσιο είναι αρκετά δύσκολο να υλοποιηθεί λόγω της φύσης των δεδομένων κατά την ανάθεση εργασιών σε τρίτους.

Στις περιπτώσεις όπου η τεχνολογία \ δεν μπορεί να δώσει τις απαραίτητες εγγυήσεις για την εξασφάλιση της ιδιωτικότητας των δεδομένων συχνά συναντάμε την αυστηρή συγγραφή συμβολαίων μεταξύ των εταιριών που διαχειρίζονται τα δεδομένα. Θα πρέπει όμως να αναλογιστούμε ότι η ύπαρξη συμβολαίων εχεμύθειας και εμπιστευτικότητας απλώς κάνουν πιο δύσκολη την διαρροή πληροφοριών χωρίς να την αποκλείουν.

Ο χώρος της ιδιωτικότητας κατά την ανάθεση έργων πληροφορικής σε τρίτους και η διαχείριση ευαίσθητων δεδομένων θα πρέπει να αναπτύξει ισχυρές τεχνολογικές και όχι μόνο λύσεις προσανατολισμένες στην προστασία των δεδομένων που διαχειρίζονται οι οργανισμοί ή επιχειρήσεις ανεξάρτητα από την θέση τους προκειμένου να μπορεί να αναπτυχθεί περαιτέρω και να προσφέρει σημαντικά οφέλη στην ανάπτυξη των πληροφοριακών συστημάτων.

8. Πρακτική Εφαρμογή

Στα πλαίσια της παρούσας διπλωματικής εργασίας υλοποιήθηκε μια εφαρμογή σχετικά με την εξασφάλιση της ιδιωτικότητας κατά την ανάθεση σε τρίτους. Η υλοποίησης αφορά την περίπτωση ανάθεσης δεδομένων τραπεζικού ομίλου σε τρίτο πάροχο είτε για πλήρες hostingείτε για περιπτώσεις σχεδίων ανάκαμψης από καταστροφή, είτε για λόγους δημιουργίας αναφορών (month client reports etc.)

Η εφαρμογή λοιπόν εφαρμόζει κρυπτογραφία στα ευαίσθητα προσωπικά δεδομένα ή σε όσα μπορεί να οδηγήσουν σε προσδιορισμό του πραγματικού πρόσωπου εξασφαλίζοντας την ιδιωτικότητα των πελατών της τράπεζας. Θεωρήθηκε λοιπόν ότι θα έχουμε δύο διαφορετικούς εξυπηρετητές. Έναν εντός του οργανισμού που μοναδικός του ρόλος είναι να διατηρεί τα κρυπτογραφικά κλειδιά, να εφαρμόζει κρυπτογραφία και να αποκρυπτογραφεί τα δεδομένα και τα διαθέτει στη βασική εφαρμογή που χρησιμοποιεί το προσωπικό του εκάστοτε οργανισμού. Ο δεύτερος είναι αυτός που διαθέτει ο πάροχος όπου αποθηκεύονται τα δεδομένα και στέλνονται κρυπτογραφημένα όταν αυτά ζητούνται μέσω ασφαλών μισθωμένων καναλιών στον οργανισμό.

Οι τεχνολογίες και εργαλεία που χρησιμοποιήθηκαν στα πλαίσια της υλοποίησης είναι:

- Microsoft Virtual PC
- Microsoft Server 2003
- Microsoft SQL Server 2008
- .net Framework 4.0
- Visual Studio 2010
- Asp C# .net
- T-SQL

Όπως αναφέρθηκε παραπάνω έχουμε δύο εξυπηρετητές και άρα δύο βάσεις δεδομένων που επικοινωνούν μεταξύ τους μια στο καθένα. Ας δούμε λίγο αναλυτικά επομένως τη κάθε βάση και το κώδικα που γράφτηκε σε T-SQL και στη συνέχεια την εφαρμογή που εμφανίζεται στο τελικό χρήστη.

