ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ Η/Υ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

Διπλωματική εργασία

OUTSOURCING NETWORK SECURITY

υπό

ΙΟΥΛΙΑΣ ΑΝΑΣΤΑΣΙΑΔΟΥ

Υπεβλήθη για την εκπλήρωση μέρους των

απαιτήσεων για την απόκτηση του

Διπλώματος Μηχανικού Η/Υ Τηλεπικοινωνιών και Δικτύων

2006

Εγκρίθηκε από τα Μέλη της Διμερούς Εξεταστικής Επιτροπής:

Πρώτος Εξεταστής (Επιβλέπων)	Δρ. Χρήστος Ηλιούδης Διδάσκων ΠΔ 407/80, Τμήμα Μηχανικών Η/Υ Τηλεπικοινωνιών και Δικτύων, Πανεπιστήμιο Θεσσαλίας
Δεύτερος Εξεταστής	Δρ. Λέανδρος Τασιούλας Καθηγητής, Τμήμα Μηχανικών Η/Υ Τηλεπικοινωνιών και Δικτύων, Πανεπιστήμιο Θεσσαλίας

Ευχαριστίες

Δεν είναι εύκολο να παραδεχτείς ότι ένα μεγάλο κομμάτι της ζωής σου, που λέγεται φοιτητική ζωή, τελειώνει. Για εμένα, αυτή η ώρα έφτασε και θέλω να ευχαριστήσω ορισμένους ανθρώπους που με βοήθησαν όλα αυτά τα χρόνια.

Καταρχήν, πρέπει να ευχαριστήσω τον επιβλέποντα της διπλωματικής εργασίας, κ. Χρήστο Ηλιούδη για την ευκαιρία που μου έδωσε να πραγματοποιήσω αυτήν την εργασία και για τη βοήθεια του σε όλη τη διάρκεια της συνεργασίας μας. Επίσης, είμαι ευγνώμων στον δεύτερο επιβλέποντα της διπλωματικής μου, Καθηγητή κ. Λέανδρο Τασσιούλα, για την προσεκτική ανάγνωση της εργασίας μου και τις πολύτιμες υποδείξεις του.

Στη διάρκεια της φοιτητικής μου ζωής, υπήρχαν άνθρωποι με του οποίους έζησα ωραίες και άσχημες στιγμές, μέσα από τις οποίες κέρδισα πολύτιμες εμπειρίες. Ζωή, Ντίνη, Αλέξανδρε, Γιώργο, Στεφανία, Βίκυ, Γιώτα, Φανή, ευχαριστώ για όλα. Θέλω, επίσης, να ευχαριστήσω το Σπύρο, γιατί τα τελευταία δύο χρόνια είναι συνεχώς δίπλα μου και αποτέλεσε στήριγμα για εμένα.

Πάνω από όλα ευχαριστώ τους γονείς μου, Άννα και Μπάμπη, γιατί συνέβαλλαν στη ολοκλήρωση του χαρακτήρα μου, μου έδωσαν τις απαραίτητες αρχές και βάσεις για να μπορέσω να αντιμετωπίσω τη ζωή και μέρος των όσων έχω καταφέρει μέχρι σήμερα οφείλεται σε αυτούς και την αδερφή μου, Κική, που εκτός από το γεγονός ότι είναι πάντα εκεί για μένα και με συμβουλεύει όποτε την χρειάζομαι, με βοήθησε πολύ και στην ολοκλήρωση της διπλωματικής μου.

Θέλω να αφιερώσω την εργασία αυτή στον παππού μου που έχασα πρόσφατα και ο οποίος αποτέλεσε σημείο αναφοράς στη ζωή μου.

Ιουλία Αναστασιάδου

Περιεχόμενα

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

Κεφάλαιο 1: Εισαγωγή

Η ανάθεση μέρους των εργασιών μιας επιχείρησης σε τρίτους αποτελεί συχνό φαινόμενο εδώ και πολλά χρόνια και καλύπτει τις περισσότερες από τις λειτουργίες της, ξεκινώντας από τις πιο βασικές (καθαριότητα, λογιστικά, μισθοδοσίες) και φθάνοντας μέχρι τις πιο εξειδικευμένες (προσλήψεις, διαχείριση ανθρώπινου δυναμικού κ.α.). Υπάρχει μια "ελεύθερη" εργασιακή σχέση με τους εξωτερικούς συνεργάτες - ελεύθερης με την έννοια ότι ο επιχειρηματίας δεν απασχολεί προσωπικό με εξαρτημένη σχέση (μισθό), αλλά καταβάλλει κάποιο αντίτιμο που έχει συμφωνηθεί για τις υπηρεσίες που λαμβάνει. Αυτή η πρακτική ονομάζεται outsourcing.

Τα τελευταία χρόνια το outsourcing έχει αρχίσει να εξαπλώνεται και στις υπηρεσίες πληροφορικής και τηλεπικοινωνιών. Η εξάρτηση των επιχειρήσεων από τις τεχνολογίες πληροφορικής γίνεται ολοένα και μεγαλύτερη καθώς είναι πλέον απαραίτητη η χρήση ηλεκτρονικών υπολογιστών καθ'όλη τη διάρκεια της παραγωγικής διαδικασίας. Η επιβίωση της επιχείρησης μέσα σε ένα ανταγωνιστικό περιβάλλον εξαρτάται από τον εκσυγχρονισμό της επιχείρησης ως προς τις υπηρεσίες πληροφορικής και τηλεπικοινωνιών που είναι διαθέσιμες την εκάστοτε χρονική στιγμή [7], [30].

Η πρακτική του outsourcing μπορεί να εφαρμοσθεί επιτυχώς και στον τομέα της ασφάλειας των δικτύων. Από τη μία η διεύρυνση των υπηρεσιών διαδικτύου και από την άλλη η αδυναμία, από τις περισσότερες επιχειρήσεις, δημιουργίας ξεχωριστού τμήματος ασφάλειας ή απασχόλησης εξειδικευμένου προσωπικού στον τομέα αυτό, οδηγούν στην ανάθεση ορισμένων υπηρεσιών ασφάλειας σε κάποια άλλη εταιρία. Ένα μεγάλο μέρος των υπαρχόντων οργανισμών και εταιριών στηρίζουν τη ζωτικότητα της επιχείρησης τους στο διαδίκτυο και στα εκάστοτε μικρότερα δίκτυα εντός των οργανισμών ή /και εταιριών. Ορισμένες από αυτές ενδιαφέρονται για την ασφάλεια των πληροφοριών που κινούνται μέσα από το δίκτυο, ενώ άλλες για την διαθεσιμότητα των υπηρεσιών που παρέχονται μέσω του δικτύου της. Η κλοπή πολύτιμων πληροφοριών μπορεί να αφαιρέσει από την εταιρία ή τον οργανισμό τα δικά του ανταγωνιστικά πλεονεκτήματα καθώς επίσης και να πλήξει τη φήμη και το γόητρό του. Επίσης, μπορεί να θέσει σε κίνδυνο την εμπιστοσύνη που η κάθε εταιρία έχει καταφέρει να κερδίσει από τους πελάτες, τους προμηθευτές και τους συνεργάτες της σε περίπτωση που η επικοινωνία

μεταξύ τους δεν είναι ασφαλής και το περιεχόμενο δεν ελέγχεται. Επιπλέον, η μη διαθεσιμότητα των υπηρεσιών μπορεί να προκαλέσει τη δυσαρέσκεια των πελατών και κατά συνέπεια την απώλεια τους. Η τεχνική του outsourcing προσφέρει μεγαλύτερο βαθμό ασφάλειας, καθώς η εταιρία που παρέχει τις υπηρεσίες αποτελείται από προσωπικό εξειδικευμένο σε θέματα ασφάλειας δικτύων και είναι εφοδιασμένη με τα πιο σύγχρονα συστήματα. Επιπρόσθετα, παρέχει εικοσιτετράωρη επίβλεψη του δικτύου με αποτέλεσμα την άμεση επίλυση οποιουδήποτε προβλήματος προκύψει ανά πάσα στιγμή. Ταυτόχρονα, μειώνεται το κόστος αφού μία συμφωνία outsourcing είναι οικονομικότερη από ότι η εύρεση και μίσθωση επαγγελματιών σε θέματα ασφάλειας και αυξάνεται ο ελεύθερος χρόνος των στελεχών της επιχείρησης, ώστε να μπορέσουν να ασχοληθούν με δραστηριότητες που αποτελούν τον πυρήνα της επιχείρησης. Γενικότερα, το outsourcing στον τομέα της ασφάλειας ενός δικτύου εκτιμάται ως μια αποτελεσματική και ωφέλιμη επιλογή η οποία καλείται να λύσει με βέλτιστο τρόπο τα θέματα της ασφάλειας Πληροφορικών Συστημάτων.

Σκοπός αυτής της διπλωματικής είναι η μελέτη της διαδικασίας ανάθεσης της προστασίας των δικτύων μιας επιχείρησης σε τρίτους, έχοντας ως στόχο την αύξηση του βαθμού ασφάλειας της επιχείρησης και τη μείωση του ετήσιου κόστους επένδυσης σε ανάλογα συστήματα ή/και σε ανθρώπινο δυναμικό που απασχολείται στον τομέα της ασφάλειας.

Τα κύρια ζητήματα, στα οποία επικεντρώθηκε η έρευνα που παρουσιάζεται στην παρούσα διπλωματική είναι:

- Η καταγραφή του πλαισίου ανάθεσης υπηρεσιών ασφάλειας σε εξωτερικούς συνεργάτες.
- Η μελέτη των χαρακτηριστικών του outsourcing, των πλεονεκτημάτων και των μειονεκτημάτων που προκύπτουν.
- Ο καθορισμός του νομικού και κανονιστικού πλαισίου που διέπει τις διαδικασίες outsourcing υπηρεσιών ασφάλειας
- Η ανάλυση πετυχημένων σεναρίων
- Η ανάπτυξη ενός εργαλείου καταγραφής τάσεων της αποδοχής του outsourcing στις υπηρεσίες ασφάλειας στην ελληνική επικράτεια.

- Η ανάπτυξη μιας εφαρμογής, στην οποία περιγράφεται η διαδικασία ανάθεσης Ψηφιακών Πιστοποιητικών σε εξωτερικούς συνεργάτες.

Παρόλο που στις περισσότερες χώρες της δύσης η πρακτική του outsourcing αποτελεί κυρίαρχη τάση, στην Ελλάδα η κατάσταση είναι τελείως διαφορετική. Η αγορά των υπηρεσιών outsourcing στην Ελλάδα βρίσκεται σε πολύ αρχικό επίπεδο αφού οι περισσότερες ιδιωτικές εταιρίες αλλά και δημόσιοι φορείς δεν δείχνουν την απαραίτητη εμπιστοσύνη σε τέτοιες λύσεις. Η λέξη "άγνοια" είναι αυτή που αντιπροσωπεύει την υφιστάμενη κατάσταση στην Ελλάδα, διότι ελάχιστοι είναι αυτοί οι οποίοι γνωρίζουν την έννοια του outsourcing σε θέματα ασφάλειας και τη διαδικασία γύρω από αυτό.

Έτσι, ένας από τους στόχους της διπλωματικής εργασίας τέθηκε η μελέτη των ιδιαιτέρων χαρακτηριστικών της ελληνικής πραγματικότητας που δεν επιτρέπουν έως σήμερα την ευρεία διάδοση της παροχής υπηρεσιών ασφάλειας σε φορείς μέσω της διαδικασίας outsourcing. Για τη μελέτη αυτή αναπτύχθηκε ένα ερωτηματολόγιο το οποίο καταγράφει την στάση των φορέων απέναντι στο outsourcing αλλά και την ετοιμότητα της αγοράς να παρέχει ανάλογες υπηρεσίες σε φορείς.

Βασικός στόχος, όμως, της διπλωματικής αποτέλεσε η δημιουργία ενός παραδείγματος χρήσης outsourcing, στο οποίο βρίσκουν εφαρμογή όλα όσα ερευνώνται στη μελέτη αυτή. Αναπτύχθηκε μια υποθετική περίπτωση ανάθεσης της έκδοσης Ψηφιακών Πιστοποιητικών και εξετάστηκαν όλες οι παράμετροι που διέπουν μια τέτοια σχέση. Η δημιουργία της Σύμβασης Διασφάλισης Επιπέδου Ποιότητας και Υπηρεσιών βασίστηκε σε ένα έτοιμο πρότυπο Συμφωνητικό Διαχείρισης Υπηρεσιών.

Η δομή της διπλωματικής έχει ως εξής:
Στο κεφάλαιο 2 εξετάζονται ζητήματα σχετικά με το outsourcing, όπως τα βασικά χαρακτηριστικά, οι κατηγορίες που υπάρχουν, πλεονεκτήματα και μειονεκτήματα και στοιχεία για το αντικείμενο και τα κριτήρια πληρότητας και αξιοπιστίας των εταιριών που παρέχουν outsourcing.

Στο κεφάλαιο 3 δίνεται το νομικό πλαίσιο, τα κριτήρια κατά ISO που πρέπει να πληρούνται, το κανονιστικό πλαίσιο από την πλευρά των πελατών, μοντέλα βέλτιστων συμβολαίων και τέλος περιγράφεται η κατάσταση στην Ελλάδα.

Στο κεφάλαιο 4 δίνονται παραδείγματα επιτυχημένης εφαρμογής του outsourcing σε θέματα ασφάλειας πληροφοριακών συστημάτων.

Στο κεφάλαιο 5 αναλύεται η διαδικασία ανάθεσης της έκδοσης Ψηφιακών Πιστοποιητικών σε μια εταιρία outsourcing. Πιο συγκεκριμένα, περιγράφεται το περιβάλλον της εφαρμογής, η διαδικασία επιλογής υπηρεσιών και παρόχων, αναπτύσσεται μια πρότυπη Σύμβαση Διασφάλισης Επιπέδου Ποιότητας και Υπηρεσιών και, τέλος, γίνεται αποτίμηση του μοντέλου.

Το κεφάλαιο 6 περιέχει τα συμπεράσματα.

Κεφάλαιο 2: Outsourcing

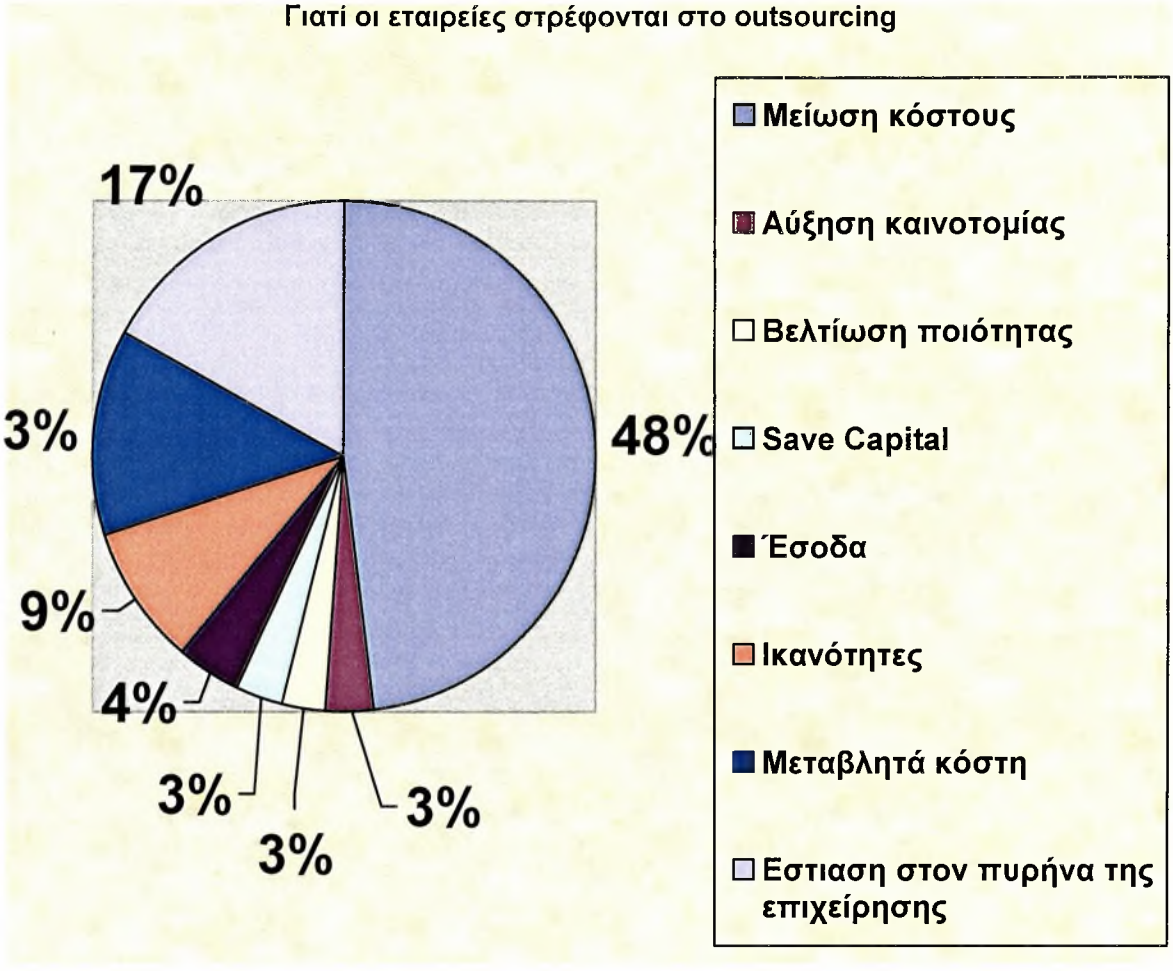
2.1 Γενικά για το outsourcing

2.1.1 Βασικά χαρακτηριστικά Outsourcing

Outsourcing είναι η ανάθεση υπηρεσιών και εργασιών μιας επιχείρησης σε εξωτερικό συνεργάτη, που μπορεί να είναι είτε μια εταιρία που εξειδικεύεται σ' έναν τομέα, είτε ένας μεμονωμένος ιδιώτης [30]. Ακριβής μετάφραση για τον όρο στα ελληνικά δεν υπάρχει. Περιφραστικά θα μπορούσαμε να πούμε ότι είναι υπηρεσίες "εξωγενών ή εξωεπιχειρησιακών πόρων".

Όπως αναφέρθηκε, η υλοποίηση – παροχή κάποιων υπηρεσιών εξωεπιχειρησιακά είναι ήδη διαδεδομένη. Η έννοια όμως του outsourcing, όπως αυτό τίθεται σήμερα, επεκτείνει τον τρόπο με τον οποίο αυτές οι υπηρεσίες παρέχονται σε σχέση με όσα ίσχυαν μέχρι τώρα. Πλέον, εμπεριέχει όρους και διαδικασίες για την εξασφάλιση της ποιότητας των παρεχόμενων υπηρεσιών. Με αυτόν τον τρόπο, η έννοια του outsourcing καλύπτει και την ποιότητα των παρεχόμενων υπηρεσιών μέσω ειδικών, για το σκοπό αυτό, συμβάσεων – συμβολαίων μεταξύ των δύο μερών [7].

Στο διάγραμμα που ακολουθεί φαίνονται οι κύριοι λόγοι για τους οποίους μια εταιρία αποφασίζει να δώσει κάποιες υπηρεσίες για outsourcing [22]:



Πηγή: Michael F.Corbet and Associates

Εικόνα 1: Γιατί οι εταιρείες στρέφονται στο outsourcing

2.1.2 Η αναγκαιότητα του outsourcing

Όλο και περισσότερες επιχειρήσεις καταφεύγουν στην τεχνική αυτή, αφού αν οργανωθεί με σωστό και ορθολογικό τρόπο μπορεί να αποφέρει σημαντικά οφέλη σε μια επιχείρηση, σε πολλά και διαφορετικά επίπεδα. Η τάση αυτή είναι αποτέλεσμα του σκληρού ανταγωνισμού ο οποίος απαιτεί από τις επιχειρήσεις να βρούνε τις καλύτερες λύσεις για τους πελάτες τους και αφορά σχεδόν όλους τους τομείς, από τη βιομηχανία της υγείας μέχρι αυτήν των τηλεπικοινωνιών.

Έρευνα που έγινε σε 500 εταιρείες της δυτικής Ευρώπης έδειξε ότι τα τελευταία τρία χρόνια το ένα τέταρτο αυτών ανέθεσαν μερικές από τις λειτουργίες τους σε άλλες χώρες, κυρίως της κεντρικής και ανατολικής Ευρώπης [22].

Η Dun & Bradstreet [22], εταιρία που παρέχει βοήθεια σε επιχειρήσεις για τη λήψη αποφάσεων, εκτιμά ότι το outsourcing, που ξεκίνησε περίπου πριν από 30 χρόνια, σήμερα έχει κέρδος 4 τρισεκατομμύρια δολάρια. Σύμφωνα με ειδικούς το 2005, 25% από έναν τυπικό προϋπολογισμό ενός οργανισμού προορίζεται για υπηρεσίες outsourcing και αναμένεται να αυξηθεί στο 34% μέχρι το τέλος του 2006. Η Microsoft [14], μία από τις πιο επιτυχημένες επιχειρήσεις τα τελευταία 25 χρόνια, θεωρεί τον εαυτό της αδέξιο σε τομείς εκτός αυτών που αποτελούν τις κύριες λειτουργίες της, δηλαδή τη σχεδίαση και την ανάπτυξη λογισμικού και το marketing. Ως αποτέλεσμα αναθέτει σε εξωτερικούς συνεργάτες ορισμένες από τις υπόλοιπες δραστηριότητες.

Άλλο ένα παράδειγμα είναι αυτό της British Airways [22], της έβδομης μεγαλύτερης αεροπορικής εταιρείας στον κόσμο, η οποία στράφηκε στο outsourcing εδώ και περίπου μια δεκαετία επιδιώκοντας τη βελτιστοποίηση της ποιότητας στις δευτερεύουσες υπηρεσίες που παρέχει στους πελάτες της. Τώρα επικεντρώνεται στις βασικές της δραστηριότητες. Συγκεκριμένα, πριν από μία δεκαετία έκλεισε συμφωνία με την EMCOR για να διαχειρίζεται ποικίλες δραστηριότητες από το φωτισμό, την ισχύ και τα συστήματα ψύξης-θέρμανσης, μέχρι την καθαριότητα των σαλονιών των επιβατών, των τηλεφωνικών κέντρων και των γραφείων. Αυτή η απόφαση μειώνει τα έξοδα της εταιρίας περίπου 15% ετησίως, αν και ο αρχικός σκοπός της ήταν η αναζήτηση καλύτερης ποιότητας υπηρεσιών.

2.1.3 Outsourcing στην πληροφορική και τις τηλεπικοινωνίες

Η αλματώδης ανάπτυξη και εξάπλωση της ψηφιακής τεχνολογίας καθώς και οι αυξημένες ανάγκες του επιχειρηματικού κόσμου για νέες τεχνολογίες είχαν αποτέλεσμα τη δραστηριοποίηση πολλών εταιριών που παρέχουν σχετικές υπηρεσίες. Ιστορικά, καθώς οι τεχνολογίες πληροφορικής και επικοινωνιών γινόντουσαν απαραίτητες για την αποδοτική λειτουργία των επιχειρήσεων, δημιουργήθηκαν τα τμήματα πληροφορικής και

μηχανογράφησης. Με τον καιρό η εξάρτηση των επιχειρήσεων από τα μηχανογραφικά τους τμήματα γινόταν όλο και μεγαλύτερη. Κάθε στάδιο της παραγωγικής διαδικασίας απαιτούσε την ύπαρξη ηλεκτρονικών υπολογιστών και εφαρμογών μετατρέποντας την πληροφορική σε κομβικό σημείο για την ανταγωνιστικότητα της επιχείρησης. Ταυτόχρονα, η ραγδαία πρόοδος των τεχνολογιών απαιτούσε τη συνεχή επένδυση σε τεχνογνωσία, εφαρμογές και τεχνολογικό υλικό από την πλευρά του τμήματος μηχανογράφησης αυξάνοντας συνεχώς τον προϋπολογισμό του σχετικού τμήματος. Η ανταγωνιστική πίεση στο πλαίσιο μιας παγκοσμιοποιημένης οικονομίας έφερε, όμως, τις επιχειρήσεις μπροστά σε μια επιτακτική ανάγκη για αύξηση της ανταγωνιστικότητας. Σε αυτό το πλαίσιο, η απόφαση περιορισμού των δαπανών των μη σχετικών με το κύριο έργο της επιχείρησης, οδήγησε τις επιχειρήσεις στο να επανεξετάσουν την αναγκαιότητα των τμημάτων πληροφορικής και τη λήψη των υπηρεσιών των τμημάτων αυτών από εξωτερικούς παρόχους [7].

Σταδιακά, η τεχνική του outsourcing άρχισε να υιοθετείται και από μικρότερες επιχειρήσεις κυρίως λόγω της διεύρυνσης της χρήσης των υπηρεσιών διαδικτύου. Σύνηθες φαινόμενο είναι η απασχόληση των εργαζομένων της επιχείρησης ή και του ίδιου του επιχειρηματία στα τμήματα πληροφορικής, χωρίς να έχουν τις απαραίτητες τεχνικές γνώσεις, γεγονός που οφείλεται στη μειωμένη εκ των πραγμάτων δυνατότητα των μικρομεσαίων επιχειρήσεων να απασχολούν εξειδικευμένο προσωπικό αποκλειστικά για τις τεχνολογίες πληροφορικής και επικοινωνιών.

2.1.4 Κατηγορίες outsourcing

Σύμφωνα με την ομάδα εργασίας Ε5 [7], στα πλαίσια του προγράμματος «Κοινωνία της πληροφορίας» που έγινε για λογαριασμό του υπουργείου Οικονομίας και Οικονομικών και του υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης, το outsourcing μπορεί να χωριστεί σε κατηγορίες και ο διαχωρισμός αυτός γίνεται ως προς συγκεκριμένα χαρακτηριστικά. Πιο συγκεκριμένα μπορεί να γίνει διαχωρισμός :

1. Ως προς τις υπηρεσίες και το αντικείμενο τους:
    - τεχνικής υποστήριξης (technical support),
    - δικτύωσης (networking),

- παροχής υποδομής (systems infrastructure),
- παροχής περιβάλλοντος ανάπτυξης (development environment),
- εφαρμογών (applications),
- περιεχόμενου (content),
- υποστήριξης διαδικασιών (process support),
- ανάληψης διαδικασιών (process execution).

2. Ως προς το χρόνο αντίδρασης του παρόχου:
    - Συνεχούς παροχής υπηρεσιών (performance), με συγκεκριμένα επίπεδα ποιότητας,
    - Απόκρισης σε σύμβαντα (reactive), όπου ο πάροχος αντιδρά στην περίπτωση κάποιου γεγονότος ή/και αιτήματος από την επιχείρηση,
    - Πρόληψης (proactive), όπου ο πάροχος παρέχει συγκεκριμένες υπηρεσίες στοχεύοντας στην πρόληψη προβλημάτων.

3. Ως προς το βαθμό εμπλοκής της επιχείρησης:
    - Υπηρεσίες για τις οποίες απαιτείται μερική δραστηριοποίηση κάποιου τμήματος της επιχείρησης (Partial Outsourcing),
    - Και στις υπηρεσίες που η παροχή των υπηρεσιών γίνεται πλήρως από τον πάροχο (Full Outsourcing).

4. Ως προς τον αριθμό των παρόχων οι οποίοι εμπλέκονται για την παροχή των Υπηρεσιών:
    - Η παροχή πραγματοποιείται από έναν πάροχο,
    - Η παροχή πραγματοποιείται από πολλούς παρόχους.

Σύμφωνα με το πρόγραμμα Δικτυωθείτε [30], μπορεί να γίνει μια περαιτέρω ανάλυση του διαχωρισμού, ως προς τις υπηρεσίες και το αντικείμενο που προσφέρουν ως εξής:

α) Υπηρεσίες παροχής υποδομών, όταν η εταιρία outsourcing διαθέτει προς χρήση της εταιρείας-πελάτη της διάφορα μηχανήματα, όπως διακομιστές (servers), δρομολογητές (routers), σταθμούς εργασίας (work stations), εξοπλισμό για ασύρματη δικτύωση κ.ά.

β) Υπηρεσίες τεχνικής υποστήριξης, όταν ο εξωτερικός συνεργάτης αναλαμβάνει τον έλεγχο, τη συντήρηση, την επιδιόρθωση και την αναβάθμιση του εξοπλισμού μιας επιχείρησης. Τα παραπάνω μπορεί να αφορούν το υλικό (Hardware), το λογισμικό (Software), όπως για παράδειγμα ανάπτυξη εφαρμογών και αναβάθμιση πακέτων λογισμικού, ή και άυλες υπηρεσίες που έχουν να κάνουν με τη λήψη αποφάσεων ή και την εκπαίδευση του προσωπικού.

γ) Υπηρεσίες παροχής λογισμικών εφαρμογών, όταν διατίθενται για χρήση από την επιχείρηση εξειδικευμένα προγράμματα όπως ERP (για τη διαχείριση των επιχειρησιακών πόρων), CRM (για τη διαχείριση των πελατών), WMS (για τη διαχείριση της αποθήκης), εφαρμογές μηχανογραφημένης λογιστικής , ηλεκτρονικού εμπορίου κ.ά. Συνήθως, οι εφαρμογές αυτές παρέχονται μαζί με εξυπηρετητές (servers), που διατίθενται προς χρήση από την ενδιαφερόμενη επιχείρηση.

δ) Υπηρεσίες παροχής και διαχείρισης δικτύωσης, όπου η εταιρία outsourcing παρέχει όλη την απαραίτητη υλικοτεχνική υποδομή για τη δικτύωση της επιχείρησης-πελάτης της είτε εσωτερικά (μέσω intranet) είτε τοπικά (μέσω LAN/δικτύων μικρής εμβέλειας ή WAN/δικτύων μεγάλης εμβέλειας) είτε, ασφαλώς, με το ίντερνετ. Στο πλαίσιο αυτό, μπορεί να αναλάβει επίσης την κατασκευή του δικτυακού τόπου της επιχείρησης, τη δημιουργία ηλεκτρονικού ταχυδρομείου για το προσωπικό της επιχείρησης καθώς και τις εφαρμογές ηλεκτρονικού εμπορίου. Όσον αφορά στην υποδομή του δικτύου μπορεί να ανήκει είτε στην επιχείρηση, στην οποία περίπτωση ο πάροχος προσφέρει μόνο τη διαχείριση του δικτύου είτε στον πάροχο. Στην τελευταία περίπτωση μετά τη λήξη του συμβολαίου επιστρέφεται σε αυτόν .

ε) Υπηρεσίες ασφάλειας, η εταιρεία outsourcing αναλαμβάνει είτε ολόκληρο τον τομέα της ασφάλειας του δικτύου των πελατών της είτε μέρος αυτής, προσφέροντας τους τον απαραίτητο εξοπλισμό (hardware), λογισμικό (software) αλλά και συνεχή παρακολούθηση του δικτύου της.

στ) Υπηρεσίες περιεχομένου, όπου η εταιρεία outsourcing παρέχει πρόσβαση σε δεδομένα απαραίτητα για την αποδοτική λειτουργία μιας επιχείρησης που μπορεί να αφορούν νομικά κείμενα, πληροφορίες τεχνικής και τεχνολογικής φύσης ή και πληροφορίες για το τμήμα αγοράς. Τα δεδομένα αυτά μπορεί να υποστούν κάποια επεξεργασία πριν δοθούν στον πελάτη αλλά μπορεί και να δοθούν ακατέργαστα.

ζ) Υπηρεσίες τήρησης αντιγράφων ασφαλείας (backup) καθώς και ανάκτησης δεδομένων (disaster recovery) ύστερα από κάποιο απρόσμενο γεγονός.

η) Υπηρεσίες τηλεφωνικής επικοινωνίας με τους πελάτες της επιχείρησης (call centers).

2.1.5 Πλεονεκτήματα

Κατά πρώτον, η υιοθέτηση του outsourcing επιτρέπει στην επιχείρηση να εξοικονομήσει σημαντικούς πόρους, γιατί αποφεύγει την αγορά υλικού (hardware) και λογισμικού (software). Οι σύγχρονες τεχνολογίες κοστίζουν ακριβά και σε πολύ μικρό χρονικό διάστημα από την αγορά τους (συνήθως μέσα σε δύο ή τρία χρόνια) κρίνονται παρωχημένες είτε γιατί μια νέα εφαρμογή έκανε την εμφάνισή της, είτε γιατί απαιτείται αναβάθμιση, είτε, τέλος, γιατί ο εξοπλισμός ολοκλήρωσε τον κύκλο ζωής του. Με το outsourcing, το ζήτημα της απαξίωσης ή της φθοράς του εξοπλισμού αφορά μόνο την εταιρία που παρέχει τις σχετικές υπηρεσίες και απαλλάσσει την εκάστοτε εταιρεία από αυτόν το φόρτο [30].

Το κόστος λειτουργίας των συστημάτων υψηλής τεχνολογίας κρίνεται ιδιαίτερα υψηλό, καθώς απαιτεί εξειδικευμένο προσωπικό, συντήρηση και αναλώσιμες δαπάνες. Με την ανάθεση, όμως, των εργασιών αυτών σε κάποιον εξωτερικό συνεργάτη αποφεύγονται δαπάνες για τη δημιουργία και στελέχωση τμημάτων που θα χειρίζονται και θα συντηρούν τις νέες τεχνολογίες και καταβάλλεται μόνο ένα ποσό για την ενοικίαση των υπηρεσιών και εργασιών. Το ποσό αυτό υπολείπεται των χρημάτων που θα ξόδευε η επιχείρηση αν αναλάμβανε η ιδία να πραγματοποιήσει τις εργασίες αυτές.

Η δέσμευση, επομένως, κεφαλαίων της επιχείρησης σε εξοπλισμό υψηλής τεχνολογίας, είναι φανερό ότι, στερεί τους πόρους αυτούς από την κύρια δραστηριότητά της. Η εκχώρηση τέτοιων υπηρεσιών σε τρίτους αφήνει αρκετούς πόρους στη διάθεση της επιχείρησης, οι οποίοι μπορούν να επενδυθούν σε άλλες πιο ουσιαστικές δραστηριότητες της όπως η παραγωγική διαδικασία ή η επέκτασή της. Οι πόροι αυτοί μπορούν να είναι είτε οικονομικοί είτε να αναφέρονται σε ανθρώπινο δυναμικό [7].

Επιπρόσθετα, η επιχείρηση η οποία αποφασίζει να επενδύσει σε τεχνολογίες που μεταβάλλονται συνεχώς ριψοκινδυνεύει σε μεγάλο βαθμό καθώς οι επενδύσεις πληροφορικής κρύβουν μεγάλους κινδύνους και απρόοπτα [30]. Η σύναψη μιας σχέσης outsourcing βοηθά στην απάλειψη του ρίσκου, καθώς πλέον η βιωσιμότητα της επιχείρησης δε συνδέεται με την επιτυχία ή αποτυχία της επένδυσης, και βελτιώνει την ανταγωνιστικότητα της επιχείρησης. Η μείωση του επιχειρηματικού κινδύνου επιφέρει ηρεμία και σιγουριά στο εργασιακό περιβάλλον και αυτό με τη σειρά του αύξηση της παραγωγικότητας. Τέλος, ιδιαίτερη σημασία έχει το γεγονός ότι η επιχείρηση συνεχίζει να βασίζεται σε σύγχρονα συστήματα με όλα τα πλεονεκτήματα που αυτά παρέχουν [7].

Μέσα από τη συνεργασία με την εταιρία παροχής υπηρεσιών, επιτυγχάνεται η εισαγωγή πρωτοτυπίας και καινοτομίας στον τρόπο λειτουργίας μίας επιχείρησης κάτι που δύσκολα θα συνέβαινε αν η επιχείρηση αναλάμβανε να πραγματοποιήσει εσωτερικά τις ίδιες εργασίες. Οι εταιρίες που εξειδικεύονται στις σύγχρονες τεχνολογίες διαθέτουν συνήθως υψηλής ποιότητας ανθρώπινο δυναμικό, βρίσκονται μέσα στις εξελίξεις της παγκόσμιας αγοράς και η λειτουργία τους βασίζεται στην καινοτομία. Αντιθέτως, οι υπόλοιπες εταιρίες είναι συνήθως λιγότερο τεχνολογικά ενημερωμένες και επιφυλακτικές στην υιοθέτηση καινοτομιών. Με την ανάθεση εργασιών σε τρίτους δίνεται η ευκαιρία σε μια επιχείρηση να παραμείνει στην αιχμή των εξελίξεων και να έχει πρόσβαση σε φρέσκιες και μοντέρνες λύσεις ενώ παράλληλα δεν χρειάζεται να επενδύει σε ανθρώπινο δυναμικό και νέες τεχνολογίες [7].

2.1.6 Υπολογισμός του κόστους outsourcing

Η μείωση του κόστους αποτελεί βασικό λόγο για τον οποίον κάποιος επιλέγει τη λύση του outsourcing. Ο υπολογισμός του είναι πολύπλοκος και πρέπει να υπολογιστεί το κόστος τόσο ενδοεπιχειρησιακά όσο και εξωεπιχειρησιακά. Η σύγκριση των δυο αυτών ποσών οδηγεί στην επιλογή της λύσης που συμφέρει περισσότερο. Η καταγραφή των μεγεθών πρέπει να γίνει ορθολογικά και όχι εμπειρικά ώστε να αποτιμηθεί το πραγματικό κόστος μιας εργασίας. Για τον υπολογισμό του ενδοεπιχειρισιακού κόστους πρέπει οπωσδήποτε να συμπεριληφθούν [30]:

- Το κόστος αγοράς του απαραίτητου εξοπλισμού, δηλαδή το κόστος των υλικών και των μηχανημάτων (servers, ups, συστήματα ασφαλείας κ.ά.) συν το κόστος του λογισμικού (εφαρμογές εμπορικής διαχείρισης , προγράμματα εξυπηρέτησης πελατών, CRM, ERP κ.ά.).
- Το κόστος συντήρησης και αναβάθμισης του εξοπλισμού και του λογισμικού που σκοπεύει μια επιχείρηση να προμηθευτεί, για τα επόμενα δύο (ή και περισσότερα) χρόνια.
- Τα χρήματα που θα δαπανηθούν για τη σύσταση κάποιου τμήματος (π.χ. του τμήματος πληροφορικής) καθώς και για την εκπαίδευση των εργαζομένων εκεί.
- Το ποσό που πρέπει να καταβληθεί για μισθούς στους εργαζόμενους που θα αναλάβουν να λειτουργήσουν αποκλειστικά τον εξοπλισμό ή που θα στελεχώσουν κάποιο συγκεκριμένο τμήμα (π.χ. το τμήμα πληροφορικής), για τα επόμενα δύο χρόνια.
- Τέλος, το κόστος των τηλεπικοινωνιακών τελών που σχετίζονται με τις υπηρεσίες/εργασίες, το κόστος σύνδεσης και χρήσης ίντερνετ, την κατανάλωση ηλεκτρικής ενέργειας, καθώς και άλλα συναφή λειτουργικά έξοδα, εφόσον υπάρχουν, για τα επόμενα δύο χρόνια.

Δεν είναι μόνο τα χρήματα που συντελούν στο κόστος μιας εργασίας. Πολύ σημαντικός παράγοντας, που δεν πρέπει να παραληφθεί, είναι, επίσης, και ο χρόνος που θα ξοδευτεί για την έρευνα αγοράς εξοπλισμού, για την κατάρτιση των προδιαγραφών ενός συστήματος και την παραμετροποίηση του, καθώς και για την εκπαίδευση του

προσωπικού. Ο χρόνος αυτός, αφού μετατραπεί σε εργατοώρες, προστίθεται στο προηγούμενο σύνολο, ώστε να υπάρχει μια πιο συνολική εικόνα του κόστους μια εργασίας ενδοεπιχειρησιακά.

Η σύγκριση του ποσού αυτού με το αντίστοιχο κόστος παροχής της υπηρεσίας από μία εταιρία outsourcing, θα οδηγήσει την επιχείρηση στη σωστή απόφαση. Στην περίπτωση του outsourcing πρέπει να συνυπολογιστεί ένα κονδύλι για μισθοδοσία στελέχους ή στελεχών που θα επιβλέπουν τη συγκεκριμένη διαδικασία, όπως, επίσης, και το κόστος διαρροών εμπιστευτικών πληροφοριών που μπορεί να οδηγήσει σε περιπέτειες νομικής φύσης και ανταγωνιστικά μειονεκτήματα [31].

2.2 Outsourcing network security

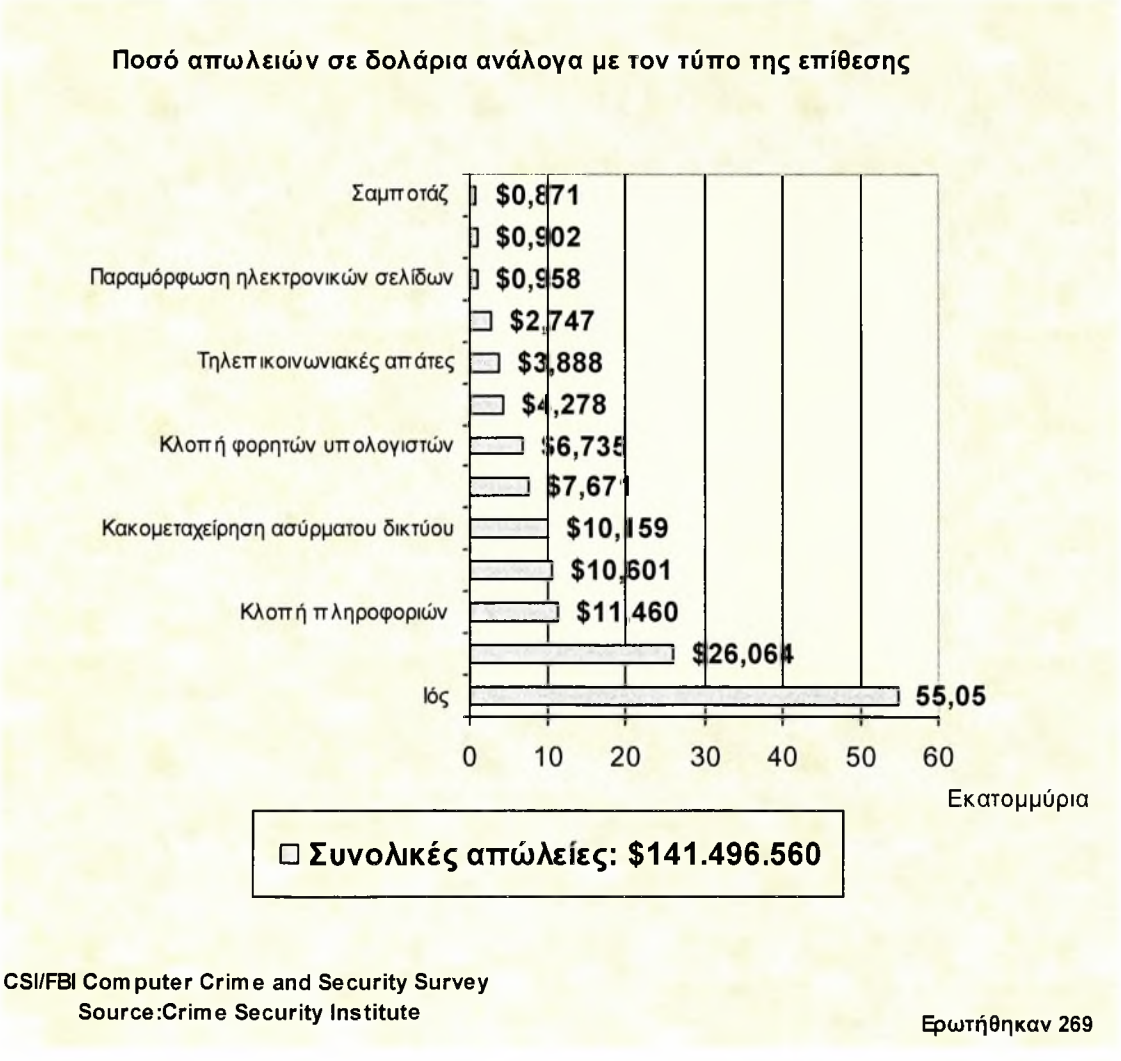
2.2.1 Εισαγωγή

Ένα δίκτυο το οποίο είναι 100% ασφαλές ακούγεται πολύ ελκυστικό. Μια επιχείρηση η οποία δεν αφήνει κανέναν να έχει πρόσβαση στα δεδομένα της ακούγεται λιγότερο ελκυστική. Υπάρχει ένα trade-off μεταξύ του επιπέδου ασφάλειας και του κόστους της απαγόρευσης πρόσβασης. Με το ίντερνετ να παίζει έναν όλο και πιο σημαντικό ρόλο στην βιωσιμότητα των επιχειρήσεων, ο κύριος στόχος τους, όσον αφορά την ασφάλεια, δεν είναι να κρατήσουν τους ανθρώπους έξω από το δίκτυο, αλλά να "οχυρώσουν" όσο το δυνατόν καλύτερα το δίκτυο τους. Όσο η επιχείρηση κερδίζει όλο και περισσότερα από τις συναλλαγές μέσω ίντερνετ, πρέπει να ξοδεύει όλο και περισσότερο χρόνο και χρήμα σε αυτήν τη βασική αλλά και δαπανηρή δραστηριότητα που λέγεται ασφάλεια δικτύων.

Η Gartner, εταιρία αναλυτών και συμβούλων στο Stamford των Ηνωμένων Πολιτειών, εκτιμά ότι μέσα στο 2006 το συνολικό παγκόσμιο ποσοστό χρημάτων που επενδύονται στην ασφάλεια θα ανέβει στο 17,6% του συνολικού ποσού που ξοδεύεται σε υπηρεσίες πληροφορικής, ενώ οι επενδύσεις στην υποδομή, όπως firewall και IDS, θα ανέλθει σε ένα ακόμα υψηλότερο 22% ετήσιο ποσοστό αύξησης [37].

Ανάγκη για ολοκληρωμένες λύσεις

Οι εταιρίες αντιμετωπίζουν πάντα την πρόκληση του να είναι όσο το δυνατόν περισσότερο ενημερωμένες για κάθε πιθανή απειλή, να παρέχουν ασφαλή επικοινωνία μέσω ίντερνετ για απομακρυσμένους υπαλλήλους, συνεργάτες και πελάτες και ταυτόχρονα να έχουν τον έλεγχο των χρημάτων που ξοδεύουν για τέτοιες δραστηριότητες. Ένα αμυντικό σύστημα από μόνο του δεν είναι αρκετό για να πετύχει τους παραπάνω στόχους. Πρέπει να συνδεθεί με ένα real-time σύστημα που προσφέρει έξυπνο έλεγχο ώστε να επιβεβαιώσει την προσαρμοστικότητα σε ένα συνεχώς αναπτυσσόμενο περιβάλλον.



Εικόνα 2: Απώλειες ανάλογα με τον τύπο της επίθεσης

Από έρευνα που έγινε από το CSI/FBI Computer Crime and Security Survey [28] το 2004, εκδόθηκε από το Crime Security Institute σε συνεργασία με το Federal Bureau of Investigation και φαίνεται στην εικόνα 2, προκύπτει ότι το 2004 έγιναν οι επιθέσεις με τις μεγαλύτερες απώλειες σε κέρδη όπως φαίνεται και από το διάγραμμα που ακολουθεί. Το 99% αυτών που ρωτήθηκαν ανέφεραν ότι χρησιμοποιούσαν λογισμικό antivirus, το 98% χρησιμοποιούσε firewalls και το 68% διέθετε IDSs. Είναι ολοφάνερο ότι μόνο με την εγκατάσταση της απαραίτητης τεχνολογίας για την ασφάλεια ενός δικτύου, η προστασία απέναντι σε πιθανές απειλές δεν είναι εγγυημένη. Στις περισσότερες περιπτώσεις απλά οδηγεί στη ψευδαίσθηση της ασφάλειας.

Λύση στο πρόβλημα

Πολλές λειτουργίες, όπως τα λογιστικά ή το ανθρώπινο δυναμικό, οι οποίες θεωρούνταν βασικές δραστηριότητες μιας εταιρίας και κατά συνέπεια εκτελούνταν ενδοεπιχειρησιακά τώρα επιλέγονται ως υπηρεσίες που θα ανατεθούν σε εξωτερικούς συνεργάτες, καθώς έχουν πλέον τυποποιηθεί. Θεωρητικά κάθε λειτουργία που δεν αποτελεί τον πυρήνα μια επιχείρησης μπορεί να ανατεθεί σε εξωτερικούς συνεργάτες αν το κόστος αυτής της ανάθεσης δεν είναι υψηλό. Η ασφάλεια των δικτύων δεν αποτελεί εξαίρεση.

Ολόκληρος ο τομέας της ασφάλειας ή μέρος αυτού ανατίθεται σε εξωτερικούς συνεργάτες. Η αυξημένη πολυπλοκότητα και η ταχύτητα με την οποία γίνονται σήμερα οι επιθέσεις απαιτούν έναν μόνιμο έλεγχο και ικανούς επαγγελματίες για να αντιδράσουν και να απαντήσουν. Σύμφωνα με τον αντιπρόεδρο του τομέα πληροφορικής της Blackboard Inc. (εταιρία E-learning που εδρεύει στην Ουάσιγκτον με τζίρο $111.4), η ασφάλεια χρειάζεται πιο ειδικευμένη τεχνογνωσία και έχει μεγαλύτερο νόημα να αναθέτεις σε τρίτους κάποιες υπηρεσίες, ώστε το προσωπικό να μπορεί να μείνει συγκεντρωμένο στο κύριο αντικείμενο της επιχείρησης [9]. Οι εξωτερικοί συνεργάτες αναλαμβάνουν την εικοσιτετράωρη επίβλεψη του δικτύου, το scanning, τις απαντήσεις σε διαφορά περιστατικά, και τη συντήρηση του δικτύου. Έτσι, δεν υπάρχει η ανάγκη για πρόσληψη και εκπαίδευση ατόμων πάνω στον τομέα αυτό.

Η διαχείριση της ασφάλειας είναι περισσότερο τέχνη παρά επιστήμη, αφού στην τελευταία ξέρουμε πως να καταφέρουμε να φτάσουμε στη βέλτιστη λύση. Στην περίπτωση της ασφάλειας δεν γνωρίζουμε καν ποιες είναι οι βέλτιστες λύσεις και το ίδιο και οι εταιρίες που παρέχουν διαχείριση της ασφάλειας. Ένα σύστημα ασφάλειας μπορεί να αποδειχθεί ένα πολύπλοκο σχέδιο. Μπορεί κάποιος να σκεφτεί ότι είναι ασφαλής εφόσον χρησιμοποιεί firewall και IDSs. Παρόλα' αυτά η κάθε επιχείρηση πρέπει να αποφασίσει ποια προϊόντα να αγοράσει, πως να κατανείμει το περιορισμένο κεφάλαιο που διαθέτει, σε έναν συνδυασμό αυτών των συσκευών ώστε να επιτύχει το μέγιστο επίπεδο ασφάλειας και πως να διαχειριστεί και να συντονίσει αυτές τις συσκευές, ώστε να ασφαλίσει το σύστημα αρκετά και να αποφύγει ψευδώς θετικούς συναγερμούς. Οι εταιρίες που διαχειρίζονται ασφάλεια αποκτούν εμπειρία πάνω σε όλα αυτά εξαιτίας της αφοσίωσης και τις εξειδίκευσης τους στον τομέα αυτόν [36].