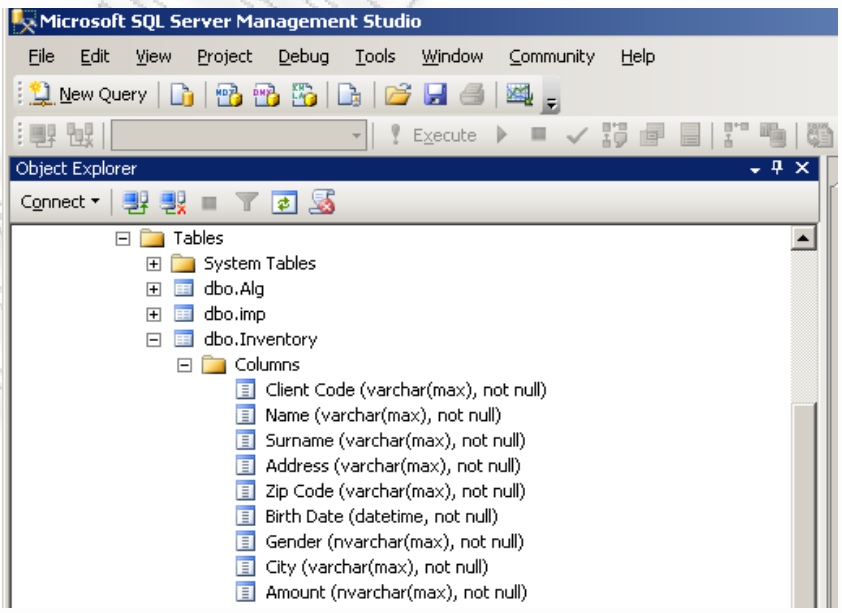
Η βάση αυτή ονομάζεται TRXκαι δημιουργήθηκε με το εξής query:

```
USE [master]
GO
/****** Object:  Database [TRX]    Script Date: 08/04/2011 13:38:03 ******/
CREATE DATABASE [TRX] ON  PRIMARY
( NAME = N'TRX', FILENAME = N'C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA\TRX.mdf' , SIZE = 3072KB , MAXSIZE = UNLIMITED, FILEGROWTH = 1024KB )
 LOG ON
( NAME = N'TRX_log', FILENAME = N'C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA\TRX_log.ldf' , SIZE = 1024KB , MAXSIZE = 2048GB , FILEGROWTH = 10%)
GO
ALTER DATABASE [TRX] SET COMPATIBILITY_LEVEL = 100
GO
IF (1 = FULLTEXTSERVICEPROPERTY('IsFullTextInstalled'))
begin
EXEC [TRX].[dbo].[sp_fulltext_database] @action = 'enable'
end
GO
ALTER DATABASE [TRX] SET ANSI_NULL_DEFAULT OFF
GO
ALTER DATABASE [TRX] SET ANSI_NULLS OFF
GO
ALTER DATABASE [TRX] SET ANSI_PADDING OFF
GO
ALTER DATABASE [TRX] SET ANSI_WARNINGS OFF
GO
ALTER DATABASE [TRX] SET ARITHABORT OFF
```

```
GO
ALTER DATABASE [TRX] SET AUTO_CLOSE OFF
GO
ALTER DATABASE [TRX] SET AUTO_CREATE_STATISTICS ON
GO
ALTER DATABASE [TRX] SET AUTO_SHRINK OFF
GO
ALTER DATABASE [TRX] SET AUTO_UPDATE_STATISTICS ON
GO
ALTER DATABASE [TRX] SET CURSOR_CLOSE_ON_COMMIT OFF
GO
ALTER DATABASE [TRX] SET CURSOR_DEFAULT  GLOBAL
GO
ALTER DATABASE [TRX] SET CONCAT_NULL_YIELDS_NULL OFF
GO
ALTER DATABASE [TRX] SET NUMERIC_ROUNDABORT OFF
GO
ALTER DATABASE [TRX] SET QUOTED_IDENTIFIER OFF
GO
ALTER DATABASE [TRX] SET RECURSIVE_TRIGGERS OFF
GO
ALTER DATABASE [TRX] SET  DISABLE_BROKER
GO
ALTER DATABASE [TRX] SET AUTO_UPDATE_STATISTICS_ASYNC OFF
GO
ALTER DATABASE [TRX] SET DATE_CORRELATION_OPTIMIZATION OFF
GO
ALTER DATABASE [TRX] SET TRUSTWORTHY OFF
GO
ALTER DATABASE [TRX] SET ALLOW_SNAPSHOT_ISOLATION OFF
GO
ALTER DATABASE [TRX] SET PARAMETERIZATION SIMPLE
GO
```

```
ALTER DATABASE [TRX] SET READ_COMMITTED_SNAPSHOT OFF
GO
ALTER DATABASE [TRX] SET HONOR_BROKER_PRIORITY OFF
GO
ALTER DATABASE [TRX] SET  READ_WRITE
GO
ALTER DATABASE [TRX] SET RECOVERY FULL
GO
ALTER DATABASE [TRX] SET  MULTI_USER
GO
ALTER DATABASE [TRX] SET PAGE_VERIFY CHECKSUM
GO
ALTER DATABASE [TRX] SET DB_CHAINING OFF
GO
```

Μέσα σε αυτή τη βάση φτιάχτηκε ένας πίνακας δειγματοληπτικά όπου αποθηκεύονται βασικά δεδομένα των πελατών. Ο πίνακας αυτός έχει την ακόλουθη δομή:



Και δημιουργήθηκε με το εξής query:

```
USE [TRX]
GO
/****** Object:  Table [dbo].[Inventory]    Script Date: 8/05/2011 16:23:21 ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
SET ANSI_PADDING OFF
GO
CREATE TABLE [dbo].[Inventory](
	[Client Code] [varchar](max) NOT NULL,
	[Name] [varchar](max) NOT NULL,
	[Surname] [varchar](max) NOT NULL,
	[Address] [varchar](max) NOT NULL,
	[Zip Code] [varchar](max) NOT NULL,
	[Birth Date] [datetime] NOT NULL,
	[Gender] [nvarchar](max) NOT NULL,
	[City] [varchar](max) NOT NULL,
	[Amount] [nvarchar](max) NOT NULL
) ON [PRIMARY]
GO
SET ANSI_PADDING OFF
GO
```