Διαχωρισμός υπηρεσιών

Οι λειτουργίες της ασφάλειας που προσφέρονται θα μπορούσαν να χωριστούν σε πέντε κατηγορίες [33]:

1) Αποτίμηση,
2) Παρακολούθηση,
3) Έλεγχος απειλών και περιστατικών,
4) Διαχείριση ταυτότητας και
5) Συμβουλές.

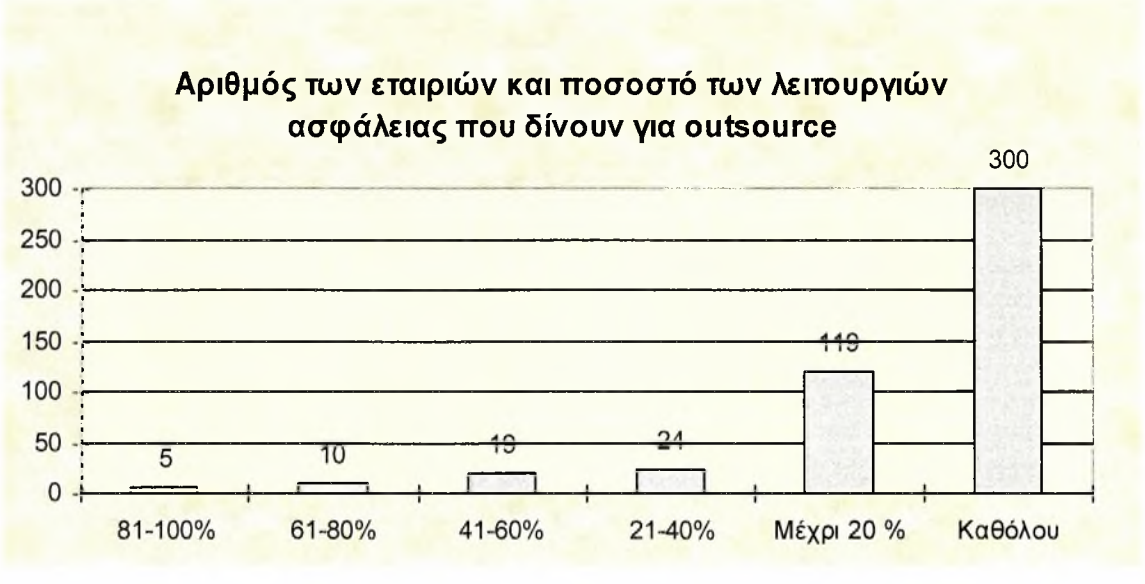
Η λίστα των διαχειρίσιμων υπηρεσιών ασφαλείας μεγαλώνει συνεχώς καθώς μεγαλώνει και η απαίτηση για καινούριες τεχνολογίες ασφάλειας. Οι εταιρίες που παρέχουν τις υπηρεσίες αυτές μπορεί να επικεντρωθούν σε μία από αυτές τις υπηρεσίες ή σε συνδυασμό αυτών, αναλόγως με την τεχνολογία που χρησιμοποιούν και το υπόβαθρο τους. Διαφορετικά πακέτα υπηρεσιών αναπτύχθηκαν για να καλύψουν τις διαφορετικές ανάγκες μεγάλων και μικρών επιχειρήσεων.

Σε αυτό το σημείο είναι σημαντικό να γίνει μια διάκριση μεταξύ των προϊόντων ασφάλειας και της διοίκησης της ασφάλειας. Η παροχή προϊόντων ασφάλειας, από τις επιχειρήσεις που τα παράγουν, περιλαμβάνει την παράδοση, την εγκατάσταση, τη

ρύθμιση των παραμέτρων ώστε να έχουν την καλύτερη δυνατή απόδοση, την τεχνική υποστήριξη για οποιοδήποτε πρόβλημα και, σε ορισμένες περιπτώσεις, τη διαχείριση αυτών των προϊόντων. Από την άλλη, η διαδικασία της διοίκησης περιλαμβάνει αποφάσεις για το πώς θα εφαρμοσθεί η ασφάλεια. Δηλαδή, αποφάσεις για το επίπεδο ασφάλειας, το πόσα firewall, IDSs, IPSs θα χρησιμοποιηθούν για την προστασία ενός συστήματος, ποια θα είναι η αρχιτεκτονική της ασφάλειας, τα δικαιώματα πρόσβασης των χρηστών, τις αντιδράσεις του συστήματος σε πιθανές επιθέσεις αλλά και το πόσο των χρημάτων που θα δαπανηθούν για την ασφάλεια του συστήματος. Πολλές φορές, όταν ένας πάροχος αναλάβει υπηρεσίες που ανήκουν και στις δύο αυτές περιοχές δημιουργούνται προβλήματα λόγω των αντικρουόμενων συμφερόντων που μπορεί να προκύψουν.

Στάση εταιριών - Επιφυλακτικότητα

Έρευνα, που έγινε και πάλι από το Computer Security Institute/FBI Computer Crime and Security Survey το 2003 [12], για το κατά πόσο οι εταιρίες δίνουν για outsource λειτουργίες της ασφάλειας έδειξε ότι οι περισσότεροι είναι ακόμα επιφυλακτικοί απέναντι σε μια τέτοια τεχνική. Συγκεκριμένα:



Πηγή: CSI 478 "Security Practitioners" Responded

Εικόνα 3: Αριθμός εταιριών και ποσοστό λειτουργιών ασφάλειας που δίνουν για outsource

Τα πράγματα, όμως, δείχνουν να αλλάζουν. Η Forester Research [16] προβλέπει ότι το ποσό που θα ξοδεύεται στην Ευρώπη σε τέτοιες υπηρεσίες θα ανέλθει ξαφνικά σε ένα ετήσιο ποσοστό αύξησης (compound annual growth rate, CAGR) 37% από το 2003 ως το 2008 ενώ στις ΗΠΑ το ποσοστό αυτό αγγίζει το 47.9% μεταξύ του 2002 και του 2006.

Η ανάθεση της ασφάλειας ενός δικτύου σε άλλους μπορεί να συγκριθεί με την ιατρική φροντίδα [1]. Όλοι δίνουμε για outsourcing την φροντίδα της υγείας μας με την έννοια του ότι δε λειτουργούμε ως γιατροί του εαυτού μας, ούτε κανείς προσλαμβάνει προσωπικό γιατρό. Το κόστος είναι σίγουρα ένας παράγοντας σε αυτήν την απόφαση αλλά υπάρχουν και άλλοι λόγοι. Μπορεί να χρειαστούμε έναν γιατρό 2 φορές το χρόνο, αλλά όταν τον χρειαστούμε μπορεί να τον θέλουμε αμέσως και μπορεί να χρειαστούμε συγκεκριμένης ειδικότητας γιατρούς. Μέσα από 100 διαφορετικές ειδικότητες γιατρών μπορεί να χρειαστούμε 2 από αυτούς και νωρίτερα δεν έχουμε ιδέα ποιες ειδικότητες θα χρειαστούμε. Κανείς δε θα σκεφτόταν να προσλάβει μια ομάδα γιατρών που να μας περιτριγυρίζουν μέχρι να αρρωστήσουμε, οπότε μπορεί να σκεφτούμε να αναθέσουμε τις ιατρικές μας ανάγκες σε μια κλινική για παράδειγμα. Με την ίδια λογική, έχει νόημα για μια εταιρία να δώσει για outsource την ασφάλεια του δικτύου της σε μια άλλη εταιρία η οποία απασχολεί μεγάλο αριθμό εργαζομένων, καθένας εξειδικευμένος σε διαφορετικό τομέα. Άλλωστε, η διαδικασία της ασφάλειας μοιάζει πολύ με αυτήν της υγείας: έξι εβδομάδες αδράνειας μπορεί να ακολουθηθούν από οκτώ ώρες πανικού και μετά εφτά εβδομάδες αδράνειας μπορεί να ακολουθηθούν από έξι ώρες πανικού. Οι επιθέσεις απέναντι σε έναν μόνο οργανισμό δεν συμβαίνουν τόσο συχνά ώστε να κρατήσουν το προσωπικό σε εγρήγορση. Για να επιστρέψουμε στο παράδειγμα της υγείας εμπιστευόμαστε περισσότερο τους γιατρούς οι οποίοι βλέπουν τον έναν ασθενή πίσω από τον άλλον και αποκτούν εμπειρία μέσω αυτής της διαδικασίας. Αντιστοίχως, είναι πιο λογικό να εμπιστευτούμε μια εταιρία που παρέχει ασφάλεια, η οποία εξετάζει συνεχώς καινούριες μορφές επιθέσεων σε δίκτυα και ξέρει ακριβώς πώς να αντιδράσει γιατί κατά πάσα πιθανότητα έχει δει κάποιο παρόμοιο περιστατικό.

2.2.2 Επιλογή των υπηρεσιών για outsourcing

Ένα ερώτημα που προκύπτει είναι το πόσες και ποιες υπηρεσίες θα πρέπει να ανατεθούν σε εξωτερικούς συνεργάτες. Το σίγουρο είναι ότι δεν δίνονται όλα για outsource, γιατί σε κάποια θέματα το outsourcing δεν είναι αποτελεσματικό. Αυτά έχουν να κάνουν με δραστηριότητες κρίσιμες και άμεσα συνδεδεμένες με την επιχείρηση ή με δραστηριότητες που είναι πολύ ακριβές να τις αναθέσεις αλλού. Για παράδειγμα, δραστηριότητες που έχουν να κάνουν με τα κυβερνητικά πλαίσια μιας εταιρίας, όπως οι πολιτικές ασφάλειας, πρέπει να παραμένουν στην επιχείρηση. Από την άλλη, δραστηριότητες όπως η διαχείριση των διαφόρων μηχανημάτων ή ο έλεγχος και η παρακολούθηση της ασφάλειας, είναι καλό να ανατίθενται σε εξωτερικούς συνεργάτες [39].

Κερδοφόρα είναι, συνήθως, η ανάθεση του ελέγχου ευπαθειών, email και web και η παρακολούθηση και διαχείριση firewall, IDSs και IPSs σε μια εταιρία διαχείρισης ασφάλειας [1]. Μπορούν επίσης οι εταιρίες-πάροχοι να συμβουλεύουν τους πελάτες τους. Δεν μπορούνε όμως να πάρουν τον έλεγχο ολόκληρης της διαδικασίας. Δεν μπορούν να αποφασίσουν πως θα αλληλεπιδρά η ασφάλεια με την υπόλοιπη επιχείρηση. Για παράδειγμα, ενώ μπορούνε να εντοπίσουν έναν hacker μέσα σε ένα δίκτυο και να καταλάβουν τι κάνει, δεν ξέρουν ποια θέλει να είναι η απάντηση σε αυτό η εταιρία-πελάτης. Μπορούνε να βρούνε έναν εισβολέα που επιτίθεται σε ένα δίκτυο αλλά δεν γνωρίζουν κατά πόσο είναι μοχθηρός ή κατά πόσο εκτελεί εξουσιοδοτημένο έλεγχο. Υπάρχουν επιχειρήσεις με πολύ ασφαλή δίκτυα που διαχειρίζονται κρίσιμες πληροφορίες οι οποίες θα προτιμούσαν να αποσυνδεθούν από το ίντερνετ εάν κάποιος hacker τριγυρίζει στο δίκτυο τους. Υπάρχουν άλλες που το να μείνουν αποσυνδεδεμένες από το ίντερνετ έστω και ένα λεπτό μπορεί να είναι καταστροφικό για αυτούς και προτιμούν λύσεις στις οποίες οι υπηρεσίες τους συνεχίζουν να λειτουργούν. Οι εταιρίες outsourcing δεν μπορούν να γνωρίζουν όλες αυτές τις παραμέτρους, οπότε και ολόκληρη η διαδικασία διαμόρφωσης της πολιτικής ασφάλειας πρέπει να μένει ενδοεπιχειρησιακά. Η εταιρία που αγοράζει υπηρεσίες ασφάλειας θα πρέπει να διατηρεί τον έλεγχο της διαχείρισης, ενώ αντιθέτως, οι εταιρίες που παρέχουν τις υπηρεσίες πρέπει να

προσφέρουν χρήσιμες και αποτελεσματικές υπηρεσίες. Με αυτόν τον τρόπο κερδίζουν και οι δύο.

Ένας άλλος τρόπος για να διαλέξει μια εταιρία ποιες υπηρεσίες θα δώσει για outsourcing, είναι να αποφασίσει ποιες είναι εκείνες οι υπηρεσίες με τις οποίες αντιμετωπίζει πρόβλημα [9]. Για παράδειγμα, αν συνειδητοποιήσει ότι δεν μπορεί να τα βγάλει πέρα με την ποικιλία των ευπαθειών που εμφανίζονται καθημερινά ή ότι δε θα τα βγάλει πέρα με τη σφοδρότατη επίθεση των υπογραφών των συστημάτων ανίχνευσης εισβολών (IDS), τότε αυτά είναι τα αντικείμενα που πρέπει να δώσει για outsource. Με αυτόν τον τρόπο θα απαλλαχθεί από δραστηριότητες που κατανάλωναν πολύτιμο χρόνο, τον οποίον μπορεί πλέον να διαθέσει αλλού.

Τέλος, άλλος ένας παράγοντας που μπορεί να επηρεάσει την επιλογή των υπηρεσιών outsourcing είναι το κόστος μετάβασης (παρακάτω επεξηγείται η έννοια του κόστους μετάβασης). Αντί της μεγάλης εξειδίκευσης, όπου οι εταιρίες δίνουν τα πάντα για outsource εκτός από μια κύρια δραστηριότητα, οι περισσότερες επιχειρήσεις διαλέγουν να κρατήσουν την πλειοψηφία των λειτουργιών ενδοεπιχειρησιακά προκειμένου να γλιτώσουν το κόστος μετάβασης. Με το να κρατήσεις μια λειτουργία ενδοεπιχειρησικακά κερδίζεις από το κόστος μετάβασης, αλλά με το να κρατάς πολλαπλές λειτουργίες μέσα στην επιχείρηση μπορεί να οδηγήσει στην απώλεια της αποτελεσματικότητας της παραγωγής. Από την σκοπιά του κόστους μετάβασης, το κατά πόσο θα κρατήσεις μια λειτουργία ενδοεπιχειρησιακά ή όχι εξαρτάται από το αν το κόστος μετάβασης είναι μεγαλύτερο από όσα θα κερδίσει η εταιρία από την εξειδίκευση [34].

2.2.3 Τα οφέλη του outsourcing στην ασφάλεια δικτύων

Τα πλεονεκτήματα που πηγάζουν από την ανάθεση της ασφάλειας του δικτύου μιας εταιρίας σε μια άλλη, αφορούν πολλούς και διαφορετικούς τομείς. Ο παρακάτω πίνακας συγκεντρώνει τα πλεονεκτήματα αυτά:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ
Συνεχής ενημέρωση: Διαρκής ενημέρωση για τις τελευταίες απειλές, όσον αφορά στην ασφάλεια δικτύων και για τον τρόπο αντίδρασης σε αυτές. Η ασφάλεια των δικτύων δεν είναι κάτι στατικό αλλά αλλάζει συνεχώς. Καθημερινά καινούργιοι ιοί δημιουργούνται, πολυμήχανοι εισβολείς επινοούν καινούργιες μορφές επιθέσεων και οι πωλητές προϊόντων ασφάλειας απαντούν με τα αντίστοιχα μέτρα. Το να αναθέτεις την ασφάλεια του δικτύου σου αλλού, σε απελευθερώνει από τη συνεχή πρόκληση του να μένεις πάντα ένα βήμα μπροστά από το δυναμικό κόσμο των απειλών.
Ανθρώπινο δυναμικό: Οι εταιρίες που επιλέγουν το outsourcing αποφεύγουν τη διαδικασία της εύρεσης, πρόσληψης, και μίσθωσης επαγγελματιών στον τομέα της ασφάλειας. Χρειάζονται από πέντε μέχρι εφτά υπάλληλοι, ίσως και περισσότεροι αν μέσα σε αυτούς βάλουμε και τους επιβλέποντες, για να έχεις προσωπικό ειδικευμένο στην ασφάλεια 24 ώρες την ημέρα 365 μέρες το χρόνο [1]. Συνήθως είναι δύσκολο να βρεις ταλαντούχους ανθρώπους αλλά και να καταφέρεις να ανταποκριθείς, από οικονομικής άποψης, στους πολύ υψηλούς μισθούς τους. Από την άλλη, το να εκπαιδεύσεις το ήδη υπάρχων προσωπικό είναι ακριβή διαδικασία και διαρκεί πολύ. Με το outsourcing η εταιρία απαλλάσσεται από ένα πολύ σημαντικό βάρος, αυτό της διαχείρισης ανθρώπινου δυναμικού.
Ελαχιστοποίηση κόστους: Μέσω του outsourcing επιτυγχάνεται η ελαχιστοποίηση ή και η εκμηδένιση του κόστους για την αγορά λογισμικού και υλικού για την προστασία ενάντια σε ιούς, για την ανίχνευση εισβολέων και για το φιλτράρισμα των περιεχομένων των δοσοληψιών μέσω ίντερνετ. Ορισμένες εταιρίες συνεχίζουν να διαθέτουν τα δικά τους εργαλεία ασφάλειας ακόμα και μετά τη σύναψη μιας σχέσης outsourcing, σε άλλες, όμως, μπορεί να τα διαθέσει η εταιρία-πάροχος. Σε αυτήν την περίπτωση, το κόστος για την απόκτηση των απαραίτητων εργαλείων επωμίζονται όλοι οι πελάτες της εταιρίας-παρόχου με αποτέλεσμα το κόστος για κάθε πελάτη να είναι μικρότερο. Αλλά ακόμα και στην πρώτη περίπτωση, οι εταιρίες που παρέχουν την ασφάλεια συνήθως διαθέτουν εξελιγμένα εργαλεία ασφάλειας, που είναι δύσκολο, από πλευράς κόστους, για μια εταιρία να αποκτήσει από μόνη της.

Ανακατανομή πόρων: Η ανάθεση ορισμένων υπηρεσιών ασφάλειας σε τρίτους εξοικονομεί ένα μεγάλο χρηματικό ποσό το οποίο προοριζόταν για μια απαραίτητη μεν δραστηριότητα, η οποία, όμως, δεν αποτελεί την βασική δραστηριότητα μιας εταιρίας. Οι περισσότερες εταιρίες προσφέρουν προϊόντα και υπηρεσίες, είτε σχετικές με τον τομέα της πληροφορικής, είτε όχι και όχι ασφάλεια δικτύων. Είναι πιο φρόνιμο να ξοδεύεις μεγάλα χρηματικά ποσά σε πρωτοβουλίες που έχουν να κάνουν με τον κύριο προϊόν-υπηρεσία της εταιρίας σου γιατί αποφέρουν μεγαλύτερη αποδοτικότητα και αυξάνουν το ανταγωνιστικό πλεονέκτημα.

Απελευθέρωση χρόνου: Ο πάροχος ελέγχει καθημερινά όλα τα περιστατικά και προωθεί στους πελάτες της μόνο εκείνα τα οποία χαρακτηρίζονται ως σοβαρά. Με τον τρόπο αυτό, η εκάστοτε εταιρία βλέπει μόνο όσα χρειάζεται να δει, κερδίζοντας έτσι πολύ χρόνο για άλλες δραστηριότητες. Μέρος του χρόνου αυτού μπορεί να διατεθεί για τη μελέτη άλλων μορφών ασφάλειας που θα μπορούσε να υιοθετήσει η εταιρία ή και για την ενδυνάμωση των δραστηριοτήτων εκείνων που συνεχίζουν να διαχειρίζονται ενδοεπιχειρησιακά. Οι δραστηριότητες αυτές θα ήταν δύσκολο να πραγματοποιηθούν εάν η διαχείριση της ασφάλειας παρέμενε ενδοεπιχειρισιακά.

Εστίαση στον πυρήνα της επιχείρησης: Δίνεται, επίσης, η δυνατότητα να δοθεί μεγαλύτερη προσοχή στην ανάπτυξη προϊόντων–υπηρεσιών που παράγει η επιχείρηση. Πολύς χρόνος μπορεί να αναλωθεί σε θέματα, σημαντικά μεν, δευτερεύοντα δε ως προς τον κύριο σκοπό της εταιρίας, όπως αυτό της ασφάλειας. Με το outsourcing ο χρόνος αυτός μπορεί να αξιοποιηθεί καλύτερα, αφιερώνοντας τον στην ανάπτυξη νέων ιδεών, μεθόδων, προϊόντων και υπηρεσιών καθώς και στην βελτίωση ή και βελτιστοποίηση των ήδη υπαρχόντων.

Ολοκληρωμένη άποψη: Επιπλέον, δημιουργείται μια πιο σφαιρική άποψη, μέσω των εξωτερικών συνεργατών, για τον τομέα της ασφάλειας. Το να διαχειρίζεται κανείς την ασφάλεια είναι αδύνατον εάν η οπτική του σκοπιά είναι μονοδιάστατη και περιορίζεται μόνο σε ένα σημείο, όπως για παράδειγμα, ένα firewall. Εφόσον τα δίκτυα των επιχειρήσεων γίνονται όλο και πιο αλληλοεξαρτώμενα, είναι λάθος να περιορίζεται κανείς σε ένα και μοναδικό δίκτυο. Οι εταιρίες outsourcing έχουν την ικανότητα να συσχετίζουν πληροφορίες που συλλέγουν από πολλές επιχειρήσεις, τις οποίες πιθανόν να διαχειρίζονται. Ένας οργανισμός ακόμα και εάν είναι ο πιο ικανός και έχει τεράστια

χρηματικά ποσά να διαθέσει για την ασφάλεια, θα είχε ένα πολύ μεγάλο μειονέκτημα αν περιοριζόταν μόνο στα όρια τις δικής του επιχείρησης. Δε θα ήταν ικανός να βλέπει τι συμβαίνει στο διαδίκτυο όσον αφορά στις απειλές, αλλά ούτε να χρησιμοποιήσει τη γνώση και την εμπειρία άλλων οργανισμών για να πάρει τα απαραίτητα μέτρα και τις σωστές λύσεις. Οι περισσότερες επιχειρήσεις σήμερα αντιδρούν ως επί τω πλείστων αφού έχουν ήδη δεχτεί ένα χτύπημα. Με το outsourcing, όμως, ο χρόνος απόκρισης μειώνεται αισθητά. Οι εταιρίες outsourcing έχουν την ικανότητα να βλέπουν τι συμβαίνει σε πολλές επιχειρήσεις ταυτόχρονα [4]. Χτυπήματα που συνέβησαν στη μία μπορούν εύκολα να αποφευχθούν στις υπόλοιπες, κάτι το οποίο δε θα μπορούσε να γίνει εάν η ίδια η επιχείρηση είχε τον έλεγχο της ασφάλειας της. Το προσωπικό των εταιριών outsourcing είναι συνεχώς σε εγρήγορση και ενημερώνεται συνεχώς για όλες τις τελευταίες εξελίξεις.

Ενημέρωση για διαδικαστικά θέματα: Επιπρόσθετα, επιτυγχάνεται η ενημέρωση για τις απαιτήσεις της ασφάλειας σε άλλα μέρη του κόσμου [9], όπως για παράδειγμα για τη νομοθεσία των Ηνωμένων Πολιτειών. Είναι φυσικό, οι περισσότερες μικρομεσαίες επιχειρήσεις να μην γνωρίζουν ακριβώς το νομοθετικό πλαίσιο γύρω από το οποίο πρέπει να κινηθούν. Μια εταιρία που ασχολείται αποκλειστικά με αυτό, γνωρίζει τις απαιτήσεις της παγκόσμιας νομοθεσίας αλλά και της ελληνικής σε θέματα ασφάλειας και μπορεί να φροντίσει ώστε η υλοποίηση της ασφάλειας να συμβαδίζει με αυτές.

Γνώση: Μέσα από το outsourcing μια επιχείρηση καταφέρνει να μάθει περισσότερα πράγματα από τους εξωτερικούς συνεργάτες. Η επαφή και η συνεργασία με ανθρώπους καταρτισμένους στο είδος τους έχει ως αποτέλεσμα το προσωπικό της εταιρίας να κερδίσει ένα μέρος της γνώσης των συνεργατών και αυτό με τη σειρά του έχει ως αποτέλεσμα την καλύτερη απόδοση τους [9].

Εμπιστοσύνη: Η ανάμιξη μιας εταιρίας παροχής υπηρεσιών ασφάλειας με μεγάλο όνομα και αναγνωρισμένη πορεία στο χώρο αυτόν μπορεί να βοηθήσει στη δημιουργία εμπιστοσύνης μεταξύ του οργανισμού και των πελατών οι οποίοι μπορεί να μη γνώριζαν την εταιρία και τις ικανότητες της σε θέματα ασφάλειας.

Μεγιστοποίηση του κέρδους από προηγούμενες επενδύσεις: Συνήθως οι περισσότερες επιχειρήσεις, πριν προβούν στο outsourcing, διαθέτουν ήδη υποδομή για την ασφάλεια των συστημάτων τους, η οποία, τις περισσότερες φορές, αποτελεί

συσσώρευση πολύχρονων επενδύσεων σε λύσεις ασφάλειας. Μια εταιρία που παρέχει outsourcing έχει τη δυνατότητα να βελτιώσει την υπάρχουσα υποδομή, με σκοπό τη μεγιστοποίηση της απόδοσης της, κάτι που δεν μπορούν να κάνουν οι περισσότερες επιχειρήσεις αφού δε διαθέτουν την απαραίτητη πείρα [29].

Πίνακας 1: Πλεονεκτήματα του Outsourcing

Πολύ σημαντικό ρόλο παίζει και ο τρόπος που θα γνωστοποιήσουν τα στελέχη μιας εταιρίας στους υπαλλήλους της, τη δημιουργία μιας σχέσης outsourcing. Το προσωπικό μιας εταιρίας πρέπει να συνεργαστεί σωστά και αποδοτικά με τους εξωτερικούς συνεργάτες της. Ο υπεύθυνος της ασφάλειας μιας επιχείρησης πρέπει να είναι σίγουρος ότι το προσωπικό καταλαβαίνει γιατί γίνεται μια τέτοια κίνηση και ότι είναι συγκεντρωμένοι στο σκοπό τους [9]. Ακόμα και μερικοί διευθυντές αντιδρούν σε μια τέτοια ιδέα γιατί φοβούνται ότι θα χάσουν τον οργανωτικό έλεγχο της διαδικασίας και των πόρων. Στην πραγματικότητα, όμως, μέσα από το outsourcing ο διοικητικός έλεγχος μπορεί να εμπλουτιστεί περαιτέρω μέσα από τη συλλογή δεδομένων και τις συχνές αναφορές κάτι το οποίο, στις περισσότερες των περιπτώσεων, δε συμβαίνει όταν ο έλεγχος της ασφάλειας μένει ενδοεπιχειρησιακά. Το αποτέλεσμα είναι ένα υψηλό επίπεδο διοικητικού ελέγχου το οποίο δεν υπήρχε μέχρι τότε.

Τέλος, θα πρέπει να αναφερθεί ότι εταιρίες οι οποίες διαχειρίζονται την ασφάλεια πολλών άλλων εταιριών ή οργανισμών, που έχουν δηλαδή τη δυνατότητα ενός κεντρικού ελέγχου πολλών δικτύων ταυτόχρονα, έχουν μεγαλύτερη αξιοπιστία στις αποφάσεις τους από στατιστικής πλευράς.

Σε ένα πετυχημένο παράδειγμα του πανεπιστημιακού νοσοκομείου του Κολοράντο [15], με την ανάθεση της ασφάλειας του δικτύου σε εξωτερικούς συνεργάτες, οι οποίοι το ελέγχουν 24 ώρες τη μέρα, 7 ημέρες της εβδομάδας, το νοσοκομείο γλίτωσε πάνω από 100,000 δολάρια ετησίως από έξοδα που θα προορίζονταν στην πρόσληψη και εκπαίδευση προσωπικού που θα ασχολούνταν με την προστασία του δικτύου. Σε αυτό πρέπει να προστεθεί το πλεονέκτημα της απελευθέρωσης προσωπικού το οποίο μπορεί τώρα να επικεντρωθεί σε πιο στρατηγικά σημεία ώστε το νοσοκομείο να λειτουργεί πιο αποτελεσματικά. Χαρακτηριστικά αναφέρεται: «Αυτό που μετράει περισσότερο είναι ότι

ποτέ δεν ανησυχούμε για την ασφάλεια του δικτύου και ποιος το ελέγχει όταν τελειώνει η βάρδια του προσωπικού».

Παρακάτω ακολουθεί ένας πίνακας ο οποίος συγκρίνει το βαθμό προσπάθειας και το κόστος και για τις δύο περιπτώσεις, για έναν οργανισμό που απασχολεί 100-200 εργαζομένους [37].

Βασικά οφέλη	**Προσπάθεια εντός της επιχείρησης**	**Βέλτιστη προσπάθεια εντός της επιχείρησης**	**Περίπτωση outsourcing-ελάχιστη ασφάλεια**
Απαιτήσεις προσωπικού	1 υπάλληλος	5 υπάλληλοι (κάλυψη 24x7)	Προσωπικό της εταιρείας
Σχεδιασμός και αρχιτεκτονική	Ίσως	Πεπειραμένος	Πεπειραμένος
Παρακολούθηση	8πμ-5πμ	24x7x365	24x7x365
Διοίκηση	8πμ-5πμ	24x7x365	24x7x365
Αντίγραφα ασφαλείας	Ίσως	Καθημερινά	Καθημερινά
Έλεγχος ευπαθειών	Ίσως	Τριμηνιαία	Μηνιαία
Κόστη	**Προσπάθεια εντός της επιχείρησης**	**Βέλτιστη προσπάθεια εντός της επιχείρησης**	**Περίπτωση outsourcing-ελάχιστη ασφάλεια**
Μισθοί	$100k+25% επιδόματα ασφάλειας και κόστη διοίκησης	$100k+25% επιδόματα ασφάλειας και κόστη διοίκησης (ανά εργαζόμενο)	-
Διευθυντής	25% time @ $150k pa.	75% time @ $150k pa.	-
Εκπαίδευση	$5k	$5k ανά εργαζόμενο(x5)	-
Υλικό	$4k για PC,$2k για δρομολογητές	$20k για 5 PCs, $4k για 2 δρομολογητές	-
Λογισμικό	%0- freeware έκδοση	%25k για λογισμικό για επικοινωνίες	-
Υπηρεσίες	$100/μήνα	20% για PCs,10% για δρομολογητές, 15% για λογισμικό	$2500-$5000/μήνα
Συνολικό ετήσιο κόστος	**$174.000**	**$794.650**	**$30.000-$50.000**

Πηγή: Βασισμένος σε μια έρευνα της Lucent, Keith White, 2005

Πίνακας 2: Υπηρεσίες διαχείρισης ασφάλειας vs. Διατήρηση υπηρεσιών μέσα στην επιχείρηση

2.2.4 Μειονεκτήματα και κίνδυνοι του outsourcing στην ασφάλεια δικτύων

Πάντα σε μια σχέση υπάρχει και η αρνητική πλευρά. Στον Πίνακα 3 φαίνονται τα μειονεκτήματα του outsourcing.

ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Εμπιστοσύνη: Όταν αποφασίσει κάποιος να δώσει για outsource την ασφάλεια του δικτύου του, επιτρέπει σε κάποιους να έχουν πρόσβαση στο περιβάλλον του. Για αυτό πρέπει να ελέγχεται το επίπεδο πρόσβασης του παρόχου και να επιβεβαιώνεται ότι οι πολιτικές που χρησιμοποιούνται για την επιλογή και τον έλεγχο των υπαλλήλων τους, ταυτίζονται με τα πρότυπα της εταιρίας. Είναι, όμως, απαραίτητη και η ύπαρξη εμπιστοσύνης μεταξύ των δύο μερών. Διαφορετικά τα πράγματα μπορεί να πάρουν άσχημη τροπή και θα υπάρχει η αμφιβολία και η ανησυχία ότι το δίκτυο κινδυνεύει.
Κόστος επιπρόσθετων υπηρεσιών: Στην περίπτωση που κάποια αλλαγή στον τρόπο διαχείρισης της ασφάλειας κριθεί απαραίτητη, η οποία, όμως, δεν αναφέρεται ρητά στο συμβόλαιο μεταξύ των δύο μερών, τότε το κόστος για την εταιρία-πελάτη μπορεί να αυξηθεί σημαντικά σε σχέση με το κόστος που θα προέκυπτε αν διαχειριζόταν η ίδια τις υπηρεσίες ασφάλειας.
Εγκλωβισμός: Ένας πάροχος υπηρεσιών ασφάλειας προκειμένου να εμφανίσει το outsourcing ελκυστικό συνήθως προσφέρει αρχικά μια πολύ ανταγωνιστική τιμή [34]. Μετά την υπογραφή του συμβολαίου, εάν ο πελάτης έχει επενδύσει σε συσκευές, που είναι απαραίτητες για τη συνεργασία του με τον συγκεκριμένο πάροχο, δεν μπορεί εύκολα να αλλάξει συνεργάτη λόγω του κόστους μετάβασης. Ο πάροχος, έχοντας γνώση της κατάστασης, συνήθως ανεβάζει τις τιμές πάνω από τα επίπεδα της αγοράς. Το παραπάνω φαινόμενο είναι γνωστό ως το φαινόμενο του εγκλωβισμού, όπου ο πελάτης αναγκάζεται να παραμείνει σε έναν συγκεκριμένο πάροχο γιατί το κόστος μετάβασης είναι πολύ υψηλό.

Βιωσιμότητα προμηθευτών: Πρέπει να δοθεί πολύ προσοχή στην επιλογή του παρόχου και να επιλεγούν εταιρίες που είναι leaders στον τομέα τους και έχουν μεγάλη ιστορία στο outsourcing. Πολλές εταιρίες ασφάλειας, που δραστηριοποιούνταν στο εξωτερικό, έκλεισαν και βρέθηκαν οι πελάτες τους σε μια κατάσταση δύσκολη να τη χειριστούν. Σύνηθες φαινόμενο είναι, επίσης, η συγχώνευση εταιριών, κάνοντας πολλούς να ανησυχούν για την περίπτωση που θα συνάψουν συμβόλαιο με μια εταιρία η οποία μετά από κάποιο διάστημα δε θα υπάρχει. Χρειάζεται, επομένως, ιδιαίτερη προσοχή στην αναζήτηση του προμηθευτή υπηρεσιών ασφάλειας [4].

Πίνακας 3: Μειονεκτήματα του outsourcing

Σε έρευνα από την Booz Allen Hamilton [26], το 30% αυτών που ρωτήθηκαν απάντησαν ότι είναι λιγότερο ικανοποιημένοι με τα αποτελέσματα του outsourcing σε σχέση με αυτό που περίμεναν. Περισσότεροι από το 20% αυτών που παρακολούθησαν την παγκόσμια σύνοδο κορυφής για το outsourcing το 2004 (The 2004 Outsourcing World Summit) είπαν ότι χάνουν περίπου το ένα τέταρτο της αξίας των συμβολαίων τους εξαιτίας των φτωχών εργασιακών σχέσεων μεταξύ των εταιριών. Η Simmons & Simmons αναφέρει ότι το 90% των οργανισμών βλέπουν πολλά θέματα να προκύπτουν μεταξύ των δύο μεριών, πολλά εκ των οποίων οδηγούν σε προσφυγές στο δικαστήριο και αντιδικίες. Μερικά από τα πιο κοινά προβλήματα που προκύπτουν είναι χαμηλή απόδοση σε σχέση με τα συμφωνημένα επίπεδα, απροσδόκητες χρεώσεις για πράγματα τα οποία ο πελάτης πίστευε ότι συμπεριλαμβάνονταν στην αρχική συμφωνία και αδυναμία εκπλήρωσης των ορόσημων /σημαντικών επιτευγμάτων (missed milestones).

2.2.5 Προτεινόμενες λύσεις για τη διασφάλιση της μυστικότητας

Όπως αναφέρθηκε, στην περίπτωση του outsourcing δίνεται στον πάροχο η δυνατότητα πρόσβασης στο δίκτυο του πελάτη. Επίσης, η ύπαρξη συνεχούς ανταλλαγής δεδομένων μεταξύ του πελάτη και του παρόχου δημιουργεί την ανάγκη για την ανάπτυξη μεθόδων που διασφαλίζουν τη μυστικότητα αλλά και την ακεραιότητα των δεδομένων που ανταλλάσσονται μεταξύ των δύο μερών.

Στο [31] προτείνεται ένας τρόπος για τη διασφάλιση της μυστικότητας των πληροφοριών που διακινούνται μεταξύ των εταιριών–παρόχων και των εταιριών-πελατών. Όπως είναι ήδη γνωστό οι πληροφορίες που διαχειρίζεται η εταιρία-πάροχος μπορεί να είναι ευαίσθητα δεδομένα που πιθανόν προστατεύονται από νόμους, ή πολύτιμες πληροφορίες για τους ανταγωνιστές των πελατών τους ακόμα και για επίδοξους hacker. Η λύση που προτείνεται είναι η ανωνυμία των log παρακολούθησης που στέλνονται στον πάροχο από τον πελάτη. Ο σκοπός αυτής της διαδικασίας είναι ο περιορισμός των δεδομένων που περιέχονται στα log και μπορεί να χαθούν κατά τη διάρκεια της επικοινωνίας πελάτη-παρόχου, αλλά, παράλληλα, να είναι αρκετά ώστε να επιτρέπεται στον πάροχο να κάνει ανάλυση της ασφάλειας. Οι τεχνικές της ανωνυμίας απομακρύνουν ευαίσθητες πληροφορίες, όπως για παράδειγμα τις ταυτότητες των επικοινωνούντων με την εταιρία-πελάτη από τα log πριν αυτά σταλθούν στον πάροχο. Τα log στέλνονται είτε σε πραγματικό χρόνο, είτε περιοδικά. Ο πάροχος κάνει τις απαραίτητες αναλύσεις και στέλνει προειδοποιήσεις πίσω στην εταιρία. Οι προειδοποιήσεις μπορεί να αφορούν ανωνυμοποιημένες ταυτότητες τις οποίες ο πελάτης μπορεί να μεταφράσει και να πάρει τα αντίστοιχα μέτρα

Η έρευνα τους επικεντρώνεται σε δύο είδη log: τα NetFlow log και syslog. Οι τεχνικές ανωνυμίας που προτείνουν είναι οι εξής:

1. **Ανωνυμία IP διευθύνσεων:** Απόκρυψη των διευθύνσεων της πηγής ή του προορισμού μιας επικοινωνίας. Υπάρχουν τρεις τύποι αυτού του είδους:

   α) *Κουτσούρεμα (truncation)*: Διαλέγονται τα λιγότερα σημαντικά bit μιας IP διεύθυνσης για να απομακρυνθούν από αυτήν. Σε περιπτώσεις που το network domain είναι σχετικά μικρό η μέθοδος αυτή μπορεί να σπάσει. Στην αντίθετη περίπτωση είναι μια ικανοποιητική τεχνική.

   β) *Τυχαίες μεταθέσεις:* Για να γίνει συνεπής η ανωνυμοποίηση μπορεί να χρησιμοποιηθεί μια τιμή η οποία θα παράγει κάθε φορά τις ίδιες μεταθέσεις στην ίδια IP διεύθυνση. Εάν χαθεί αυτή η τιμή, η τεχνική των τυχαίων μεταθέσεων δεν μπορεί να αντιστραφεί για να βρεθεί η αρχική διεύθυνση.

γ) *Διατήρηση του προθέματος:* Είναι μια ειδική περίπτωση μεταθέσεων. Δύο ανωνυμοποιημένες IP διευθύνσεις ταιριάζουν σε ένα πρόθεμα εάν και μόνο εάν και οι κανονικές IP διευθύνσεις ταιριάζουν στο ίδιο πρόθεμα. Αυτή η τεχνική διατηρεί αρκετές πληροφορίες, ώστε να είναι δυνατόν να αποκαλυφθεί αν μια επίθεση είναι συντονισμένη ή είναι ανεξάρτητο γεγονός.

2. Ανωνυμία χρονοσφραγίδων: Απόκρυψη των πληροφοριών σχετικά με το χρόνο που συνέβη ένα γεγονός. Υπάρχουν τρεις τύποι:

α) *Εκμηδένιση μονάδων του χρόνου:* Μπορεί να σβηστεί για παράδειγμα η ώρα ή τα δευτερόλεπτα που συνέβη ένα γεγονός αλλά να μπορέσουμε να πάρουμε αυτές τις πληροφορίες από τη διάρκεια του γεγονότος. Η διαδικασία μπορεί να συμβεί και αντίστροφα, δηλαδή, να σβηστεί η διάρκεια αλλά να έχουμε τους χρόνους εκκίνησης και τερματισμού.

β) *Τυχαία ολίσθηση του χρόνου:* Όλες οι χρονοσφραγίδες ολισθαίνουν κατά έναν τυχαίο αριθμό αφήνοντας τα σχετικά διαστήματα μεταξύ των γεγονότων και τις διάρκειες αυτών ανεπηρέαστα. Ορισμένες φορές είναι πιο σημαντικό να γνωρίζουμε τις παραπάνω πληροφορίες από το να ξέρουμε την ακριβή ώρα και μέρα ενός περιστατικού.

γ) *Απαρίθμηση*: Όλες οι χρονικές πληροφορίες απομακρύνονται εκτός από τη σειρά των γεγονότων. Διαλέγεται ένας τυχαίος χρόνος για την πρώτη εγγραφή και ολισθαίνει τους χρόνους εκκίνησης όλων των υπολοίπων, ώστε να ισαπέχουν μεταξύ τους και να διατηρούν τη μεταξύ τους σειρά. Οι χρόνοι τερματισμού υπολογίζονται από την αρχική διάρκεια της ροής. Εμφανίζει πρόβλημα όταν οι εγγραφές μέσα σε ένα log δεν είναι ταξινομημένες.

3. Ανωνυμία αριθμού θύρας: Οι αριθμοί θύρας είναι, συχνά, η πιο πολύτιμη πληροφορία για την ανίχνευση επιθέσεων, ενώ οι περισσότερες θύρες μπορεί να χρησιμοποιούνται και για νόμιμους αλλά και για παράνομους σκοπούς. Η γνώση των θυρών που χρησιμοποιήθηκαν μπορεί να αποκαλύψει όλες τις υπηρεσίες που τρέχουν σε ένα δίκτυο αλλά και το ποιοι host τις τρέχουν. Βέβαια, εάν η εταιρία-πάροχος δε

γνωρίζει αυτές τις πληροφορίες, η ανάλυση της ασφάλειας γίνεται δυσκολότερη. Μπορούμε να διακρίνουμε τρεις τύπους:

α) *Ισότιμη κατηγοριοποίηση:* Αντιστοίχηση όλων των θυρών είτε κάτω από τη θύρα 1024 (συνηθισμένες υπηρεσίες), είτε πάνω από αυτήν (εφήμερες υπηρεσίες). Το να γνωρίζεις σε ποια από τις δύο κατηγορίες ανήκει κάθε υπηρεσία μπορεί να είναι αποκαλυπτικό ακόμα και χωρίς να γνωρίζεις την ακριβή πληροφορία. Η μέθοδος μπορεί να σπάσει αλλά παρόλα αυτά είναι μια ικανοποιητική μέθοδος για να θολώσει το τοπίο.

β) *Μαύρο μαρκάρισμα:* Αντικατάσταση όλων των αριθμών των θυρών με μια σταθερά.

γ) *Τυχαία μετάθεση:* Μεταθέτει τυχαία το σύνολο των πιθανών θυρών (0 μέχρι 65.535).

Ένας ακόμα τρόπος, είναι να προστεθεί θόρυβος στα δεδομένα των log όπως, για παράδειγμα, ψεύτικες εγγραφές για υπάρχοντες χρήστες. Η τεχνική αυτή μπορεί να μειώσει την αποτελεσματικότητα της δουλειάς των παρόχων και να μειώσει τον αριθμό των ψευδώς θετικών συναγερμών.

2.2.6 Από την πλευρά της εταιρείας παροχής του outsourcing

2.2.6.1 Αντικείμενο

Οι εταιρίες που ασχολούνται με outsourcing έχουν επιφορτισθεί με μια δύσκολη και κρίσιμη εργασία καθώς καλούνται να διαχειριστούν και να επεξεργαστούν πληροφορίες που έρχονται από πολλά διαφορετικά συστήματα ανίχνευσης εισβολέων. Όπως είναι φυσικό, το επίπεδο θορύβου σε τέτοιες περιπτώσεις είναι εξαιρετικά υψηλό και συνήθως οφείλεται σε όχι καλά σχεδιασμένες υπηρεσίες, σε λάθη των χρηστών, σε κατεστραμμένα ή χαμένα πακέτα δεδομένων, στις υπηρεσίες διαχείρισης του δικτύου και σε άλλες δραστηριότητες που δεν έχουν καμία σχέση με προσπάθειες εισβολής. Για αυτό πολύ συχνά συμβαίνουν ψευδώς θετικοί συναγερμοί. Οι υπεύθυνοι των κέντρων διαχείρισης των δικτύων βλέπουν καθημερινά ένα μεγάλο αριθμό γεγονότων και καλούνται να αποφασίσουν σε ποια από αυτά πρέπει να δοθεί η αρμόζουσα προσοχή και ποια από αυτά πρέπει να αγνοηθούν τελείως. Η κύρια ασχολία τους, όπως αυτή

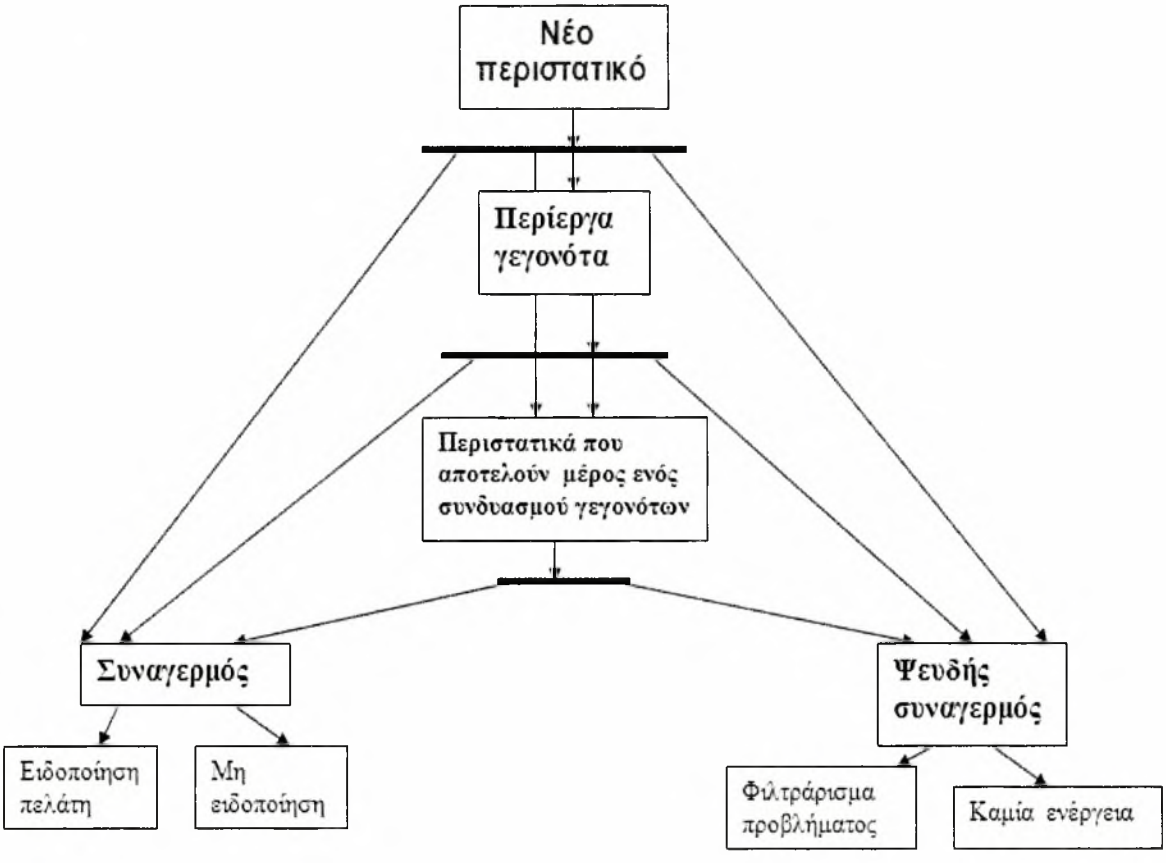
περιγράφεται στο [2], είναι να εντοπίζουν, να αναγνωρίζουν και να αναφέρουν στους πελάτες οποιαδήποτε ανωμαλία συμβεί στο εκάστοτε δίκτυο. Βλέπουν καθημερινά εκατοντάδες περιστατικά και όταν κάποιο από αυτά είναι ύποπτο, ενημερώνουν τον πελάτη και του προτείνουν λύσεις για το συγκεκριμένο πρόβλημα. Επιπρόσθετα, πρέπει να ελέγχουν την κατάσταση των συστημάτων, να μένουν ενήμεροι για τις τελευταίες εξελίξεις, να κρατάνε αρχείο των εργασιών τους και να σχηματίζουν αναφορές για τους πελάτες.

Η διαδικασία που ακολουθείται για τον προσδιορισμό των γεγονότων ως επικίνδυνων ή μη περιγράφεται στο [3].

I. **Βήμα 1^{ο}**: Για κάθε νέο γεγονός αποφασίζουν εάν είναι προφανές ότι ανήκει στα περιστατικά εκείνα για τα οποία πρέπει να ενημερωθεί άμεσα ο πελάτης (κατηγορία 1) ή στα περιστατικά εκείνα τα οποία αποτελούν ψευδείς συναγερμούς (κατηγορία 2). Μια τρίτη κατηγορία είναι τα περίεργα γεγονότα τα οποία απαιτούν μια πιο λεπτομερή ανάλυση και για τα οποία ο διαχειριστής πρέπει να αποφασίσει εάν το γεγονός είναι μέρος ενός συνδυασμού γεγονότων που μπορεί να οδηγήσουν σε μια μη επιθυμητή κατάσταση οπότε και να τα κατατάξει στην 1^{η} κατηγορία ή διαφορετικά να τα κατατάξει στη 2^{η} κατηγορία.
II. **Βήμα 2^{ο}**: Για τα περιστατικά που ανήκουν στην κατηγορία των περίεργων γεγονότων, γίνεται πιο λεπτομερής έλεγχος των χαρακτηριστικών τους. Δηλαδή, συλλέγονται και εξετάζονται ιδιότητες, που αρχικά δεν ήταν γνωστές, όπως, για παράδειγμα, περισσότερες πληροφορίες για μια IP διεύθυνση. Μετά από αυτήν την ανάλυση κατηγοριοποιούνται και αυτά τα περιστατικά στην πρώτη ή τη δεύτερη κατηγορία.
III. **Βήμα 3^{ο}**: Εφόσον ένα περιστατικό ανήκει στην πρώτη κατηγορία πρέπει να αποφασιστεί η σημαντικότητα του και η ενέργεια που θα ακολουθήσει. Δηλαδή, για παράδειγμα, εάν πρέπει οπωσδήποτε να ενημερωθεί ο πελάτης εκείνη τη στιγμή τηλεφωνικά ή αν αρκεί να σταλεί με email μια αναφορά που θα το περιέχει.
IV. **Βήμα 4^{ο}**: Στην περίπτωση που ανήκει στη δεύτερη κατηγορία, οι διαχειριστές πρέπει να αποφασίσουν εάν θα αλλάξουν τη δομή του συστήματος ώστε να μην

χρειαστεί μελλοντικά να ασχοληθούν με παρόμοια περιστατικά αλλά το σύστημα να τα αναγνωρίζει από μόνο του και να τα κατηγοριοποιεί.