Πάνω σε αυτό το πίνακα δημιουργήθηκε ένα triggerόπου κάθε φορά που μέσα από την εξωτερική εφαρμογή πάει να γίνει εισαγωγή ή αλλαγή σε ένα πελάτη τα δεδομένα αυτά εισάγονται κρυπτογραφημένα στον εξυπηρετητή του παρόχου. Το trigger αυτό θα μπορούσε να τροποποιηθεί κατάλληλα ώστε να εισάγονται και στους 2 ανάλογα με την συμφωνία με το πάροχο και τη χρήση του παρόχου.

```
USE [TRX]
GO
/****** Object:  Trigger [dbo].[IT1]    Script Date: 10/05/2011 16:27:23 ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
create trigger [dbo].[IT1] on [dbo].[Inventory]
instead of insert
as begin
declare @typeofkeyvarchar(255)
select @typeofkey=Typeofkey from dbo.Alg
if @typeofkey='AsymKey'
begin
insert into Trxoutsourced.dbo.ENCRINVENTORY([Client Code],
            [Name],
            [Surname],
            [Address],
            [Zip Code] ,
            [Birth Date],
            [Gender] ,
            [City],
            [Amount])
            SELECT [Client Code],
            encryptbyasymkey(Asymkey_ID('Asymkey'),Name),
            encryptbyasymkey(Asymkey_ID('Asymkey'),SurName),
            encryptbyasymkey(Asymkey_ID('Asymkey'),[Address]),
            [Zip Code],
            [Birth Date],
            [Gender] ,
            [City],
            [Amount]
            from inserted
```

```
end
if @typeofkey='SymKey'
begin
OPEN SYMMETRIC KEY Asymkey DECRYPTION
BY CERTIFICATE EncryptTestCert
insert into Trxoutsourced.dbo.ENCRINVENTORY([Client Code],
            [Name],
            [Surname],
            [Address],
            [Zip Code] ,
            [BirthDate],
            [Gender] ,
            [City],
            [Amount])
            SELECT [Client Code],
            encryptbykey(KEY_GUID('Asymkey'),Name),
            encryptbykey(KEY_GUID('Asymkey'),SurName),
            encryptbykey(KEY_GUID('Asymkey'),[Address]),
            [Zip Code],
            [Birth Date],
            [Gender] ,
            [City],
            [Amount]
            from inserted
end
end
```

Στα πλαίσια της κρυπτογράφησης των δεδομένων αξιοποιώντας τις δυνατότητες του SQL Server αφού κατασκευάζουμε κάθε φορά τα απαιτούμενα κλειδιά. Αντίστοιχοι πίνακες έχουν φτιαχτεί στον εξυπηρετητή του παρόχου όπου η βάση του ονομάζεται TRXOutsourced.

Η εξωτερική εφαρμογή που χρησιμοποιούν οι υπάλληλοι και οι IT administrators δίνει δυνατότητα κρυπτογραφημένης εισαγωγής, αναζήτησης σε κρυπτογραφημένα δεδομένα, αποκρυπτογράφησης και κρυπτογράφησης με διαφορετικό αλγόριθμο. Οι αλγόριθμοι που έχουν εφαρμοστεί είναι:

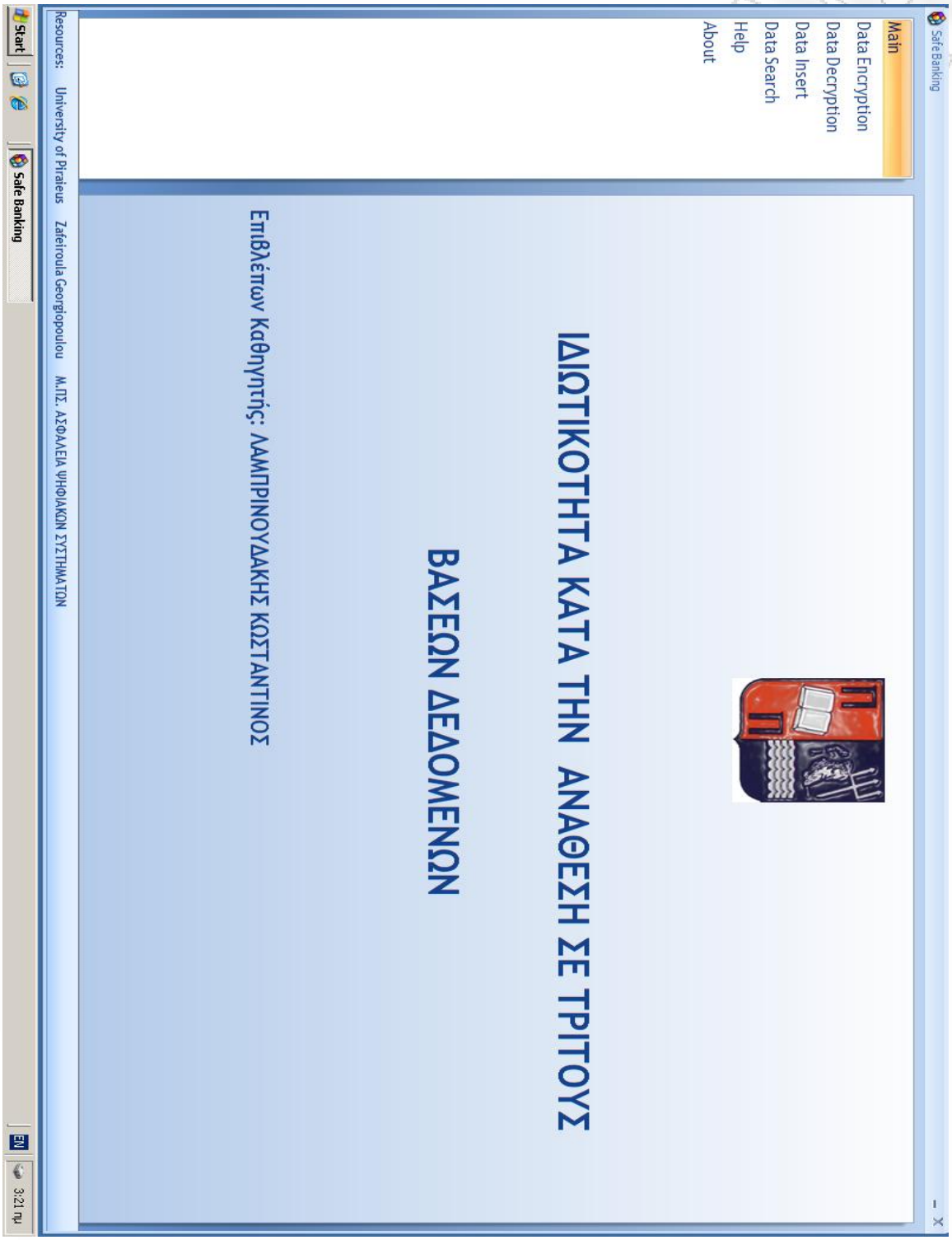
1. DES
2. TRIPLE_DES
3. RC2
4. RC4
5. RC4_128
6. DESX
7. AES_128
8. AES_192
9. AES_256
10. RSA_512
11. RSA_1024
12. RSA_2048

Στη βάση κατασκευάσαμε ένα masterkey και ένα πιστοποιητικό (x509) ως εξής και στη συνέχεια κάθε φορά που αλλάζει ο αλγόριθμος δημιουργούνται συμμετρικά και ασύμμετρα κλειδιά ως εξής:

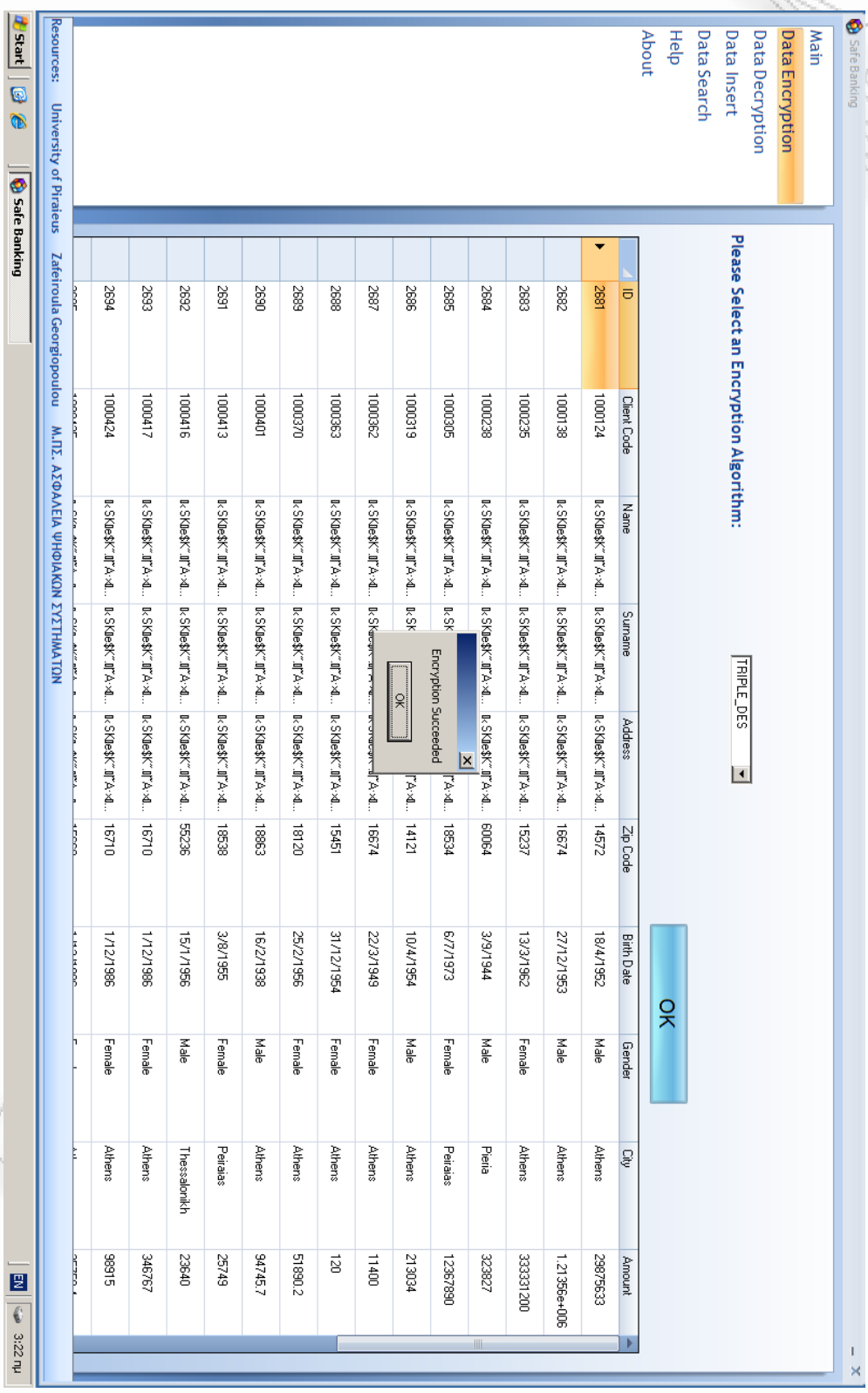
```
CREATE MASTER KEY ENCRYPTION
BY PASSWORD = 'SQLAuthority'
GO

CREATE CERTIFICATE EncryptTestCert
WITH SUBJECT = 'SQLAuthority'
GO

create asymmetric key AsymKey With Algorithm =encryptionalgorithm

create symmetric key AsymKey With Algorithm =encryptionalgorithm ENCRYPTION BY CERTIFICATE EncryptTestCert'
```