Στην εικόνα 4 φαίνεται σχηματικά η παραπάνω διαδικασία.



Εικόνα 4: Διαδικασία κατηγοριοποίησης των νεοαφιχθέντων περιστατικών

2.2.6.2 Κριτήρια πληρότητας και αξιοπιστίας μιας εταιρίας που παρέχει υπηρεσίες outsourcing.

Η απόφαση σχετικά με το ποια εταιρία θα επιλέξει κάποιος για να του παρέχει υπηρεσίες ασφάλειας, πρέπει να λαμβάνεται με μακροπρόθεσμους στόχους. Η ταλάντευση μεταξύ συμβολαίων με άλλες εταιρίες και διατήρησης της ασφάλειας ενδοεπιχειρησιακά, καθώς και η συχνή αλλαγή εταιριών outsourcing οδηγούν σε περιττά έξοδα που έχουν να

κάνουν με κόστος μετάβασης, διακοπή της φυσικής ροής μιας συνεχόμενης επαγγελματικής σχέσης και των οφελών που προκύπτουν από αυτήν και μπορεί να οδηγήσουν ακόμα και στη μείωση της προστασίας ενός δικτύου [29]. Η επιλογή της εταιρίας πρέπει να γίνει προσεκτικά και με βάση συγκεκριμένα κριτήρια-χαρακτηριστικά των εταιριών που προσφέρουν τις υπηρεσίες. Ο Πίνακας 4 περιλαμβάνει αυτά τα κριτήρια.

ΚΡΙΤΗΡΙΑ ΠΛΗΡΟΤΗΤΑΣ ΚΑΙ ΑΞΙΟΠΙΣΤΙΑΣ
Προσωπικό: Μια εταιρία που παρέχει διαχείριση της ασφάλειας ενός δικτύου, θα πρέπει να απαρτίζεται από άτομα ιδιαιτέρως ικανά και πλήρως καταρτισμένα στον χώρο της ασφάλειας. Για να το πετύχει αυτό θα πρέπει να εκπαιδεύει συνεχώς το προσωπικό της, ώστε να μένουν πάντα ενημερωμένοι για όλες τις τελευταίες εξελίξεις στον τομέα τους.
Στην αιχμή της τεχνολογίας: Έχει μεγάλη σημασία η εταιρία που παρέχει τις υπηρεσίες ασφάλειας να είναι πάντοτε ενημερωμένη για τις τελευταίες εξελίξεις στο συγκεκριμένο χώρο. Πρέπει να γνωρίζει τα πιο σύγχρονα προϊόντα ασφάλειας που υπάρχουν, τις τελευταίες εκδόσεις αυτών καθώς και όλα τα τελευταία νέα που αφορούν σε hacker tools αλλά και σε ευπάθειες συστημάτων.
Επενδύσεις: Οι επενδύσεις που έχει κάνει σε συστήματα ασφάλειας πρέπει να είναι αξιόλογες και η υποδομή της ασφάλειας θα πρέπει να έχει την ικανότητα να εξουδετερώνει κάθε πιθανή απειλή.
Αντικρουόμενα συμφέροντα: Οι εταιρίες-πάροχοι δε θα πρέπει να έχουν συγκρουόμενα συμφέροντα [4]. Μερικές εταιρίες πουλάνε προϊόντα ασφάλειας και ταυτόχρονα προσφέρουν υπηρεσίες διαχείρισης ασφάλειας (managed security services), όπως, επίσης, υπάρχουν εταιρίες που παρέχουν στους πελάτες τους πολιτικές ασφάλειας και ταυτόχρονα, αναλαμβάνουν και την παρακολούθηση του δικτύου τους [4]. Σε τέτοιες περιπτώσεις μπορεί να προκύψουν συγκρούσεις συμφερόντων γιατί αν, για παράδειγμα, εντοπιστεί πρόβλημα σε κάποιο από τα προϊόντα της εταιρίας, θα βρεθεί σε δίλλημα ανάμεσα στο να το πει στον πελάτη ή να προσπαθήσει να το διορθώσει σιωπηλά. Όπως, επίσης, μπορεί να μειώσει την τιμή για ορισμένες υπηρεσίες ασφαλείας προκειμένου να προωθήσει κάποιο από τα προϊόντα της. Οι εταιρίες-

πάροχοι θα πρέπει να παρέχουν συγκεκριμένες υπηρεσίες στις οποίες είναι εξειδικευμένες και δε θα πρέπει να προσπαθούν να τα κάνουν όλα μαζί. Οι επιτυχημένες στο χώρο εταιρίες προσφέρουν πολύ καλά ορισμένες υπηρεσίες.

Χρόνος απόκρισης-Συνεχής εγρήγορση: Απαραίτητο είναι, η εταιρία να διαθέτει προηγμένες τεχνικές εξόρυξης γνώσης, ευρεία ορατότητα και ικανότητα για συσχέτιση γεγονότων που αφορούν την ασφάλεια, ώστε να μπορεί να συσχετίζει, να φιλτράρει, να αναλύει και να ερμηνεύει το μεγάλο όγκο πληροφοριών που σχετίζονται την ασφάλεια του δικτύου σε πραγματικό χρόνο. Ως αποτέλεσμα αυτού, θα πρέπει να εξασφαλίζει στους πελάτες της μια άμεση και τάχιστη αντίδραση σε απειλές της ασφάλειας, σύμφωνα πάντα με τα πρότυπα και τις διαδικασίες που υπάρχουν και που είναι αναγνωρισμένες διεθνώς. Μια εταιρία που παρέχει διαχείριση της ασφάλειας ενός δικτύου θα πρέπει να δουλεύει 24 ώρες τη μέρα, 7 ημέρες την εβδομάδα και 365 μέρες το χρόνο (24x7x365). Μια επίθεση στο δίκτυο ενός οργανισμού μπορεί να συμβεί ανά πάσα στιγμή, για αυτό και πρέπει όσοι ασχολούνται με την ασφάλεια ενός δικτύου να είναι συνεχώς σε εγρήγορση.

Στρατηγική: Η ανάπτυξη σεναρίων, στρατηγικών και τακτικών, τις οποίες η εταιρία θα ακολουθήσει για πιθανές μελλοντικές καταστάσεις ανάγκης, είναι μια απαραίτητη διαδικασία, που όλες οι εταιρίες αυτού του είδους πρέπει να ακολουθούν ώστε να είναι έτοιμες να αντιμετωπίσουν ή και να αποφύγουν δυσάρεστες εκπλήξεις στο μέλλον. Σε συνδυασμό με αυτό, πρέπει να αναπτύσσουν τεχνικές ανάκαμψης, ώστε να απομονώνουν και να αποτιμούν τη ζημία, αλλά και για να κινούνται γρήγορα και να μπορούν να αποκαταστήσουν τη λειτουργία που χτυπήθηκε, στην περίπτωση που μια από τις εταιρίες-πελάτες της πέσει θύμα κάποιου εισβολέα.

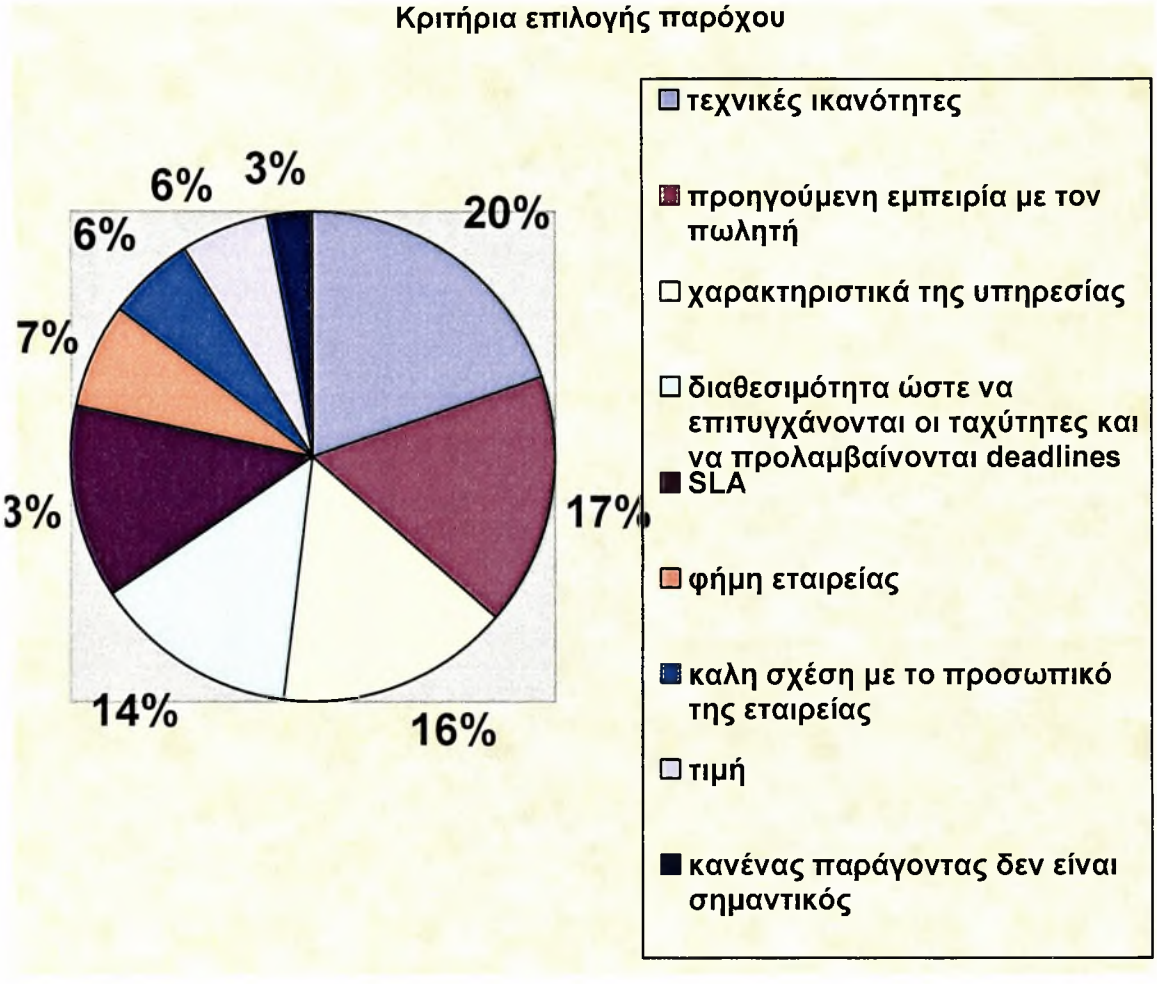
Διαθεσιμότητα: Είναι πολύ πιθανόν να χτυπηθεί η εταιρία παροχής των υπηρεσιών. Τη λύση σε μια τέτοια περίπτωση δίνει η ύπαρξη δύο κέντρων διαχείρισης της ασφάλειας (SOCs, security operation centers). Με αυτόν τον τρόπο διασταυρώνονται τα στοιχεία, επιβεβαιώνονται κάποια γεγονότα, και, επίσης, παρέχονται αντίγραφα ασφαλείας σε περίπτωση καταστροφής.

Ενημέρωση-Εκπαίδευση: Θα πρέπει να παρέχουν στους πελάτες τους έντυπα πρότυπα και πολιτικές τις οποίες θα πρέπει να ακολουθήσουν για να χειριστούν

περιστατικά που μπορεί να συμβούν. Επίσης, πρέπει να διαθέτουν μια ποικιλία μεθόδων ειδοποίησης των πελατών σε περίπτωση συναγερμού, ώστε οι τελευταίοι να μπορούν να μετριάσουν το ρίσκο. Οι αναφορές που θα δίνουν στους πελάτες τους πρέπει να είναι λεπτομερείς, ώστε να μπορεί ο πελάτης να αποφασίσει την αποτελεσματικότητα από άποψη κόστους των υπηρεσιών που αγόρασε. Μια πλήρης αναφορά θα πρέπει να περιέχει πληροφορίες που προέρχονται από τις διάφορες συσκευές (firewall, IDS κ.τ.λ.), από οποιαδήποτε αλλαγή έκανε η εταιρία στις συσκευές, πληροφορίες για τις τελευταίες απειλές καθώς και προτεινόμενες απαντήσεις για όλα τα περιστατικά.
Πιστοποίηση: Οι εταιρίες-πάροχοι πρέπει να πληρούν κριτήρια κατά ISO και να υπάρχουν τρίτοι έμπιστοι οργανισμοί οι οποίοι να επικυρώνουν τις διαδικασίες και τις στρατηγικές που χρησιμοποιούνται για την ασφάλεια.
Εμπειρία: Πολύ βασικό είναι μια εταιρία η οποία θα αναλάβει την ασφάλεια ενός δικτύου ή μέρος αυτής να έχει ισχυρούς οργανωτικούς πόρους και να έχει ήδη καταγεγραμμένες επιτυχίες από άλλους οργανισμούς ή εταιρίες. Βασική προϋπόθεση είναι να διαθέτει παρόμοια εμπειρία στον τομέα της βιομηχανίας ή και σε κυβερνητικούς οργανισμούς. Η διατήρηση των πελατών της και η επέκταση των συμβολαίων είναι αποδείξεις για την ικανοποίηση των πελατών της [29].
Διάρκεια: Η οικονομική σταθερότητα είναι επίσης σημαντική καθώς δείχνει την ικανότητα της εταιρίας να συνεχίσει να διατηρεί αλλά και να βελτιώνει τα συστήματά της αλλά και το προσωπικό της, ώστε να μπορεί να υποστηρίζει τους πελάτες της [4].
Έρευνα: Μια εταιρία που παρέχει υπηρεσίες ασφάλειας θα πρέπει να έχει ανάμιξη στην βιομηχανία της ασφάλειας, να έχει καινοτομήσει πάνω σε συγκεκριμένα θέματα και να έχει συμμετάσχει σε μεγάλα συνέδρια όπου μοίρασε τη γνώση που έχει αποκτήσει από την εμπειρία της [29].

Πίνακας 4: Κριτήρια πληρότητας και αξιοπιστίας

Από έρευνα του IT services marketing association το 2001 [8], προκύπτει ότι 20% από αυτούς που αγοράζουν προϊόντα και υπηρεσίες πληροφορικής πιστεύουν πως οι τεχνικές ικανότητες της εταιρίας-παρόχου είναι ο σημαντικότερος παράγοντας στην λήψη της απόφασής τους. Τα υπόλοιπα ποσοστά φαίνονται στην Εικόνα 5.



Εικόνα 5: Κριτήρια επιλογής παρόχου

Σύμφωνα με προβλέψεις της Gartner το 2004, οι επιχειρήσεις θα διαλέγουν τον πάροχο όχι σύμφωνα με την ικανότητα του να αναγνωρίζει εισβολείς και να ειδοποιεί την επιχείρηση, άλλα σύμφωνα με την ικανότητα του να αναγνωρίζει πιθανές ευπάθειες και να μπλοκάρει οποιονδήποτε προσπαθήσει να εκμεταλλευτεί τις ευπάθειες αυτές.

Κεφάλαιο 3: Κανονιστικό και Μεθοδολογικό πλαίσιο

3.1 Νομοθετικό πλαίσιο στην Ελλάδα και την Ευρωπαϊκή Ένωση

Τα θέματα που ρυθμίζονται από το νομοθετικό πλαίσιο, τόσο το Ελληνικό όσο και από την πλευρά της Ευρωπαϊκής Ένωσης αφορούν [5]:

- Το Ηλεκτρονικό Εμπόριο και τις Ηλεκτρονικές Υπογραφές
- Τα Ηλεκτρονικά συστήματα πληρωμών – Το Ηλεκτρονικό Χρήμα
- Την Πνευματική Ιδιοκτησία
- Την Προστασία των Δεδομένων
- Την Προστασία του Καταναλωτή

Παρακάτω αναφέρονται αναλυτικότερα οι νομοθεσίες που είναι περισσότερο σχετικές με το αντικείμενο της διπλωματικής.

Η κοινοτική νομοθεσία περιέχει τους παρακάτω νόμους:

- Ηλεκτρονικό Εμπόριο-Ηλεκτρονικές Υπογραφές:

1. Πρόταση Οδηγίας στις 24 Σεπτεμβρίου 2002 για την τροποποίηση της Οδηγίας 68/151/ΕΟΚ σχετικά με τις απαιτήσεις δημοσιότητας για ορισμένες μορφές εταιριών
2. Κανονισμός 44/2001 ΕΚ για την διεθνή δικαιοδοσία (σε αντικατάσταση της Σύμβασης των Βρυξελλών), άρθρο 23 παρ.2 που αναγνωρίζει το κύρος της ηλεκτρονικής υπογραφής σε συμφωνίες παρέκτασης της διεθνούς δικαιοδοσίας
3. Απόφαση της Επιτροπής (2001) για έγκριση ενός παγκοσμίου δικτύου (Identrus) για την πιστοποίηση των ηλεκτρονικών υπογραφών και άλλων συναλλαγών ηλεκτρονικού εμπορίου
4. Απόφαση 2000/709 της Επιτροπής για τους φορείς ελέγχου και συμμόρφωσης των διατάξεων δημιουργίας της ηλεκτρονικής υπογραφής στους όρους ασφάλειας του Παραρτήματος ΙΙΙ της Οδηγίας 99/93/ΕΚ
5. Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8^{ης} Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της

πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά ("Οδηγία για το ηλεκτρονικό εμπόριο").

6. Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

7. Οδηγία 98/84/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη νομική προστασία των υπηρεσιών που βασίζονται ή συνίστανται στην παροχή πρόσβασης υπό όρους.

8. Οδηγία 98/48/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Ιουλίου 1998 για την τροποποίηση της οδηγίας 98/34/ΕΚ για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών

9. COM(97) 157 Μια Ευρωπαϊκή Πρωτοβουλία στο Ηλεκτρονικό Εμπόριο.

- Ηλεκτρονικές Επικοινωνίες:

1. Οδηγία 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά στα δίκτυα και στις υπηρεσίες ηλεκτρονικών επικοινωνιών

2. Οδηγία 2002/21/ΕΚ για το κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών

3. Οδηγία 2002/20/ΕΚ για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών

4. Οδηγία 2002/19/ΕΚ για την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφής ευκολίες

5. Οδηγία 96/2/ΕΚ για τροποποίηση της οδηγίας 90/388/ΕΟΚ όσον αφορά τις κινητές και προσωπικές επικοινωνίες

- Πνευματική Ιδιοκτησία:

1. Οδηγία 2001/29/ΕΚ της 22ας Μαΐου 2001 για την εναρμόνιση ορισμένων πτυχών του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας.

2. Οδηγία 96/9/ΕΟΚ της 11ης Μαρτίου 1996 σχετικά με τη νομική προστασία των βάσεων δεδομένων.

3. Οδηγία 92/100/ΕΟΚ σχετικά με το δικαίωμα εκμίσθωσης το δικαίωμα δανεισμού και ορισμένα δικαιώματα συγγενικά προς την πνευματική ιδιοκτησία στον τομέα των προϊόντων της διανοίας.

4. Οδηγία 91/250/ΕΟΚ για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών

- Ηλεκτρονικό Έγκλημα:

1. Σύσταση του Συμβουλίου 25 Ιουνίου 2002 για σημεία επαφής που λειτουργούν 24 ώρες το εικοσιτετράωρο για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας

2. Έγγραφο Διαβουλεύσεων της Επιτροπής, Ιούνιος 2002 για την ασφάλεια των ηλεκτρονικών δικτύων

3. Σχέδιο Κανόνων της Επιτροπής, Απρίλιος 2002 για τον κοινό ορισμό ορισμένων αδικημάτων που αφορούν υπολογιστές

4. Ψήφισμα του Συμβουλίου 1 Μαρτίου 2002 για την προστασία των καταναλωτών, ιδίως των νέων, με την επισήμανση ορισμένων βιντεοπαιχνιδιών και ηλεκτρονικών παιγνίων αναλόγως της ηλικίας

5. Έγγραφο Πολιτικής της Επιτροπής, Ιανουάριος 2002 για την καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικού υπολογιστή και την βελτίωση της ασφάλειας των υποδομών πληροφορικής με την λήψη νομοθετικών και μη νομοθετικών μέτρων.

6. Απόφαση – Πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου της 28-5-2001 για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών

7. Ανακοίνωση COM (2000) 890 της Επιτροπής «Για μια ασφαλέστερη Κοινωνία της Πληροφορίας με τη βελτίωση της ασφάλειας των υποδομών πληροφόρησης και την καταπολέμηση του εγκλήματος πληροφορικής».

8. Απόφαση 276/1999/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για ένα πολυετές κοινοτικό πρόγραμμα δράσης για ασφαλέστερη χρήση του Ίντερνετ μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχομένου στα παγκόσμια δίκτυα

- Προστασία δεδομένων:

1. Οδηγία 2002/58/ΕΚ της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)
2. Οδηγία 97/66/ΕΚ περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα.
3. Οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Η εθνική νομοθεσία περιέχει τους παρακάτω νόμους.

- Ηλεκτρονικό Εμπόριο-Ηλεκτρονικές Υπογραφές:

1. Σχέδιο ΠΔ για το ηλεκτρονικό εμπόριο
2. ΠΔ 342/2002 για την διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ των δημοσίων υπηρεσιών, ΝΠΔΔ, ΟΤΑ ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων
3. ΠΔ 388/2002 για τις διαφορές που υπόκεινται στην μόνιμη διαιτησία της ΕΕΤΤ
4. Κανονισμός ΕΕΤΤ 248/71 για την Παροχή Πιστοποίησης ηλεκτρονικής υπογραφής
5. ΠΔ 150/2001 Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.
6. ΠΔ 39/2001 για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας της πληροφορίας σε συμμόρφωση προς τις Οδηγίες 98/34/ΕΚ&98/48/ΕΚ.
7. Σύσταση Γραφείου της Εθνικής Επιτροπής Ηλεκτρονικού Εμπορίου(ΦΕΚ 453/Τ. Β΄/4-4-2000).
8. Ν. 2672/1998 (Άρθρο 14) για τη διακίνηση εγγράφων μεταξύ Δημοσίου, ΝΠΔΔ και ΟΤΑ και ιδιωτών με ηλεκτρονικά μέσα (τηλεομοιοτυπία και ηλεκτρονικό ταχυδρομείο). Στο άρθρο αυτό για πρώτη φορά αναφέρεται ο ορισμός της ψηφιακής υπογραφής και στη συνέχεια στην παράγραφο 19 προβλέπεται η έκδοση Προεδρικού Διατάγματος που θα καθορίζει τις προϋποθέσεις και τη διαδικασία έκδοσης, διακίνησης, διαχείρισης και

διασφάλισης της ψηφιακής υπογραφής, τις προϋποθέσεις παροχής και το περιεχόμενο των υπηρεσιών πιστοποίησης και άλλα συναφή ζητήματα

9. Υπουργική Απόφαση αρ.1342/1997 για το Μητρώο Προμηθευτών του α.4 του Ν.2251/1994

10. Ν. 2251/1994 για την προστασία του καταναλωτή και ειδικότερα α.4 για τις συμβάσεις που συνάπτονται από απόσταση

- Πνευματική ιδιοκτησία :

1. 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"

2. 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)

3. Ν 2557/1997/Α-271 Θεσμοί μέτρα και δράσεις πολιτιστικής ανάπτυξης (Τροποποίηση του Ν. 2121/93)

4. Ν 2435/1996 (Τροποποίηση του Ν. 2121/93)

5. Ν. 2121/1993 Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα.

- Προστασία προσωπικών δεδομένων :

1. Ν. 2819/2000 α.8. Τροποποίηση του Ν. 2472/1997.

2. Ν. 2774/1999 Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.

3. Απόφαση 408/1998 Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Ενημέρωση υποκειμένων επεξεργασίας δεδομένων προσωπικού χαρακτήρα δια του τύπου Κωδικοποίηση σε ενιαίο κείμενο του

4. Ν. 2472/1997 για την Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα μετά τις σχετικές τροποποιήσεις από τους Ν.2623/1998, 2703/1999, 2721/1999, 2819/2000 και 2915/2001.

- Ηλεκτρονικό Έγκλημα:

1. Ειδικά ποινικά αδικήματα του Π.Κ. σχετικά με τη χρήση ηλεκτρονικών υπολογιστών. άρθρο 370Β ΠΚ, άρθρο 370 Γ ΠΚ, άρθρο 386 Α ΠΚ,

- Ηλεκτρονικές επικοινωνίες:

1. Απόφαση ΕΕΤΤ 264/140 περί ορισμού υπόχρεων Παροχής Καθολικής Υπηρεσίας
2. Απόφαση ΕΕΤΤ 255/83 περί καθορισμού του περιεχομένου της Καθολικής Υπηρεσίας
3. Ν. 2867/2000 (Φ.Ε.Κ. 273 Α΄/19 Δεκεμβρίου 2000) - Οργάνωση και λειτουργία των Τηλεπικοινωνιών και άλλες διατάξεις.
4. Π.Δ. 165/1999 (Φ.Ε.Κ. Α΄-159) για την τροποποίηση του Ν. 2246/1994, όπως εκάστοτε ισχύει, σε συμμόρφωση α) προς την Οδηγία 97/33/ΕΚ για τη διασύνδεση στο χώρο των τηλεπικοινωνιών προκειμένου να διασφαλιστεί καθολική υπηρεσία και διαλειτουργικότητα, με εφαρμογή των αρχών παροχής ανοικτού δικτύου (ONP) και β) σε συμμόρφωση προς την Οδηγία 98/61/ΕΚ «Περί τροποποιήσεως της Οδηγίας 97/33/ΕΚ σε ό,τι αφορά τη φορητότητα των αριθμών και την προεπιλογή φορέα».
5. Κανονισμός αρ. 78794/1999. Διαδικασίας έκδοσης και τροποποίησης Γενικών Αδειών, Υποβολής, Τροποποίησης και Ανανέωσης Δήλωσης Καταχώρησης και αφαίρεσης του δικαιώματος χρήσης Γενικής Αδείας.
6. Κωδικοποίηση σε ενιαίο κείμενο του Ν. 2246/1994 για την Οργάνωση και λειτουργία του τομέα τηλεπικοινωνιών, όπως ισχύει μετά τις τροποποιήσεις των Ν. 2366/1995,2374/1996, 2465/1997, 2578/1998, 2668/1998, 2801/2000, 2840/2000 και των Π.Δ.212/1997, 123/1998, 124/1998, 156/1999, 157/1999 και 165/1999

3.2 ISO

Το ISO/IEC 17799:2005 [11] περιέχει οδηγίες και γενικές αρχές για το ξεκίνημα, την υλοποίηση, την συντήρηση και τη βελτίωση της διαχείρισης της ασφάλειας πληροφοριών μέσα σε έναν οργανισμό. Οι στόχοι που σκιαγραφούνται στο ISO παρέχουν γενικές οδηγίες για τους κοινώς αποδεκτούς σκοπούς της διαχείρισης της ασφάλειας. Το

ISO/IEC 17799:2005 περιλαμβάνει τις καλύτερες πρακτικές των στόχων ελέγχου στα παρακάτω πεδία της διαχείρισης ασφάλειας πληροφορίας :

- Πολιτική ασφαλείας
- Οργάνωση της ασφάλειας πληροφορίας
- Διαχείριση πόρων
- Ασφάλεια ανθρώπινου δυναμικού
- Υλική και περιβαλλοντική ασφάλεια
- Διαχείριση επικοινωνιών και λειτουργιών
- Έλεγχος πρόσβασης
- Απόκτηση, ανάπτυξη και διατήρηση πληροφοριακών συστημάτων
- Διαχείριση περιστατικών σχετικών με την ασφάλεια πληροφορίας
- Διαχείριση επιχειρησιακής συνέχειας (business continuity)
- Συμμόρφωση

Οι στόχοι ελέγχου και οι έλεγχοι στο ISO προορίζονται να υλοποιηθούν με σκοπό να συναντήσουν τις απαιτήσεις που προσδιορίζονται από την αποτίμηση των κινδύνων. Πρόκειται για έναν πρακτικό οδηγό για την ανάπτυξη οργανωτικών προτύπων ασφαλείας και αποτελεσματικών πρακτικών διαχείρισης της ασφάλειας και ο οποίος αποσκοπεί στο να βοηθήσει στο χτίσιμο εμπιστοσύνης μεταξύ οργανισμών.

3.3 Χαρακτηριστικά του πλαισίου ανάθεσης

Η μορφή του outsourcing καθορίζεται από τη σύμβαση-συμβόλαιο που υπογράφεται ως μία διμερής συμφωνία μεταξύ του παρόχου και του πελάτη και η οποία περιλαμβάνει όλα εκείνα τα στοιχεία που χαρακτηρίζουν αυτήν τη σχέση. Στο συμβόλαιο πρέπει να αναφέρονται με σαφήνεια οι υποχρεώσεις και τα δικαιώματα των δύο εμπλεκόμενων μερών, το είδος και η ποιότητα των υπηρεσιών καθώς και οι ρήτρες που εφαρμόζονται σε περίπτωση που είτε ο πάροχος, είτε ο πελάτης παραβιάσουν τους όρους του συμβολαίου.

Είναι απαραίτητη η ενσωμάτωση στο συμβόλαιο όρων, οι οποίοι εξασφαλίζουν την ικανοποίηση και των δύο πλευρών. Ο πελάτης πρέπει να λάβει άψογης ποιότητας

υπηρεσίες ασφάλειας σε κάποιο λογικό κόστος. Αντίστοιχα, ο πάροχος πρέπει να έχει συγκεκριμένα οικονομικά οφέλη από τη συνεργασία αυτή. Ο πελάτης θα πρέπει να έχει κατά νου ότι εάν ο πάροχος δεν αποκομίζει κέρδη από τη μεταξύ τους σχέση τότε η ποιότητα των παρεχόμενων υπηρεσιών θα μειώνεται συνεχώς ανεξάρτητα με ότι αναφέρεται στο συμβόλαιο.

Για να εξασφαλιστεί ο σωστός τρόπος λειτουργίας της σχέσης outsourcing, θα πρέπει να αναλύεται λεπτομερώς στο συμβόλαιο η Περιγραφή των Εργασιών-Υπηρεσιών και η Σύμβαση του Επιπέδου Ποιότητας [7].

- **Η Περιγραφή των Εργασιών-Υπηρεσιών:** Μέρος του συμβολαίου στο οποίο περιγράφονται με σαφήνεια ότι αναμένεται να παραδίδει-προσφέρει ο πάροχος, καθώς, επίσης, και οι ρόλοι και αρμοδιότητες των ανθρώπων που θα εμπλακούν. Μεγάλη προσοχή πρέπει να δίνεται ώστε να περιλαμβάνονται όλες οι πιθανές περιπτώσεις που μπορεί να προκύψουν, καθώς τις περισσότερες φορές δεν υπάρχει σαφής αναφορά σε αυτές στο συγκεκριμένο κείμενο.
- **Η Σύμβαση του Επιπέδου Ποιότητας:** Τμήμα του συμβολαίου το οποίο ενσωματώνει ποινές-ρήτρες. Η μη τήρηση των επιπέδων απόδοσης και ποιότητας, όπως η διαθεσιμότητα της υπηρεσίας ή ο χρόνος απόκρισης και λύσης των προβλημάτων, πρέπει να τιμωρείται με συγκεκριμένες ποινές. Μια Σύμβαση Επιπέδου Ποιότητας χωρίς ποινές είναι ουσιαστικά ανεφάρμοστη. Επιπλέον των ποινών η σύμβαση μπορεί να περιέχει και όρους επιβράβευσης σε περίπτωση που τα επίπεδα απόδοσης και ποιότητας ξεπεράσουν κάποια δεδομένα για συγκεκριμένο χρονικό διάστημα. Αναλυτική περιγραφή της Σύμβασης Επιπέδου Ποιότητας αναφέρονται στην επόμενη ενότητα.

Σύμφωνα με την Gartner [6], το 50 % των συμφωνιών outsourcing καταλήγουν σε "διαζύγιο". Οι ειδικοί υποστηρίζουν ότι αυτό το πολύ υψηλό ποσοστό οφείλεται στην απογοήτευση από την πλευρά του αγοραστή όταν οι οικονομικές και μη προσδοκίες του δεν επαληθεύονται. Αυτό κυρίως οφείλεται σε τρεις παράγοντες-κλειδιά:

- Έλλειψη συμμόρφωσης στους στόχους και έλλειψη συμφωνίας για το πώς μετράτε η επιτυχία μεταξύ προμηθευτή και πελάτη.
- Κακοσχεδιασμένες συμφωνίες.
- Έλλειψη μιας καλής πολιτικής διαχείρισης- διακυβέρνησης.

3.3.1 Χαρακτηριστικά του πλαισίου ανάθεσης από την πλευρά των εταιριών-πελατών

Εάν επιλεγεί η ανάθεση μέρους της ασφάλειας σε κάποια άλλη εταιρία πρέπει να εξεταστούν πρώτα κάποιες παράμετροι ώστε να βεβαιωθεί η σωστή διεκπεραίωση της συναλλαγής καθώς και η εξασφάλιση της ποιότητας σε συγκεκριμένα επίπεδα. Η ποιότητα της υπηρεσίας μπορεί να μετράτε σε χρόνο απόκρισης σε γεγονότα, σε όγκο δεδομένων που διακινούνται, σε ρυθμούς-ταχύτητα δεδομένων, σε αριθμό συναλλαγών που πραγματοποιούνται στη μονάδα του χρόνου κ.λ.π.

Ο παρακάτω πίνακας συνοψίζει τη διαδικασία λήψης απόφασης για την αγορά υπηρεσιών outsourcing:

ΔΙΑΔΙΚΑΣΙΑ ΛΗΨΗΣ ΑΠΟΦΑΣΗΣ	
Βήμα 1^{ο} : Καταγραφή αναγκών	Μια επιτυχημένη σχέση outsourcing έχει ως αφετηρία την αναγνώριση της ήδη υπάρχουσας κατάστασης στην επιχείρηση, όσον αφορά στην ασφάλεια, όπως, επίσης, και των αναγκών της, ώστε να ληφθούν οι υπηρεσίες που ανταποκρίνονται περισσότερο στις απαιτήσεις της εταιρίας. Η κίνηση αυτή έχει ως στόχο την μείωση του κόστους και, ταυτόχρονα, την αναβάθμιση της ποιότητας των παρεχόμενων υπηρεσιών. Με την καταγραφή της υπάρχουσας κατάστασης σε όρους ποιότητας, όπως αυτοί εξηγούνται παραπάνω, είναι εφικτή ανά πάσα στιγμή η αντιπαράθεση της νέας κατάστασης με την καταγεγραμμένη. Σκοπός

	αυτής της αντιπαράθεσης είναι η έκβαση συμπερασμάτων για την ποιότητα των υπηρεσιών και για τα οφέλη που αποκομίζει η επιχείρηση από τη λήψη των υπηρεσιών ασφάλειας μέσω του outsourcing.
Βήμα 2^{ο} : Αναζήτηση παρόχων	Το επόμενο βήμα είναι η αναζήτηση παρόχων και υπηρεσιών οι οποίες καλύπτουν τις ανάγκες της επιχείρησης. Σε αυτό το στάδιο πρέπει να ληφθεί υπ' όψιν ότι στον τομέα της ασφάλειας δικτύων οι εξελίξεις είναι ραγδαίες και αρκούν λίγα εικοσιτετράωρα για να αλλάξει εντελώς το τοπίο. Η αναζήτηση μεγάλου αριθμού λύσεων δίνει στην επιχείρηση περισσότερες δυνατότητες επιλογής. Μεγάλη προσοχή πρέπει να δοθεί στα τεχνικά χαρακτηριστικά των προσφερόμενων υπηρεσιών και να μην αναζητείται πάντα η οικονομικότερη λύση. Η επιλογή της τεχνολογίας ασφάλειας θα πρέπει να βασίζεται σε σύγχρονες τάσεις και να περιλαμβάνονται ευέλικτοι μηχανισμοί οι οποίοι θα επιτρέπουν την υιοθέτηση νέων τεχνολογιών και συστημάτων
Βήμα 3^{ο} : Τελική απόφαση	Τέλος, πρέπει να αποφασιστεί αν είναι πιο συμφέρουσα η λήψη υπηρεσιών ασφάλειας από τρίτους ή η παραγωγή των υπηρεσιών εντός της επιχείρησης. Σε αυτό θα βοηθήσει ο υπολογισμός του κόστους και για τις δύο περιπτώσεις, όπως έχει ήδη αναλυθεί. Θα πρέπει, επίσης, να ληφθεί υπ' όψιν η ποιότητα των υπηρεσιών και στις δύο περιπτώσεις, αν και συνήθως τέτοια στοιχεία είναι δύσκολο να ποσοτικοποιηθούν. Συνήθως, η ποιότητα της διαδικασίας της ασφάλειας στην περίπτωση που οι υπηρεσίες παράγονται ενδοεπιχειρησιακά παραμένει σταθερή ή χειροτερεύει, ενώ στην αντίθετη περίπτωση μπορεί και να βελτιώνεται. Επίσης, σε αυτό το στάδιο πρέπει να δοθούν απαντήσεις σε ερωτήματα όπως τι θεωρείται επιτυχημένη λήψη υπηρεσιών ασφάλειας, πως θα έχει ιδανικά διαμορφωθεί η υφισταμένη κατάσταση σε ένα ή δυο χρόνια πέρα από όρους εξοικονόμησης

	χρήματος και επιπέδου υπηρεσιών και πως αναμένεται να έχει διαμορφωθεί η σχέση με τον πάροχο.
Βήμα 4^{ο}: Ορισμός των όρων που διέπουν τη συμφωνία	Η επιχείρηση θα πρέπει να ορίσει ποια θα είναι τα αποτελέσματα της διαδικασίας σε κάθε στάδιο αυτής και να θέσει τους τυχόν περιορισμούς και υποχρεώσεις του εξωτερικού συνεργάτη που θα αναλάβει την διαδικασία του outsourcing [31].

Πίνακας 5: Διαδικασία λήψης απόφασης για αγορά υπηρεσιών outsourcing

Σημεία κλειδιά κατά τη σύναψη μιας σχέσης outsourcing αποτελούν τα στελέχη και οι εργαζόμενοι μιας επιχείρησης και είναι πολύ σημαντικό να καθοριστούν από την αρχή οι ρόλοι του καθενός .

Στελέχη επιχείρησης

Κατά τη σύναψη μιας σχέσης outsourcing τα υψηλόβαθμα στελέχη έχουν ενεργό ρόλο. Αυτοί αποφασίζουν για το αν η επιχείρηση θα προβεί στη σύναψη μιας τέτοιας συμφωνίας και διαπραγματεύονται τους όρους της.. Τα στελέχη πρέπει να είναι ικανά να αποτιμούν εναλλακτικές δομές δαπανών και να καταλαβαίνουν το στρατηγικό κίνδυνο του να αναθέτεις την ασφάλεια του δικτύου σου σε κάποιον συνεργάτη έναντι κάποιου άλλου. Πρέπει να ελέγχουν τη συμφωνία, μέσα από την προσωπική επαφή, χωρίς να ανακατεύονται και να παρεμβαίνουν και να καταφέρνουν να διατηρούν τον στρατηγικό έλεγχο.

Όσο κάποια εταιρία αναθέτει όλο και περισσότερες λειτουργίες ασφάλειας σε, περισσότερους του ενός, εξωτερικούς συνεργάτες υπάρχει η ανάγκη για καλύτερη διαχείριση και συντονισμό των διαδικασιών που ακολουθούν τέτοιες συμφωνίες.

Εργαζόμενοι

Μετά τη λήψη μιας τέτοιας απόφασης αλλάζει ο τρόπος λειτουργίας της εταιρίας. Το προσωπικό, που μέχρι τότε απασχολούνταν στο τμήμα της ασφάλειας, μπορεί να

αναλάβει τη διαχείριση και την παρακολούθηση αυτών των σχέσεων. Η ύπαρξη του τεχνικού υπόβαθρου σε θέματα σχετικά με την ασφάλεια Πληροφοριακών συστημάτων για την προδιαγραφή και την παρακολούθηση των υπηρεσιών αποτελεί μεγάλο πλεονέκτημα έναντι της πρόσληψης νέων εργαζομένων με κριτήριο τις διαπραγματευτικές τους ικανότητες. Απαραίτητη είναι, όμως, η εκπαίδευση των ήδη υπαρχόντων εργαζομένων πάνω σε θέματα διαπραγμάτευσης και διαχείρισης σχέσεων ώστε να μπορούν να ανταπεξέλθουν στα νέα τους καθήκοντα. Μόνο όταν δεν είναι δυνατή η κάλυψη των αναγκών αυτών από το προσωπικό της επιχείρησης θα πρέπει να ξεκινήσει η διαδικασία αναζήτησης νέων εργαζομένων.

Αυτή η αλλαγή στον τρόπο λειτουργίας της επιχείρησης, πολλές φορές εκλαμβάνεται ως απειλή από την πλευρά των εργαζομένων, οι οποίοι μπορεί να νοιώσουν ότι παραμερίζονται. Όμως, η πιθανή δυσαρέσκεια των εργαζομένων μπορεί να οδηγήσει στην αποτυχία της σχέσης outsourcing. Για αυτό τον λόγο είναι σημαντικό οι άνθρωποι οι οποίοι εμπλέκονται να είναι ευχαριστημένοι. Για να αντιμετωπιστούν αυτού του είδους τα προβλήματα, είναι απαραίτητο, οι επικοινωνίες και οι διαδικασίες να είναι ειλικρινείς και ανοιχτές για όλους από την αρχή.

Ταυτόχρονα, οι άνθρωποι που συμμετέχουν στην ομάδα πρέπει να ανταμείβονται για τη συνεισφορά τους στην εύρυθμη λειτουργία της σχέσης outsourcing. Από την πλευρά της επιχείρησης-πελάτη, θα πρέπει να έχουν ληφθεί τα κατάλληλα μέτρα, ώστε να εξασφαλίζεται ότι οι άνθρωποι οι οποίοι συμμετέχουν στην ομάδα διαχείρισης δεν πρόκειται να αποχωρήσουν κατά τη διάρκεια της συνεργασίας με τον πάροχο. Οι άνθρωποι κοστίζουν αλλά, ταυτόχρονα, αποτελούν το πιο σημαντικό πάγιο σε μια σχέση outsourcing και κυρίως όταν πρόκειται για θέματα ασφάλειας όπου διακυβεύονται σημαντικές πληροφορίες. Η ισορροπία μεταξύ των δύο αυτών άκρων είναι ζωτικής σημασίας για την επιτυχία και τη σωστή αξιοποίηση των υπηρεσιών [7].

Ένας εμπειρικός κανόνας για το ύψος του ετήσιου προϋπολογισμού των μισθών μιας ομάδας εργαζομένων σε θέματα ασφάλειας, είναι ότι αυτός κυμαίνεται μεταξύ 3-11% του συνολικού συμφωνημένου αντιτίμου με τον πάροχο. Το ποσό αυτό εξασφαλίζεται

από τη μείωση του κόστους των υπηρεσιών που παρέχονται πλέον μέσω της σχέσης outsourcing [7].

Σαφώς καθορισμένοι ρόλοι

Οι ρόλοι και οι συνεργασίες των μελών της ομάδας παρακολούθησης και διαχείρισης των σχέσεων outsourcing πηγάζουν από τις διαδικασίες και τις σχέσεις αυτές. Θα πρέπει να είναι σαφώς καθορισμένο το τι, με ποιον τρόπο και πότε κάνει κάθε μέλος της ομάδας του πελάτη κάθε του κίνηση. Οι αντίστοιχες απαιτήσεις στα προσόντα και τις δεξιότητες που πρέπει να κατέχει κάθε μέλος της ομάδας εξάγονται από τη διαδικασία καθορισμού των ρόλων.

Σε συνδυασμό με όλα τα παραπάνω, οι επιχειρήσεις πριν τη σύναψη του συμβολαίου μπορούν:

- ✓ Να ζητήσουν τη συνδρομή κάποιου συμβούλου επιχειρήσεων εξειδικευμένου σε θέματα outsourcing. Ο μέσος επιχειρηματίας συνήθως δεν έχει την απαιτούμενη κατάρτιση, έτσι ώστε να μπορέσει να αποφύγει τα "ψιλά γράμματα" των συμβολαίων και τους ασαφείς ή διφορούμενους όρους που μπορεί να περιληφθούν σε μια σύμβαση σε αντίθεση με τις εταιρίες που παρέχουν υπηρεσίες outsourcing. Οι τελευταίες έχουν την πολυτέλεια να διαθέτουν μεγάλο και αξιόλογο επιτελείο στελεχών, το οποίο είναι φυσικό να προσπαθεί να πετύχει την καλύτερη δυνατή συμφωνία για αυτήν. Η δουλειά του συμβούλου είναι να αποφύγει τις παγίδες που πιθανά ελλοχεύουν σε ένα νομικό κείμενο, να θέσει τα σωστά ερωτήματα για τις επιδιώξεις και στόχους της επιχείρησης, να ενημερωθεί αναφορικά με τις καλύτερες πρακτικές, να βελτιώσει την επικοινωνία με τον πάροχο υπηρεσιών, να διαπραγματευθεί σε ίσους όρους με τον πάροχο και να γνωρίζει τη σωστή τιμή για κάθε εργασία.
- ✓ Να ζητήσουν βοήθεια από ειδικούς του τμήματος ασφάλειας της εταιρίας ή από άτομα με γνώσεις πάνω στο θέμα, για να καταλάβουν όλες τις τεχνολογικές λεπτομέρειες. Οι πάροχοι υπηρεσιών ασφάλειας μπορούν εύκολα να αποπροσανατολίσουν ένα άτομο που δεν είναι σχετικό με την ασφάλεια δικτύων.

- ✓ Να ζητήσουν πληροφορίες και από άλλες επιχειρήσεις που χρησιμοποιούν ή χρησιμοποίησαν σε κάποια χρονική στιγμή το outsourcing και να καταγραφούν οι εμπειρίες και οι εντυπώσεις τους. Οι πληροφορίες που θα προκύψουν από αυτήν την περίπτωση θα είναι πολύ χρήσιμες εάν υποτεθεί ότι οι επιχειρήσεις αυτές θα εξιστορήσουν πραγματικά γεγονότα και περιστατικά. Εφόσον δε θα είναι όλες οι συστάσεις αξιόπιστες, καλό είναι να τεθούν συγκεκριμένες ερωτήσεις όπως:
    1. Αν χρησιμοποιούν ακόμα τα συστήματα ή τις υπηρεσίες ασφάλειας που είχαν αγοράσει και αν όχι γιατί.
    2. Τι ακριβώς χρησιμοποίησαν από αυτήν τη εταιρία, ποια συστήματα και ποιες εκδόσεις. Την κάθε επιχείρηση την ενδιαφέρουν μόνο περιπτώσεις που έχουν χρησιμοποιήσει συστήματα παρόμοια με αυτά που σκοπεύει να αγοράσει.
    3. Με ποιον τρόπο χρησιμοποιούν το σύστημα. Μπορεί κάποια εφαρμογή να μην είναι δυνατόν να πραγματοποιηθεί σε κάποια εταιρία.
    4. Γιατί χρησιμοποίησαν το συγκεκριμένο σύστημα ασφάλειας, ποιες είναι οι δυνατότητες του και ποιοι οι περιορισμοί του.
    5. Αν υπάρχουν κάποια bugs, ποια είναι αυτά και πως ο πάροχος διευθέτησε αυτά τα προβλήματα.
    6. Πόσο καιρό πήρε η υλοποίηση και συμβουλές για το πως θα γίνει ευκολότερη.
    7. Αν είναι καλή η εξυπηρέτηση πελατών του παρόχου, αν η ανταπόκριση του γραφείου εξυπηρέτησης πελατών είναι γρήγορη, αν υπήρχαν ποτέ προβλήματα και πως τα χειρίστηκαν.
- ✓ Να ζητήσουν πληροφορίες από τα διάφορα επιμελητήρια (εμπορικά, τεχνικά κ.λ.π.). Πολύ πιθανόν ορισμένα από αυτά να μπορούν να επισημάνουν ορισμένα σημεία-κλειδιά στα οποία πρέπει να δοθεί ιδιαίτερη προσοχή.
- ✓ Να ζητήσουν από την εταιρία-πάροχο προηγούμενα συμβόλαια με αντίστοιχες εταιρίες για να δουν κατά πόσο τους ικανοποιούν.

Και πρέπει επίσης:

- ✓ Να ληφθούν υπόψη δύο σημαντικές παράμετροι πριν τη λήψη μιας απόφασης: το κόστος και η ποιότητα. Δεδομένης της κρίσης που περνούν τα τελευταία χρόνια οι εταιρίες πληροφορικής είναι δύσκολο να προσφέρουν υπηρεσίες υψηλού επιπέδου σε χαμηλή τιμή. Η προσπάθεια να επιτευχθεί η χαμηλότερη τιμή, τις περισσότερες φορές, οδηγεί σε λάθος αποφάσεις. Ο κύριος στόχος είναι η εξασφάλιση ποιοτικών υπηρεσιών ασφάλειας και δευτερευόντως χαμηλές τιμές .
- ✓ Το πρώτο συμβόλαιο να αφορά μικρό, σχετικά, χρονικό διάστημα ώστε να διαπιστωθεί η αξιοπιστία του συνεργάτη
- ✓ Στη φάση της διαπραγμάτευσης και της συμφωνίας να οριστούν κάποιοι δείκτες που αφορούν τους τρόπους μέτρησης της υπηρεσίας. Οι δείκτες αυτοί, όπως αναφέρθηκε, μπορεί να αφορούν το χρόνο απόκρισης σε γεγονότα, τον όγκο δεδομένων που διακινούνται, την ταχύτητα δεδομένων, τη διαθεσιμότητα της υπηρεσίας, τον αριθμό συναλλαγών που πραγματοποιούνται στη μονάδα του χρόνου κ.λ.π. Είναι σημαντικό να ορίζεται ο τρόπος μέτρησης και παρουσίασης των δεικτών αυτών. Για παράδειγμα, η λειτουργία ενός firewall κατά το 99% του χρόνου σημαίνει πολύ διαφορετικό επίπεδο υπηρεσίας εάν αναφερόμαστε σε μία ώρα (οπότε το firewall δε θα πρέπει να είναι εκτός λειτουργίας για παραπάνω από 36 δευτερόλεπτα κάθε ώρα) ή σε ένα έτος (οπότε το firewall δεν θα πρέπει να είναι εκτός λειτουργίας για παραπάνω από 3,65 μέρες το χρόνο).
- ✓ Να συμπεριληφθούν ασφαλιστικές δικλείδες στο συμβόλαιο. Δηλαδή, να υπάρχουν ποινές οι οποίες να επιβάλλονται στην περίπτωση που κάποιοι από τους όρους του συμβολαίου παραβιαστούν, ενώ αντίστοιχα να υπάρχουν επιβραβεύσεις όταν ο εξωτερικός συνεργάτης προσφέρει περισσότερα από όσα είχαν αρχικά συμφωνηθεί. Τόσο οι ποινές, όσο και οι επιβραβεύσεις μπορούν να αναφέρονται σε καθαρά οικονομικές επιπτώσεις, όπως γίνεται συνήθως, ή σε κάποια άλλη μορφή, η οποία συμφωνείται μεταξύ του παρόχου και της επιχείρησης. Μια τέτοια ποινή μπορεί να είναι ακόμα και λήξη της συνεργασίας των δύο μερών. Πολλές φορές, οι ποινές αυτές μπορεί να μην

αντισταθμίζουν τα όσα έχασε μια εταιρία από τη μη τήρηση κάποιου όρου του συμβολαίου. Αλλά η ποινή θα κάνει τον πάροχο να προσπαθήσει να φτιάξει το πρόβλημα ώστε να μη ξανασυμβεί

Είναι, επίσης, ευρέως αποδεκτό ότι σε μια σχέση outsourcing πρέπει να υπάρχει εμπιστοσύνη ανάμεσα στα εμπλεκόμενα μέρη, αλλά, ταυτόχρονα, από την πλευρά του πελάτη πρέπει να επαληθεύεται το αν λειτουργούν σωστά όλα όσα έχουν συμφωνηθεί. Ένας πολύ απλός έλεγχος είναι η παύση της λειτουργίας ενός μέρους της ασφάλειας για πολύ λίγο, ώστε να διαπιστωθεί αν η αντίδραση από τον συνεργάτη θα είναι άμεση και θα ακολουθήσει ενημέρωση για αυτό που έγινε. Για παράδειγμα, μπορεί κάποιος να αποσυνδέσει τον αισθητήρα του IDS και να περιμένει να δει πόσο γρήγορα θα τηλεφωνήσει η εταιρία για να τους πει ότι δε λειτουργεί. Φυσικά, αυτό δεν πρέπει να γίνεται σε εξοπλισμούς που παρέχουν την κύρια ασφάλεια ενός δικτύου [25].