Η τελική εφαρμογή που θα χρησιμοποιούν οι πελάτες και υλοποιήθηκε δίνει δυνατότητα στους εργαζόμενους και στους IT administrator,της εκάστοτε τράπεζας, εισαγωγής κρυπτογραφημένων δεδομένων στη βάση του παρόχου, αναζήτησης σε κρυπτογραφημένα δεδομένα, κρυπτογράφησης με αλγορίθμους που αναφέραμε παραπάνω και αποκρυπτογράφησης. Ακολουθούν ορισμένα print screens. Παράλληλα μέρος της διπλωματικής είναι ο κώδικας και η εφαρμογή σε συνοδευτικό CD.

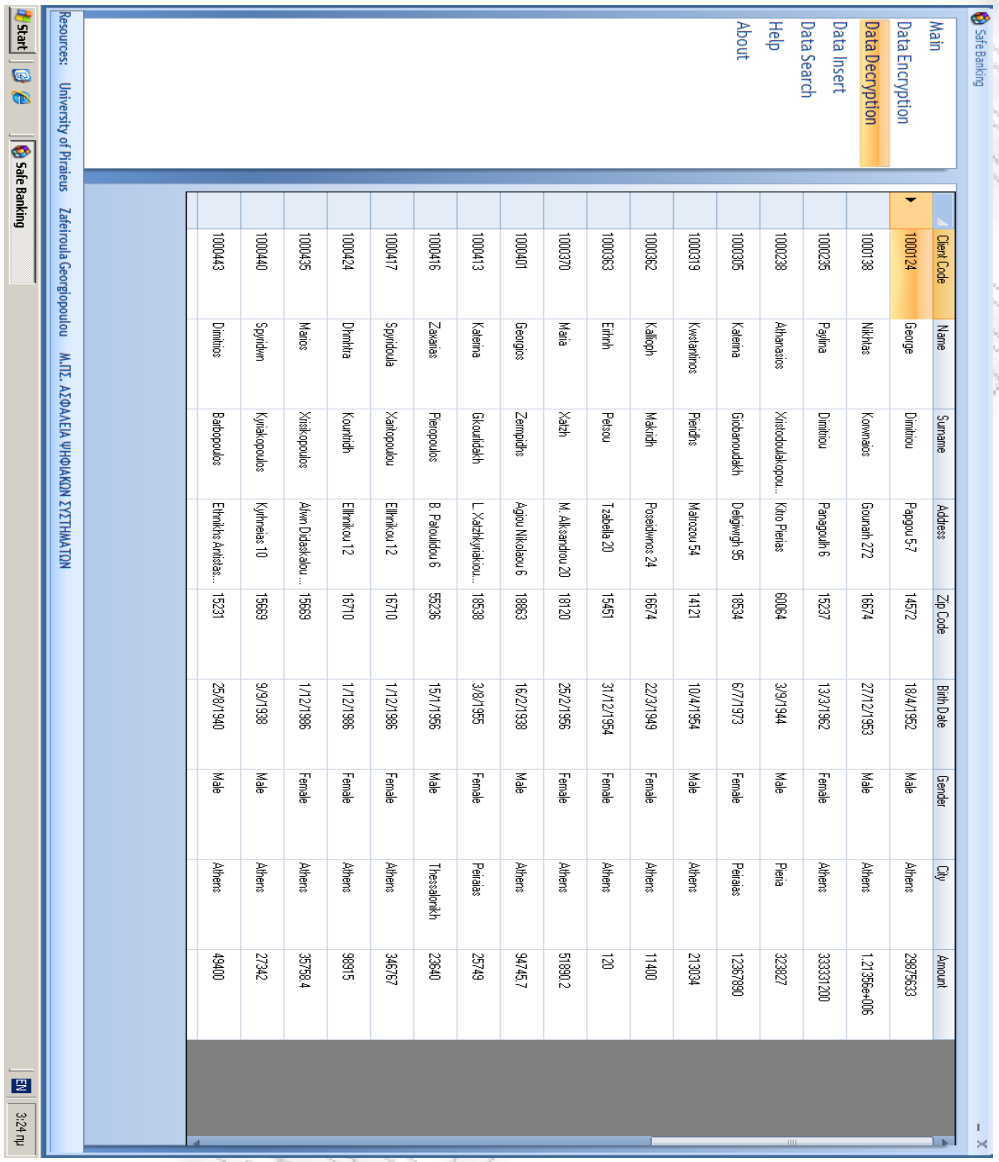
Βασικό μενού



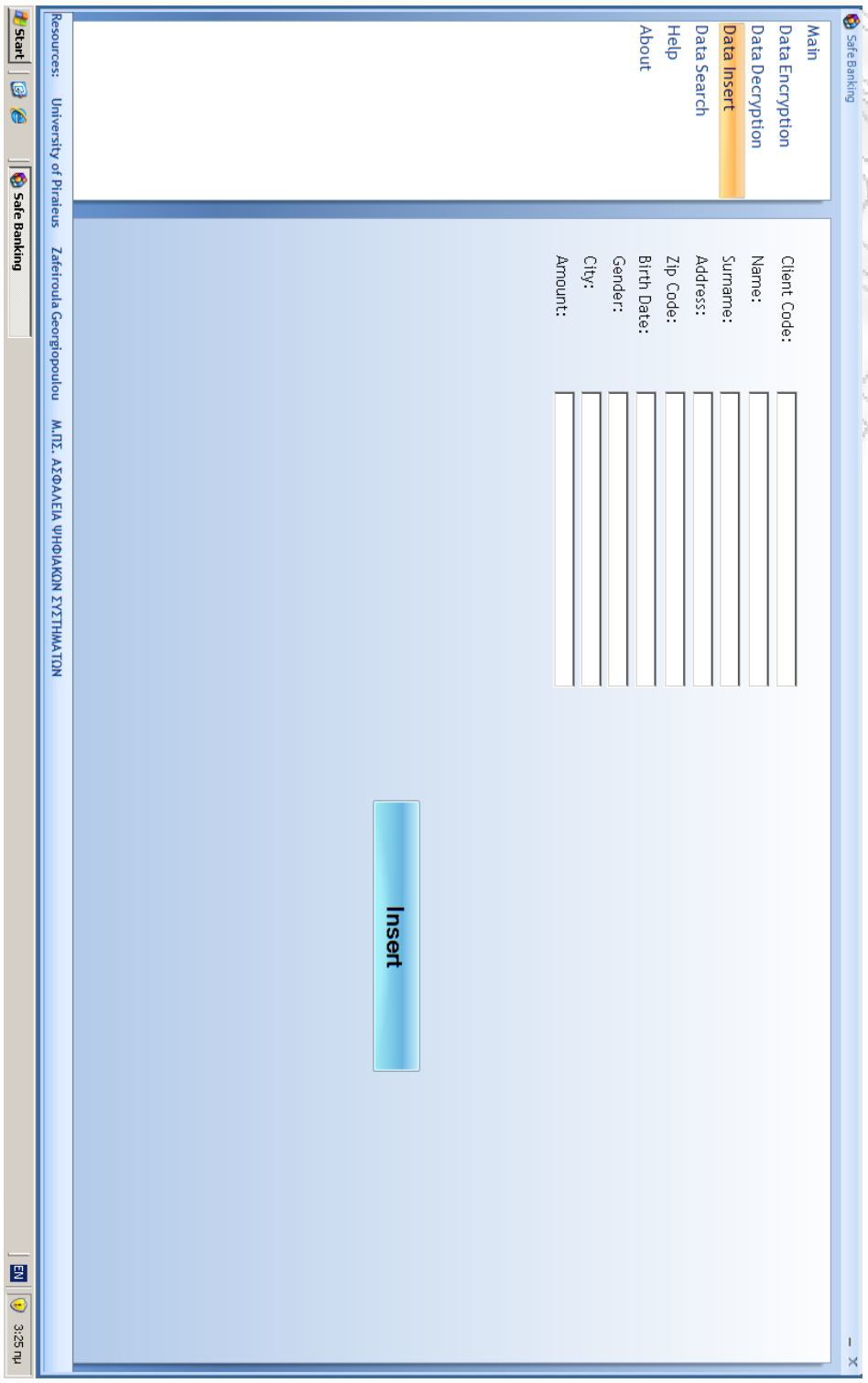
Κρυπτογράφηση



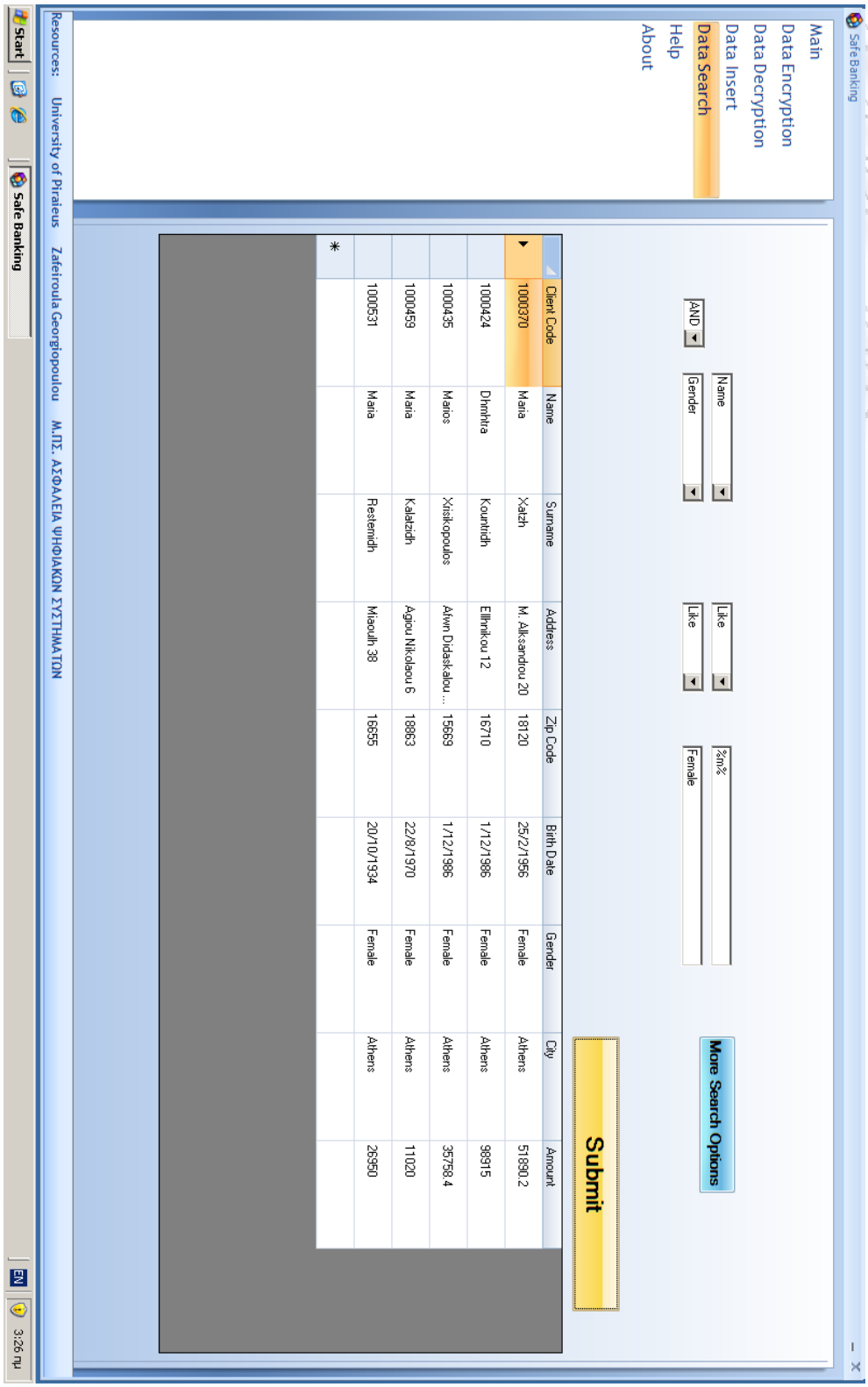
Αποκρυπτογράφηση



Εισαγωγή


Safe Banking
Main
Data Encryption
Data Decryption
Data Insert
Data Search
Help
About
Client Code:
Name:
Surname:
Address:
Zip Code:
Birth Date:
Gender:
City:
Amount:
Insert
Resources: University of Piraeus Zafeiroula Georgiopoulou Μ.ΠΣ. ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Start
Safe Banking
EN
3:25 πμ

Αναζήτηση


Safe Banking
Main
Data Encryption
Data Decryption
Data Insert
Data Search
Help
About
Name
Like
%m%
AND
Gender
Like
Female
More Search Options
Submit
Client Code
Name
Surname
Address
Zip Code
Birth Date
Gender
City
Amount
1000370
Maria
Xatzh
M. Aleksandrou 20
18120
25/2/1956
Female
Athens
51890.2
1000424
Dhmhtra
Kountridh
Ellhnikou 12
16710
1/12/1986
Female
Athens
98915
1000435
Marios
Xrisikopoulos
Afwn Didaskalou ...
15669
1/12/1986
Female
Athens
35758.4
1000459
Maria
Kalatzidh
Agiou Nikolaou 6
18863
22/8/1970
Female
Athens
11020
1000531
Maria
Restemidh
Miaoulh 38
16655
20/10/1934
Female
Athens
26950
Resources:
University of Piraieus
Zafeiroula Georgiopoulou
Μ.ΠΣ. ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Start
Safe Banking
EN
3:26 πμ