Το ψηφιακό κέντρο έρευνας [31] προτείνει τη δημιουργία ενός πίνακα στον οποίο σημειώνονται η απόδοση του εξωτερικού συνεργάτη και τα αποτελέσματα του outsourcing, ο οποίος μπορεί να βοηθήσει την επιχείρηση στη διαχείριση της διαδικασίας:

Κριτήρια αξιολόγησης	Υπό-κριτήρια	Πιθανοί τρόποι μέτρησης
Εμπειρία	Εξειδικευμένες γνώσεις	
	Τεχνολογικές Γνώσεις	
Επικοινωνία	Παρουσιάσεις	Αριθμός ανά μήνα
	Συχνότητα ενημερώσεων	Αριθμός ανά μήνα
Τήρηση συμφωνιών	Έγκαιρη παράδοση	% περισσότερος χρόνος
	Τήρηση προϋπολογισμού	% μεγαλύτερο κόστος
	Τήρηση όρων συμφωνίας	Αριθμός τιμωριών
Αξιοπιστία	Έγκαιρη ολοκλήρωση	
	Ποιοτικό αποτέλεσμα	
	Επίτευξη στόχου	

Πίνακας Αξιολόγησης Outsourcing. Πηγή: Avlonitis G

Πίνακας 6: Πιθανοί τρόποι μέτρησης της απόδοσης

Σύμβαση Διασφάλισης Επιπέδου Ποιότητας και Υπηρεσιών (Service Level Agreement-SLA)

Όπως προαναφέρθηκε, για κάθε σχέση outsourcing είναι απαραίτητη μια Σύμβαση Διασφάλισης Επιπέδου Ποιότητας και Υπηρεσιών (Service Level Agreement-SLA). Η σύμβαση αυτή αποτελείται από τους δείκτες, τους τρόπους μέτρησης και τις ποινές-επιβραβεύσεις. Συνήθως, ορίζονται περισσότερα από ένα SLA για κάθε σχέση outsourcing και όλα μαζί αποτελούν το κυρίως μέρος της συμφωνίας των δύο πλευρών.

Σύμφωνα με την εργασία "Outsourcing" της ομάδας εργασίας E5 [7], κατά τη σχεδίαση των SLA πρέπει να δίνεται μεγάλη σημασία στα εξής σημεία:

- Οι δείκτες να είναι σαφείς.
- Η μεθοδολογία της μέτρησης να είναι δυνατό να επαναλαμβάνεται. Μετρήσεις, οι οποίες πραγματοποιούνται πολλαπλές φορές κάτω από τις ίδιες συνθήκες, πρέπει να έχουν ως αποτέλεσμα τις ίδιες μετρήσεις.
- Οι δείκτες να λαμβάνουν υπ' όψιν τους και να ενσωματώνουν το γεγονός ότι οι υπηρεσίες υλοποιούνται με διαφορετικές τεχνολογίες.
- Οι δείκτες να είναι χρήσιμοι τόσο στους χρήστες όσο και στους παρόχους, ώστε να κατανοούν το επίπεδο της υπηρεσίας το οποίο απολαμβάνουν ή παρέχουν, αντίστοιχα.
- Να μην περιλαμβάνονται μη λογικά επίπεδα απόδοσης.
- Οι ρήτρες και οι επιβραβεύσεις δεν πρέπει να είναι εξαντλητικές ούτε για τους παρόχους ούτε και για τις επιχειρήσεις

Επιπλέον, κατά το σχεδιασμό μιας SLA πρέπει να διευκρινιστεί ο τρόπος με τον οποίο θα ελέγχεται η συμφωνία, πως θα παρακολουθούνται τα επίπεδα ποιότητας, πόσο συχνά θα στέλνονται αναφορές και πόσο συχνά θα αναθεωρούνται όλα τα παραπάνω. Ταυτόχρονα, πρέπει να εξασφαλίζεται ότι το επίπεδο των υπηρεσιών θα αναβαθμίζεται περιοδικά ώστε να συμβαδίζει με τα πρότυπα της βιομηχανίας καθώς όροι που αναφέρονται σε ένα συμβόλαιο διαρκείας 5 ή 10 χρόνων μπορεί στο μεσοδιάστημα να θεωρηθούν απαρχαιωμένοι [8]. Τέλος, πρέπει πάντα να καθορίζονται σαφώς τα επιθυμητά επίπεδα υπηρεσιών αλλά και η χειρότερη περίπτωση.

Μέσα σε μια SLA πρέπει να αναφέρονται σαφώς και ξεκάθαρα οι ρόλοι και οι ευθύνες όσον αφορά την ασφάλεια. Δηλαδή, πρέπει να οριστούν οι στόχοι που υπάρχουν για την ακεραιότητα, την εμπιστευτικότητα, τη διαθεσιμότητα, την υπευθυνότητα και τον έλεγχο της χρήσης (use control) [10]. Είναι σημαντικό ένα τέτοιο συμβόλαιο να προστατεύει τις εταιρίες-πελάτες από ανάρμοστη χρήση των δεδομένων ή και του δικτύου από τον πάροχο. Για αυτό θεμιτό είναι το συμβόλαιο να περιέχει μια πρόταση που να δίνει το δικαίωμα στην εταιρία-πελάτη να διατηρεί την ικανότητα για έλεγχο και λεπτομερή εξέταση του περιβάλλοντος του παρόχου, για να μπορεί να διαπιστωθεί αν χρησιμοποιούνται οι πρακτικές που έχουν συμφωνηθεί ή αν παραβαίνονται όροι του συμβολαίου. Σε συνδυασμό με αυτό, καλό είναι να περικλείονται στο συμβόλαιο ενέργειες που πρέπει να κάνει ο πάροχος για να διορθώσει καταστάσεις όπου γίνεται ανάρμοστη χρήση. Πρέπει επίσης να εξασφαλίζεται ότι το προσωπικό του παρόχου καταλαβαίνει και παραμένει πιστό στις εσωτερικές πολιτικές ασφάλειας του πελάτη.

Τέλος, το συμβόλαιο πρέπει να είναι ευέλικτο και να περιλαμβάνει διαδικασίες αλλαγής, δηλαδή, να περιέχει όρους για την περίπτωση που κάποια από τα συστατικά του συμβολαίου αλλάξουν με ένα δίκαιο τρόπο και για συγκεκριμένους επιχειρηματικούς λόγους.

Μια καλή πολιτική διακυβέρνησης εξασφαλίζει σημαντικές παραμέτρους σε μια σχέση outsourcing [27]. Το πρώτο είναι η ομαλή μετάβαση μεταξύ των όσων ίσχυαν μέχρι εκείνη τη στιγμή στον οργανισμό (διαδικασίες, τεχνολογίες, ανθρώπινο δυναμικό), και του καινούριου παρόχου. Επιπλέον, εξασφαλίζει το μετασχηματισμό του οργανισμού έτσι ώστε να μπορέσει να χειριστεί τα καινούρια θέματα που θα προκύψουν και να καλύψει τις νέες ανάγκες. Τέλος, εγγυάται και για τα δύο μέρη την επιτυχία των στόχων που είχαν θέσει αρχικά.

3.3.2 Μοντέλο συμβολαίου βασισμένο στην απόδοση

Στο [33] προτείνεται μία φόρμουλα για να βρίσκεται το βέλτιστο συμβόλαιο (όσον αφορά σε πληρωμές) για την αγορά του outsourcing στην ασφάλεια δικτύων με τη δημιουργία ενός οικονομικού πλαισίου που συνδυάζει το φαινόμενο "moral hazard" και τις επιδράσεις της φήμης ενός παρόχου, όπου η τελευταία μετράτε από τον αριθμό των πελατών που έχει. Το φαινόμενο "moral hazard" είναι η περίπτωση όπου οι πάροχοι προσπαθούν να αποφύγουν κρυφά, ορισμένα καθήκοντα και εργασίες με σκοπό να αυξήσουν τα κέρδη τους. Θεωρείται ότι το πρόβλημα αυτό δεν είναι τόσο σημαντικό στην περίπτωση της ασφάλειας, γιατί οι πάροχοι πρέπει να δουλέψουν σκληρά για να χτίσουν και να διατηρήσουν μια καλή φήμη που είναι απαραίτητη για να επιβιώσουν από τον ανταγωνισμό. Οι αγοραστές δε θα υπογράψουν συμβόλαια με εξωτερικούς παρόχους που δεν μπορούν να προσφέρουν υψηλής ποιότητας υπηρεσίες με συνέπεια. Η φήμη της εταιρίας μετριάζει το πρόβλημα "moral hazard".

Ένα βέλτιστο συμβόλαιο βασίζεται στην απόδοση [33]. Ο βαθμός εξάρτησης από την απόδοση μειώνεται αν οι επιδράσεις της φήμης γίνουν πιο σημαντικές. Επίσης, δείχνεται ότι μια μεγάλη πελατειακή βάση βοηθάει τον πάροχο να βελτιώσει την ποιότητα των υπηρεσιών σημαντικά.

Παρακάτω εμφανίζεται το επαναληπτικό μοντέλο που χειρίζεται όλα τα παραπάνω [33]:

$$
\begin{aligned}
K(v,N) = \max_{p(y),w(y),a} & \int \{y - p(y) + \rho K(w(y),N')\} f(y|a,N)dy \\
\text{st} \quad & N \cdot \int \{(u(p(y)) + \rho w(y))\} f(y|a,N)dy - \phi(a,N) \\
& \quad + (N' - N) \cdot \int \rho w(y) f(y|a,N)dy \geq v \qquad (PK) \\
& a \in \arg\max \{N \cdot \int \{u(p(y)) + \rho w(y)\} f(y|a,N)dy - \phi(a,N) \\
& \quad + (N' - N) \cdot \int \rho w(y) f(y|a,N)\}dy \qquad (IC) \\
& N' = G(y)
\end{aligned}
\tag{1}
$$

όπου

-y: η απόδοση της τρέχουσας περιόδου

-p(y): πληρωμή στον παρόχου

-u: η ροή εισοδήματος του παρόχου προεξοφλημένη μέχρι την τρέχουσα περίοδο

-w(y): το εισόδημα του παρόχου από τη επόμενη περίοδο

-u(.): συνάρτηση χρησιμότητας του παρόχου

-a: το επίπεδο προσπάθειας του παρόχου

-Φ(a,N): το κόστος του να εξυπηρετεί ο πάροχος έναν πελάτη από τους N σε ένα επίπεδο προσπάθειας a

-f(y/a,N): η κατανομή πιθανότητας της απόδοσης δεδομένου του επιπέδου προσπάθειας του παρόχου και του αριθμού των πελατών

-N: ο αριθμός των πελατών

-N΄= G(y): Η επίδραση της φήμης, που σημαίνει ότι ο αριθμός πελατών του παρόχου της επόμενης περιόδου εξαρτάται από την τρέχουσα απόδοση

Αυτό το μοντέλο χρησιμοποιεί την ιδέα του δυναμικού προγραμματισμού: Βελτιστοποιούμε μια περίοδο τη φορά υποθέτοντας βέλτιστη συμπεριφορά για τις επερχόμενες περιόδους. Έτσι, η αντικειμενική συνάρτηση περιέχει δύο όρους: y-p(y) είναι η πληρωμή (με την έννοια του οφέλους) του πελάτη για την τρέχουσα περίοδο και K(w(y),N΄) που αναπαριστά την καλύτερη πληρωμή του πελάτη για την επόμενη περίοδο. Με τον συντελεστή παρούσας αξίας ρ, το y-p(y)+ρK(w(y)) αναπαριστά το μειωμένο κέρδος του πελάτη. Αφού η απόδοση y είναι τυχαία, η αναμενόμενη πληρωμή υπολογίζεται με την ολοκλήρωση του τύπου.

Ο πρώτος περιορισμός, συνήθως, καλείται "promise keeping" (PK) περιορισμός. Περιορίζει την επιλογή του συνόλου p(y) και w(y) από την πλευρά του πελάτη σε αυτά που παρέχουν ικανοποιητική πληρωμή για τον πάροχο. Ο δεύτερος περιορισμός καλείται "incentive compatibility" (IC) περιορισμός. Αυτός ο περιορισμός ενσωματώνει το φαινόμενο "moral hazard" στο μοντέλο, το οποίο σημαίνει ότι για οποιαδήποτε p(y) και w(y), ο πάροχος πάντα επιλέγει το επίπεδο προσπάθειας a που τον συμφέρει περισσότερο. Και οι δύο περιορισμοί πολλαπλασιάζονται με το N που είναι ο αριθμός

πελατών. Οι δεύτεροι όροι στους περιορισμούς αναπαριστούν τη διαφορά στα έσοδα του παρόχου εξαιτίας της αλλαγής στον αριθμό των πελατών. Εάν N΄ > N αυξάνονται τα κέρδη του παρόχου εξαιτίας της αύξησης της ζήτησης.

Γίνονται οι εξής δύο υποθέσεις για το μοντέλο. Καταρχήν, για δεδομένο επίπεδο προσπάθειας, όσο αυξάνεται ο αριθμός των πελατών αυξάνεται και η απόδοση (τεχνολογία κλιμάκωσης). Η δεύτερη υπόθεση έγκειται στο ότι όσο αυξάνεται η προσπάθεια ενός παρόχου αυξάνεται και η απόδοσή του.

Τα συμπεράσματα που βγαίνουν είναι δύο. Το πρώτο αφορά τη δεύτερη υπόθεση και σύμφωνα με αυτό η πληρωμή του παρόχου, p(y), αυξάνεται όσο αυξάνεται το επίπεδο προσπάθειας του (p΄(y)>0). Αυτό σημαίνει ότι η βέλτιστη λύση για την τρέχουσα πληρωμή πρέπει να βασίζεται στην απόδοση.

Το δεύτερο έχει να κάνει με την πληρωμή της επόμενης περιόδου, w(y), και είναι πιο πολύπλοκο. Όταν η μείωση του κέρδους του πελάτη, εξαιτίας της αύξησης του u, είναι μεγαλύτερη όταν ο πάροχος έχει περισσότερους πελάτες, συμβαίνει το εξής: όσο μεγαλύτερη είναι η επίδραση της φήμης του παρόχου, τόσο μικρότερη είναι η διακύμανση του w(y). Είναι η περίπτωση όπου η επίδραση της φήμης ελλατώνει το φαινόμενο "moral hazard". Όταν η μείωση του κέρδους του πελάτη, εξαιτίας της αύξησης του u, είναι μικρότερη όταν ο πάροχος έχει περισσότερους πελάτες, συμβαίνει το εξής: το w(y) αυξάνεται όσο αυξάνεται το y. Είναι η περίπτωση όπου το φαινόμενο της κλιμάκωσης της τεχνολογίας παίζει σημαντικό ρόλο. Σε αυτήν την περίπτωση η πληρωμή πρέπει πάντα να βασίζεται στην απόδοση.

Συνολικά, το μοντέλο δείχνει πως ένας πελάτης μεγιστοποιεί το κέρδος του διαλέγοντας μια πληρωμή p(y) για την τρέχουσα περίοδο και μια μελλοντική πληρωμή w(y), συμπεριλαμβανομένου και του φαινόμενου "moral hazard". Ένα συμβόλαιο βασισμένο σε αυτό το μοντέλο αναμένεται να δώσει κίνητρα στους παρόχους για να δουλέψουν σκληρά.

3.3.3 Μοντέλο συμβολαίου βασισμένο στην τιμή

Εάν ο πελάτης έχει τις κατάλληλες πληροφορίες μπορεί να ελέγχει το περιβάλλον του προμηθευτή έτσι ώστε να αποφευχθεί το φαινόμενο "moral hazard". Σε αυτήν την περίπτωση το πρόβλημα μετατρέπεται στο εξής [36]:

$$\begin{aligned} K(v) &= \max_{P(y),w(y),a} \int [y - P(y) + \rho K(w(y))] f(y,a) dy \\ \text{st} &\quad \int [u(P(y)) + \rho w(y)] f(y,a) dy - \phi(a) \geq v \qquad \text{(PK)} \end{aligned} \tag{2}$$

Λύνοντας αυτό το πρόβλημα καταλήγουμε στο συμπέρασμα ότι η βέλτιστη πληρωμή και η πληρωμή της επόμενης περιόδου δεν εξαρτώνται από την απόδοση.

3.3.4 Κόστος μετάβασης

Ως κόστος μετάβασης εννοούμε οποιοδήποτε κόστος προκύπτει όταν κάνουμε μια οικονομική ανταλλαγή. Στην περίπτωση του outsourcing για την ασφάλεια, το κόστος μετάβασης περιλαμβάνει τα παρακάτω [34]:

- ✓ Κόστος αναζήτησης: Αναφέρεται στα χρήματα, στο χρόνο και στην προσπάθεια που κάνει κάποιος όταν ψάχνει την κατάλληλη εταιρία-πάροχο. Δυστυχώς, η επιλογή δεν είναι εύκολη γιατί δεν υπάρχουν ομόφωνες μετρικές σύγκρισης των πωλητών ασφάλειας.

- ✓ Κόστη συμβολαίου: Αναφέρεται στα λεφτά και την προσπάθεια που απαιτείται για να αναπτυχθεί ένα συμβόλαιο υπηρεσιών το οποίο συγκεκριμενοποιεί τις ευθύνες και του αγοραστή και του παρόχου. Ένα συμβόλαιο βασισμένο στην απόδοση είναι πιο αποτελεσματικό από ότι ένα συμβόλαιο το οποίο περιέχει μια συγκεκριμένη πληρωμή για τον πάροχο [33]. Σε ένα συμβόλαιο βασισμένο στην απόδοση πρέπει να βρεθεί ένα μέτρο για την ποιότητα της απόδοσης όπως επίσης και μια ποινή αν το μέτρο αυτό δεν ικανοποιείται. Η χρονική διάρκεια του συμβολαίου είναι επίσης σημαντική. Η απόφαση μεταξύ ενός βραχυπρόθεσμου

συμβολαίου και ενός μακροπρόθεσμου έχει αντίκτυπο στο κόστος μετάβασης. Ένα μακροπρόθεσμο γλιτώνει χρήματα από τη συνεχή ανάπτυξη συμβολαίων ενώ ένα βραχυπρόθεσμο είναι πιο εύκαμπτο. Ένα βραχυπρόθεσμο συμβόλαιο είναι κατάλληλο για λειτουργίες με μεγάλη αβεβαιότητα. Επειδή ο τομέας της ασφάλειας έχει μεγάλο βαθμό βεβαιότητας, αναμένεται ότι ένα τέτοιο συμβόλαιο θα είναι καλύτερο.

- ✓ Κόστος εγκατάστασης: Αναφέρεται στο κόστος της απόκτησης και του συντονισμού των απαραίτητων συσκευών για το δίκτυο των υπολογιστών ούτως ώστε να υποστηριχτούν οι υπηρεσίες ασφάλειας. Οι περισσότερες εταιρίες βασίζονται σε συγκεκριμένες πλατφόρμες. Για παράδειγμα, πολλοί χειρίζονται μόνο συσκευές συγκεκριμένων κατασκευαστών. Οπότε, αν οι συσκευές που χρησιμοποιεί ένας πιθανός πελάτης μιας εταιρίας-παρόχου δεν ταιριάζουν στις δικές του απαιτήσεις, μπορεί ο πελάτης να αναγκαστεί να αγοράσει καινούριο εξοπλισμό.

- ✓ Κόστος παρακολούθησης: Αναφέρεται στο χρόνο, το χρήμα και την προσπάθεια που απαιτείται για να παρακολουθείς την απόδοση του παρόχου. Είναι πολύ σημαντικό, ο πάροχος να κάνει ότι καλύτερο μπορεί για να προστατέψει μια εταιρία. Για να το ελέγξει αυτό ένας αγοραστής πρέπει περιοδικά να μαζεύει και να αναλύει πληροφορίες σχετικές με την απόδοση του παρόχου όπως επίσης και να αποφασίζει αν τα δεδομένα που του παρουσιάζει ο πάροχος είναι αξιόπιστα.

- ✓ Κόστος συντονισμού: Αναφέρεται στα χρήματα, στο χρόνο και στην προσπάθεια που ξοδεύονται στην επικοινωνία μεταξύ των δύο μερών. Όταν δεν συμβαίνουν σοβαρές επιθέσεις που χρειάζονται άμεση προσοχή, οι πάροχοι, συνήθως, στέλνουνε περιοδικά αναφορές στους πελάτες. Όταν συμβούν σοβαρές επιθέσεις ο πάροχος πρέπει να ξέρει τι πρέπει να κάνει από όσα έχουν ήδη συμφωνηθεί . Σε ορισμένες περιπτώσεις, μπορεί να χρειαστεί να δράσει πριν το αναφέρει στον πελάτη. Σε άλλες περιπτώσεις, μπορεί να χρειαστεί να επικοινωνήσει κατευθείαν με τον πελάτη για να πάρει την συγκατάθεση του πριν κάνει οτιδήποτε. Για

συμβόλαια βασισμένα στην απόδοση, οι διαπραγματεύσεις για να αξιολογηθεί η απόδοση είναι άκρως απαραίτητες για να αποφασιστεί το ποσό της πληρωμής.

- ✓ Κόστος αλλαγής: Αναφέρεται στο χρόνο, το χρήμα και την προσπάθεια που πρέπει να κάνει μια εταιρία για να αλλάξει πάροχο ή για να αναλάβει ενδοεπιχειρησιακά τις υπηρεσίες που μέχρι τότε είχε αναθέσει αλλού. Αυτό το κόστος περιλαμβάνει τα χρήματα που επενδύθηκαν σε υποδομή, η οποία πλέον μπορεί να μην είναι χρήσιμη. Μια εταιρία που θα αποφασίσει μια τέτοια αλλαγή μπορεί να χρειαστεί να αναζητήσει και να προσλάβει καινούριο προσωπικό ή να απολύσει το ήδη υπάρχων. Αν το κόστος αλλαγής είναι μεγάλο, συμφέρει περισσότερο να μείνει στην εταιρία στην οποία έχει ήδη συμβόλαιο και αυτή η περίπτωση καλείται εγκλωβισμός.

Μοντέλο βέλτιστου συμβολαίου για τους πελάτες

Η σχέση που μας δίνει το βέλτιστο συμβόλαιο βασισμένο στην απόδοση μπορεί να τροποποιηθεί ελαφρώς ώστε να συμπεριλάβει και το κόστος μετάβασης. Έτσι, γίνεται ως εξής [34]:

$$
\begin{aligned}
K(v) \quad &= \quad \max_{P(y),w(y),a} \int [y-(1+\alpha)P(y)+\rho K((1+\alpha)w(y))]f(y,a)dy \\
\text{st} \quad &\int [u(P(y))+\rho w(y)]f(y,a)dy-\phi(a) \geq v \qquad \text{(PK)} \\
&a \in \arg\max \int [u(P(y))+\rho w(y)]f(y,a)dy-\phi(a) \quad \text{(IC)}
\end{aligned}
\tag{3}
$$

Όπου aP(y) είναι το κόστος μετάβασης. Το κόστος μετάβασης μοντελοποιείται ως ένα ποσοστό τις αξίας του συμβολαίου, γιατί όσο ένα συμβόλαιο γίνεται μεγαλύτερο, αγοραστής και πάροχος πρέπει να ξοδέψουν περισσότερο χρόνο και χρήμα στο στάδιο των διαπραγματεύσεων πριν και μετά την υπογραφή του συμβολαίου. Αποτελέσματα έρευνας [35] έδειξαν ότι το κόστος μετάβασης μπορεί να είναι ίσο με το 6% του συμβολαίου για συμβόλαια κάτω από $10 εκατομμύρια.