9. Βιβλιογραφία

[1] Ball, D., Barton, D., Earl, C., et al. A study of outsourcing and externalization. Library and Information Commission Research Report 132, 2002

[2] Mayer Brown. Security & Privacy Regulations Affecting Outsourcing And How To Comply. IAOP Data Security Meeting 2010

[3] Pierangela Samarati, Latania Sweeny. Protecting Privacy when disclosing information.,2000

[4] LI XIONG, SUBRAMANYAM CHITTI and LING LIU. Preserving Data Privacy in Outsourcing Data Aggregation Services. Emory University

[5] Pierangela Samarati and Sabrina De Capitani di Vimercati. Data Protection in Outsourcing Scenarios: Issues and Direction.

[6] Sabrina De Capitani di Vimercati, Sara Foresti, and Pierangela Samarati. Protecting Information Privacy in the Electronic Society

[7] Weichao Wang, Zhiwei Li, Rodney Owens and Bharat Bhargava. Secure and Efficient Access to Outsourced Data. 2009

[8] Carlo Curino, Evan P. C. Jones, Raluca Ada Popa, Nirmesh Malviya. Relational Cloud: A Database as a Service for the Cloud. 2011

[9] Herr Dipl.-Math. Sergei Evdokimov. Secure Outsourcing of IT Services in a Non-Trusted Environment. 2008

[10] White Sands Technology, Inc. Fragmentation and Database Performance. 2004

[11] Daniel P. Lorence , Amanda Spink. Healthcare information systems outsourcing. 2004

[12] Man Lung Yiu, Gabriel Ghinita, Christian S. Jensen and Panos Kalnis. Outsourcing Search Services on Private Spatial Data. 2009

[13] Basel Committee on Banking Supervision. Outsourcing in Financial Services. 2005

[14] CHARU C. AGGARWAL, PHILIP S. YU. PRIVACY-PRESERVING DATA MINING: MODELS AND ALGORITHMS. 2007

[15] Lena Wiese. Horizontal Fragmentation for Data Outsourcing with Formula-Based Confidentiality Constraints. 2010

[16] Li, Meng and Li, Dong."A Survey and Analysis of the Literature on Information Systems Outsourcing" PACIS 2009 Proceedings.2009

[17] Dibbern J. Goals. Information System Outsourcing: A survey and analysis of literature. ACM SIDMIS Database. 2004

[18] Maria Karyda, Evangelia Mitrou and Gerald Quicmhayr. A Framework for Outsourcing IS/IT services. 2006

[19] Directives of European Parliament

[20] Woolckocks L., Fitzerald G. A business guide to IT outsourcing.1994

[21] ΣΗΜΕΙΩΣΕΙΣ ΣΤΑ ΠΛΑΙΣΙΑ ΜΑΘΗΜΑΤΟΣ ΑΡΧΕΣ ΔΙΚΑΙΟΥ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΔΙΔΑΣΚΟΥΣΑ ΤΗΣ ΛΙΛΙΑΝ ΜΗΤΡΟΥ

[22] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών

[23] Outsourcing, e-business Forum, 2003

[24] Lee A. Bygrav, Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling, Published in Computer Law & Security Report, 2001

[25] Data Protection Act 1998 , European Commision,1998

[26] ISO 27701, Directive for Secure Outsourcing

[27] Τράπεζα της Ελλάδος, ΕΞΩΤΕΡΙΚΗ ΑΝΑΘΕΣΗ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΣΕ ΤΡΙΤΟΥΣ (OUTSOURCING),2006

[28]Sara Foresti, Preserving Privacy in Data Outsourcing, 2008

[29] G. Aggarwal, M. Bawa, P. Ganesan, H. Garcia-Molina, K. Kenthapadi, R. Motwani, U. Srivastava, D. Thomas, and Y. Xu. Two can keep a secret: a distributed architecture for

secure database services. In Proc. of the 2nd Biennal Conference Innovative Data Systems Research (CIDR 2005), Asilomar, CA, January 2005.

[30] Khahjlfan A.M. Information Security Considerations In Is It Outsourcing Projects, International Journal of Information Management 24, pp29-42, 2004

[31]Mary C. Lacity, The Information Systems Outsourcing Bandwagon, 1993

[32]MitrouE., Προσωπικά δεδομένα, ιδιωτικότητα και απόρρητο. Συνήγορος του πολίτη. Αθήνα,2006

[33] Woolcock P. & Pinnington A., The role of vendor companies in IS/IT outsourcing. International Journal of Information management, 17(3) pp.199-210.1997

[34] Huang J. & Yuang C. A decision model for IS outsourcing. International Journal of Information Management, 20(3), pp.225-239