Η λύση αυτού του προβλήματος βελτιστοποίησης (η οποία δεν παρατίθεται γιατί βγαίνει έξω από τους σκοπούς της διπλωματικής αυτής) δείχνει ότι όταν το κόστος μετάβασης

αυξάνεται ενώ όλες οι άλλες παράμετροι παραμένουν ίδιες, ελαττώνεται η θέληση του αγοραστή να προχωρήσει σε outsourcing και μειώνεται το ποσό που είναι διατεθειμένος να πληρώσει για την αγορά των υπηρεσιών.

Μοντέλο βέλτιστου συμβολαίου για τις εταιρίες-προμηθευτές

Οι εταιρίες-πάροχοι διαλέγουν μια τιμή για τα προϊόντα-υπηρεσίες τους η οποία μεγιστοποιεί το κέρδος τους, δεδομένων των τιμών των άλλων εταιριών που παρέχουν παρόμοιες υπηρεσίες ώστε να μπορούν να είναι ανταγωνιστικές. Το πρόβλημα της μεγιστοποίησης του κέρδους για έναν προμηθευτή i μπορεί να μοντελοποιηθεί ως εξής:

$$\max_{P^i}\{P^i \cdot N^i((1+\alpha)P) - C^i(N^i((1+\alpha)P))\} \qquad (4)$$

όπου P^i αναφέρεται στην τιμή την οποία χρεώνει ο i προμηθευτής, P είναι το διάνυσμα που περιέχει όλες τις τιμές όλων των προμηθευτών, N^i είναι η ζήτηση για τον i προμηθευτή και εξαρτάται από το διάνυσμα P. Επίσης, εξαρτάται από την ποιότητα υπηρεσιών του κάθε προμηθευτή. $C^i(.)$ είναι το συνολικό κόστος για τον προμηθευτή i ώστε να εξυπηρετεί N^i πελάτες. Το κόστος αυξάνεται όσο αυξάνεται ο αριθμός των πελατών. Επίσης, το $C^i(.)$ περιλαμβάνει τόσο σταθερά όσο και μεταβλητά κόστη.

Λύνοντας αυτό το πρόβλημα καταλήγουμε στο συμπέρασμα ότι η τιμή για κάθε προμηθευτή εξαρτάται από τις τιμές των υπολοίπων καθώς και στο ότι όταν υπάρχει κόστος μετάβασης οι προμηθευτές χαμηλώνουν τι τιμές τους.

3.4 Η κατάσταση στην Ελλάδα

Στο χώρο των ελληνικών επιχειρήσεων η μέθοδος της λήψης υπηρεσιών μέσω σχέσεων outsourcing δεν γνωρίζει αντίστοιχη αναγνώριση με αυτή του εξωτερικού. Πολύ λίγες είναι οι επιχειρήσεις που καταφεύγουν σε αυτή τη λύση και ως επί των πλείστον οι περιπτώσεις αυτές δεν αφορούν τις υπηρεσίες ασφάλειας.

Σε πολλές περιπτώσεις, μεγάλοι οργανισμοί-εταιρίες προχωρούν στην ίδρυση θυγατρικής η οποία αναλαμβάνει όλες τις υποδομές των τμημάτων πληροφορικής και παρέχει τελικά υπηρεσίες στη μητρική εταιρεία.

Χρήση υπηρεσιών outsourcing στην Ελλάδα κάνουν βέβαια τα παραρτήματα πολυεθνικών επιχειρήσεων. Στις περισσότερες περιπτώσεις, οι υπηρεσίες αυτές παρέχονται από τα κεντρικά γραφεία της επιχείρησης. Έτσι, ο πάροχος των υπηρεσιών είναι συνήθως μεγάλη επιχείρηση του εξωτερικού. Με τον τρόπο αυτό, οι επιχειρήσεις πετυχαίνουν ενιαίο ομοιόμορφο περιβάλλον εργασίας για τους εργαζόμενους τους ανεξάρτητα σε ποιο τοπικό γραφείο βρίσκονται αυτοί.

Η κατάσταση στο δημόσιο

Η κατάσταση στο δημόσιο είναι σχεδόν η ίδια. Η διάδοση της λήψης υπηρεσιών μέσω outsourcing είναι αρκετά μικρή. Το Ελληνικό δημόσιο με πολύ αργά βήματα προχωρά στη λήψη τέτοιων υπηρεσιών αποθαρρύνοντας ουσιαστικά και αντίστοιχες προσπάθειες από τις επιχειρήσεις τόσο αναφορικά με την προσφορά όσο και με τη ζήτηση υπηρεσιών πληροφορικής και επικοινωνιών.

Ενδεικτικά αναφέρουμε έναν ελληνικό οργανισμό, που μετά από παράκληση για διατήρηση της ανωνυμίας τους δε θα αναφέρουμε το όνομα του. Ο συγκεκριμένος οργανισμός διαθέτει δικό του τμήμα πληροφορικής με περίπου 100 άτομα και τμήμα ασφάλειας το οποίο απαρτίζεται από 6 άτομα. Το δίκτυο της επιχείρησης χαρακτηρίζεται ως δίκτυο μέγιστης σημασίας, με πληροφορίες ζωτικής σημασίας να διακινούνται καθημερινά μέσα από αυτό. Το δίκτυο του είναι κατανεμημένο ανά την Ελλάδα και συνδέεται με δίκτυα αντίστοιχων οργανισμών του εξωτερικού.

Στάση φορέων απέναντι στο outsourcing

Μετά από συνέντευξη με έναν από τους υπεύθυνους της ασφάλειας του δικτύου, ήταν φανερό ότι όχι απλά δεν υπήρχε καμία πρόθεση για να προχωρήσει ο οργανισμός στη λήψη υπηρεσιών μέσω outsourcing αλλά υπήρχε και άγνοια επί του θέματος. Συγκεκριμένα:

- Τα μέλη του τμήματος ασφάλειας δεν γνώριζαν ότι μπορούσαν να αναθέσουν την ασφάλεια του δικτύου τους σε άλλη εταιρία και όπως ήταν φυσικό είναι πολύ καχύποπτοι απέναντι σε μια τέτοια κίνηση.
- Επίσης, θεωρούν ότι καμία σοβαρή εταιρία δε θα επέτρεπε σε οποιονδήποτε άλλον, να έχει την οποιασδήποτε μορφής πρόσβαση στο δίκτυο της.
- Ο υπεύθυνος της ασφάλειας δήλωσε κατηγορηματικά ότι δε θα ανέθετε την ασφάλεια του δικτύου αλλού γιατί δεν θα το εμπιστευόντουσαν σε κάποιον άλλον.
- Επιπλέον, πιστεύει ότι η ήδη υπάρχουσα νομοθεσία δεν είναι αρκετή για να προστατέψει τέτοιου είδους σχέσεις.
- Γενικότερα, ο οργανισμός δεν ήταν ενημερωμένος για το πως λειτουργεί μια τέτοια διαδικασία και για τα πλεονεκτήματα που πηγάζουν από αυτήν.
- Ακόμα όμως και μετά από μια μικρή ενημέρωση συνέχισαν να είναι καχύποπτοι και αρνητικοί απέναντι σε μια τέτοια κίνηση.

Προϊόντα ασφάλειας

Όπως είναι φυσικό, ο συγκεκριμένος οργανισμός συνεργάζεται με εταιρίες που παρέχουν ασφάλεια για την αγορά υλικού και λογισμικού που είναι απαραίτητα για την προστασία του δικτύου, όπως Firewalls και IDSs. Μέσα από διαγωνισμούς επιλέγουν αυτές που ικανοποιούν καλύτερα τις ανάγκες του και αφού εγκαταστήσουν τα προϊόντα τους δεν εμπλέκονται σε καμία άλλη διαδικασία. Συγκεκριμένα, η λέξη που χρησιμοποιήθηκε είναι ότι μετά την εγκατάσταση "εξαφανίζονται". Την πολιτική ασφάλειας που θα ακολουθήσει το Firewall την αποφασίζουν οι ίδιοι και στήνουν το Firewall μόνοι τους. Υπογράφουν με τους προμηθευτές πολύ αυστηρά συμβόλαια και συμβάσεις εμπιστευτικότητας οι οποίες προϋποθέτουν ότι μετά το πέρας της συνεργασίας τους δε θα έχουν καμία ανάμειξη στην περαιτέρω διαδικασία της ασφάλειας. Από τις εταιρίες αυτές ο συγκεκριμένος οργανισμός ζητάει, επίσης, μέσω σεμιναρίων, την τεχνογνωσία, τη δύναμη και τη γνώση να μπορούν να υποστηρίξουν μόνοι τους το οποιοδήποτε προϊόν και υπηρεσία και μετά δεν θέλουν καμία σχέση με αυτούς. Σκοπός του οργανισμού είναι να είναι ανεξάρτητος και να μην εμπλέκεται στο δίκτυο της επιχείρησης κάνεις άλλος πέρα από τους ίδιους. Συχνά προσλαμβάνουν συμβούλους, με τους οποίους ακολουθούν

την ίδια ακριβώς πολιτική, για να τους βοηθήσουν στις διάφορες επιλογές που έχουν αλλά και για να μάθουν από αυτούς,

Παρακολούθηση και έλεγχος δικτύου

Σε ερώτηση για το ποια προϊόντα θα εμπιστευόντουσαν σε μια άλλη εταιρία απάντησαν κατηγορηματικά όχι σε ότι αφορούσε την παρακολούθηση και τον έλεγχο του δικτύου καθώς και την ανάλυση συναγερμών και προειδοποιήσεων. Είναι εργασίες που διατηρούνται ενδοεπιχειρησιακά και θεωρούνται μεγάλης σημασίας για να τις αναθέσουν κάπου αλλού.

Ψηφιακά πιστοποιητικά

Η έκδοση ψηφιακών πιστοποιητικών γίνεται από τον ίδιο τον οργανισμό μέσω έτοιμης εμπορικής λύσης. Μέσα από σεμινάρια, οι υπεύθυνοι της ασφάλειας μάθανε τον τρόπο λειτουργίας της και δημιούργησαν μόνοι τους τα πιστοποιητικά. Θεωρούν ότι με αυτόν τον τρόπο, μπορούν οι ίδιοι να αποφασίζουν για το πότε θα ανανεώνονται, από ποιον, πόσο μεγάλο θα είναι το κλειδί κτλ. Επίσης, είναι πιο οικονομική λύση αφού ανά πάσα στιγμή μπορείς να προσθέσεις, να σβήσεις ή να τροποποιήσεις ένα πιστοποιητικό χωρίς να πρέπει να πληρώσεις επιπλέον και το κόστος από άποψης χρόνου και εργασίας των υπαλλήλων του οργανισμού είναι ελάχιστο σε σχέση με αυτό που θα πλήρωνες σε μια εταιρία. Επιπλέον, υπάρχει πάντα και το θέμα της εμπιστοσύνης γιατί η εταιρία που θα σου προσφέρει τα πιστοποιητικά θα ξέρει ένα μέρος του κλειδιού σου. Σε περίπτωση που ο οργανισμός αποφάσιζε να αναθέσει τη δημιουργία πιστοποιητικών σε άλλη εταιρία, θα επιλεγόταν κάποια μεγάλη εταιρία με κύρος στον τομέα της όπως η Verisign με την οποία και συνεργάζονται συμβουλευτικά για το θέμα των πιστοποιητικών.

Πολιτική ασφάλειας

Η πολιτική ασφάλειας αναπτύσσεται ενδοεπιχειρησιακά. Θα εμπιστευόντουσαν, όμως, μια εταιρία που παρέχει ασφάλεια να τους συμβουλέψει για το πώς θα πρέπει να την αναπτύξουν, αλλά μέχρι εκεί ώστε να μην μπορεί να έχει πρόσβαση η ίδια στο δίκτυο της.

Όπως είναι ξεκάθαρο, ο φορέας δεν είναι θετικά προκατειλημμένος απέναντι σε μία τέτοια κίνηση. Γενικεύοντας, οι υπεύθυνοι της ασφάλειας είχαν την άποψη ότι καμία εταιρία που διαχειρίζεται κρίσιμα δεδομένα δεν πρόκειται να εμπιστευτεί την ασφάλεια του δικτύου της αλλού. Μόνο μικρές επιχειρήσεις θα μπορούσαν να προβούν σε μία τέτοια κίνηση.

Μετά από μία απαρίθμηση ορισμένων πλεονεκτημάτων που απορρέουν από την ανάθεση της ασφάλειας του δικτύου ή μέρος αυτής σε τρίτους, πολύ σημαντικά θεωρήθηκαν η αποδέσμευση του προσωπικού και η απελευθέρωση χρόνου ώστε να δοθεί μεγαλύτερη προσοχή το αντικείμενο που αποτελεί τον πυρήνα της επιχείρησης.

Υπήρχε μια επιφυλακτικότητα, από την πλευρά των υπευθύνων, για το κατά πόσο το κόστος μειώνεται μέσω του outsourcing, όπως, επίσης, και για το ότι οι εταιρίες–πάροχοι θα διαθέτουν τα πιο σύγχρονα τεχνολογικά μέσα και εφαρμογές. Ο έλεγχος του δικτύου 24 ώρες τη μέρα, η συνεχής ενημέρωση και η γνώση μέσω της συνεργασίας θεωρήθηκαν θετικά στοιχεία μεν αλλά όχι κύριας σημασίας.

Συμπερασματικά, η κατάσταση που υπάρχει αυτήν τη στιγμή στην Ελλάδα δεν ενδείκνυται για την ανάπτυξη σχέσεων outsourcing. Η νοοτροπία των επιχειρήσεων-οργανισμών είναι τέτοια που δύσκολα θα εμπιστευτούν σε τρίτους τα πολύτιμα δεδομένα της επιχείρησης τους. Η κατάσταση αυτή θα αργήσει να αλλάξει. Υπάρχει, όμως, η πεποίθηση ότι στο πλαίσιο του Γ' ΚΠΣ και του προγράμματος για την Κοινωνία της Πληροφορίας, θα δημιουργηθεί το κατάλληλο θεσμικό πλαίσιο και θα οριστούν οι πρότυπες διαδικασίες, οι οποίες θα αποτελέσουν τη βάση για την εξάπλωση των υπηρεσιών outsourcing στον Ελληνικό Δημόσιο και Ιδιωτικό τομέα.

4.1 Case study 1: Regence Group

Το Regence Group, ένας από τους μεγαλύτερους και πιο σημαντικούς ασφαλιστικούς οργανισμούς στον τομέα της υγείας, αποτελεί μια ένωση ασφαλιστικών εταιριών στην Ουάσιγκτον, στο Όρεγκον, στη Γιούτα και το Αίνταχο. Πριν από τέσσερα χρόνια περίπου αποφασίστηκε να συγχωνεύσουν τα μεμονωμένα τμήματα της ασφάλειας σε κάθε οργανισμό σε ένα τμήμα και να συγκεντρώσουν την εταιρική ασφάλεια του δικτύου κάτω από ένα και μόνο άτομο [43].

Το τμήμα της ασφάλειας πληροφορίας του Regence Group δεν είχε το προσωπικό, ούτε σε ποσότητα αλλά ούτε και σε τεχνογνωσία για να διαχειρίζεται έναν σταθμό ελέγχου 24 ώρες τη μέρα, 7 ημέρες την εβδομάδα, παρόλο που αυτό χρειαζόταν η εταιρία. Επιπρόσθετα, το δίκτυο της εταιρίας χρησιμοποιούσε πολλές και διαφορετικές πλατφόρμες το οποίο απαιτούσε και περισσότερη πραγματογνωμοσύνη.

Τότε άρχισαν να μελετούν την περίπτωση του outsourcing. Το πρώτο πράγμα που έκαναν είναι να αναλογιστούν τι χρειάζεται ώστε να έχει η εταιρία ένα αποτελεσματικό πλαίσιο ασφάλειας. Χωρίσανε τα καθήκοντα τους σε δύο κατηγορίες: σε αυτά που πρέπει να γίνονται εσωτερικά και αυτά που θα δώσουν για outsourcing. Η παρακολούθηση περιστατικών παραβιάσεων ασφάλειας ήταν από τα πρώτα πράγματα που σκέφτηκαν αφού δεν είχαν το προσωπικό για να χειρίζεται ένα full-time σταθμό ελέγχου. Το προσωπικό που υπήρχε δεν ήξερε πολλά για τις διάφορες πλατφόρμες σε κάθε σημείο του Regence Group. Όσον αφορά τη διαδικασία ελέγχου, δεν υπήρχαν οι άνθρωποι που θα μπορούσαν να συσχετίζουν και να αναγνωρίζουν αληθινές απειλές, να εξυγιαίνουν τις ανωμαλίες και να ξεκαθαρίζουν τα αποτελέσματα του scanning και γενικότερα να είναι μπροστά από κάθε απειλή που αναδύεται.

Το Regence Group έψαξε ανάμεσα σε πολλές εταιρίες που παρέχουν παρακολούθηση της ασφάλειας. Τα κριτήρια της επιλογής της ήταν η αδιάλειπτη παροχή των υπηρεσιών ασφάλειας καθώς και η φήμη στην αγορά.

Αποτελέσματα: Αποτελεσματική ασφάλεια δικτύου με μειωμένο αριθμό συναγερμών ώστε να μπορούν να τους χειριστούν εσωτερικά από την επιχείρηση.

Για τη Regence η επένδυση που κάνανε τους επιστράφηκε ως εξής:

1. Με μία σχεδόν τέλεια καταγραφή της ασφάλειας του δικτύου
2. Με την ικανότητα του παρόχου να μειώνει τους συναγερμούς υψηλού επιπέδου σε έναν αριθμό ο οποίος είναι εύκολο να χειριστεί από το υπάρχων, περιορισμένο δυναμικό της επιχείρησης.

Σύμφωνα με στατιστικά του οργανισμού πριν και μετά την ανάθεση της ασφάλειας στον πάροχο, το τέταρτο τρίμηνο του 2002, το σύστημα ανίχνευσης εισβολέων κατέγραψε 145,465 περιστατικά. Από αυτά 12,875 ήταν συναγερμοί υψηλού επιπέδου, δηλαδή σοβαρές προσπάθειες να εισβάλουν στο δίκτυο της επιχείρησης. Άλλες 12,300 ήταν συναγερμοί μεσαίου επιπέδου και οι υπόλοιπες 120,000 ήταν συναγερμοί χαμηλού επιπέδου. Ο έλεγχος και το φιλτράρισμα των γεγονότων από τον πάροχο μείωσε τον αριθμό των περιστατικών με τα οποία έπρεπε να ασχοληθεί η Regence στα 200. Ο επικεφαλής σχεδιασμού ασφάλειας του οργανισμού, δήλωσε ότι δεν είχε προσωπικό να ασχοληθεί με 140.000 περιστατικά. Μάλιστα δεν είχε καν το προσωπικό να ασχοληθεί με τα 12.000 περιστατικά. Χάρη στον πάροχο έφταναν σε αυτούς μόνο οι πληροφορίες που ήταν απαραίτητες και μπορούσαν να συγκεντρωθούν σε επιθέσεις που είχαν πραγματική σημασία η αξία του οποίου θεωρεί τεράστια.

Η γρήγορη επέμβαση της εταιρίας που ανέλαβε την ασφάλεια μείωσε επίσης και τα αποτελέσματα των επιθέσεων. Σύμφωνα με το FBI, περίπου το 1% των επιθέσεων στο ίντερνετ είναι επιτυχείς [43]. Δηλαδή, στη συγκεκριμένη περίπτωση θα έπρεπε η εταιρία να είχε δεχθεί 1400 πετυχημένες επιθέσεις μέσα σε ένα τρίμηνο. Ακόμα και αν λάβουμε υπ' όψιν μόνο τον αριθμό των συναγερμών υψηλού επιπέδου, ο οποίος ήταν 12.000,

αυτό σημαίνει 120 πετυχημένες επιθέσεις. Επειδή ο πάροχος μπορούσε να τους ενημερώνει άμεσα ώστε να μπορούν να ανταποκριθούν στις επιθέσεις όταν αυτές συνέβαιναν, υπήρχε μόνο μία σοβαρή παραβίαση εκείνη την περίοδο και ήταν ο Nimda. Αλλά ακόμη και ο Nimda ο οποίος κατάστρεψε τόσες άλλες εταιρίες, περιορίστηκε πολύ γρήγορα στο δίκτυο της Regence. Πριν ακόμα ο Nimda χτυπήσει το δίκτυο της, ο πάροχος επικοινώνησε τηλεφωνικά και εξήγησε τι συνέβαινε. Στη Regence άρχισαν να κλείνουν όλες τις πόρτες του συστήματος και να το ενημερώνουν, με αποτέλεσμα ο Nimda να χτυπήσει μόνο το 10% των υπολογιστών γραφείων και το 5% των server.

Η Regence αρχικά είχε κάνει συμβόλαιο δύο χρόνων με τον πάροχο με την προοπτική ότι αυτά τα δύο χρόνια θα τα χρησιμοποιούσαν ώστε να μάθουν και να αναπτύξουν τις δικές τους ικανότητες παρακολούθησης των συμβάντων. Μετά θα αναλάμβαναν οι ίδιοι. Αλλά την πρώτη χρονιά κατάλαβαν ότι η Regence δεν μπορούσε να αντιγράψει την ταχύτητα και την ακρίβεια των υπηρεσιών που προσέφερε ο πάροχος, και ότι το να συνεχίσουν να δίνουν την ασφάλεια για outsourcing ήταν η καλύτερη απόφαση.

4.2 Case study 2: A Global Supplier of Integrated Circuits

Για λόγους εμπιστευτικότητας και ασφάλειας το όνομα της εταιρίας που έδωσε για outsource την ασφάλεια δε θα αναφερθεί. Κάθε φορά που θα γίνεται αναφορά στην εταιρεία θα αποκαλείται εταιρία Α.

Η εταιρία Α είναι ένας παγκόσμιος προμηθευτής ολοκληρωμένων κυκλωμάτων και τηλεπικοινωνιακού εξοπλισμού. Το παγκόσμιο δίκτυο της είναι διασκορπισμένο όπως και η επιχείρηση και αποτελείται από 20.000 υπολογιστές και 12.000 ανθρώπους. Ο διευθυντής ασφάλειας της ηλεκτρονικής πληροφορίας και το ανά τον κόσμο διασκορπισμένο προσωπικό του είναι υπεύθυνοι για τη φύλαξη του δικτύου της εταιρίας [42].

Όταν έγινε προφανές ότι η εταιρία έπρεπε να κάνει περισσότερα για την ασφάλεια αποφάσισαν να αξιολογήσουν τη λύση του outsourcing. Ο διευθυντής ασφάλειας δήλωσε

ότι είχαν κουραστεί να ξοδεύουν τον περισσότερο χρόνο τους με το να αναλύουν συναγερμούς, να ξεκαθαρίζουν τους ψεύτικους από τους αληθινούς και να θέτουν προτεραιότητες. Με αυτόν τον τρόπο τους έμενε πολύ λίγος χρόνος να ερευνούν και να κάνουν τις κατάλληλες ενέργειες. Επιπρόσθετα, λόγω του μικρού αριθμού του ανθρώπινου δυναμικού και των παγκοσμίων διαστάσεων απαιτήσεων δεν μπορούσαν να παρέχουν εικοσιτετράωρη κάλυψη για όλα τα συστήματα που διακινούσαν κρίσιμες πληροφορίες. Η εταιρεία Α χρειαζόταν real-time προστασία και έλεγχο. Για αυτό θέλανε κάποιος άλλος να αναλάβει τη λεπτομερή ανάλυση των γεγονότων, ώστε να φτάνουν σε αυτήν μόνο οι περιπτώσεις που απαιτούσαν προσοχή. Προτίμησαν να χρησιμοποιήσουν τους ανθρώπους τους με καλύτερο τρόπο, ώστε να εξασφαλίζουν ότι τα υπόλοιπα project τους, αναπτύσσονται με ασφάλεια. Μηχανικός ασφάλειας της εταιρίας, που ασχολήθηκε με την ατελείωτη ροή συναγερμών και προειδοποιήσεων, δήλωσε χαρακτηριστικά: «Ξόδευα μεγάλο μέρος του χρόνου κάνοντας αναλύσεις. Δεν μπορούσα ποτέ να κάνω real-time έλεγχο. Ήμουν τουλάχιστον μία μέρα πίσω. Τη συγκεκριμένη χρονική στιγμή η εταιρία προσέθετε και άλλες επιχειρηματικές λειτουργίες στις πύλες του ίντερνετ. Αυτές οι καινούριες λειτουργίες δεν είχαν πάντα την καλύτερη δυνατή ασφάλεια άλλα έπρεπε να τις υποστηρίζουμε για επιχειρηματικούς λόγους. Ο έλεγχος ήταν η προφανής λύση αλλά δε θέλαμε να αγοράσουμε προϊόντα και να το κάνουμε μόνοι μας γιατί δεν είχαμε ούτε χρόνο ούτε ο προσωπικό για να υποστηρίξουμε ακόμα περισσότερα προϊόντα. Χρειαζόμασταν κάποιον να λύσει το πρόβλημα για εμάς.»

Η λύση βρέθηκε μέσα από το outsourcing. Η εταιρία Α αξιολόγησε πέντε υποψηφίους και επέλεξαν εκείνον που θεώρησαν πιο ικανό. Κατά τη διάρκεια της αξιολόγησης εξέτασαν πολλές εκδοχές αλλά προτίμησαν αυτή που φαινόταν η πιο απλή: εγκαταστάθηκε μια εφαρμογή, η οποία εξασφάλιζε ασφαλή επικοινωνία μεταξύ του παρόχου και του πελάτη. Η εγκατάσταση της εφαρμογής ήταν εύκολη και δεν επηρέαζε το δίκτυο της εταιρείας, που διαχειρίζονταν κρίσιμες πληροφορίες. Επίσης, λύθηκε και το πρόβλημα του εσωτερικού ελέγχου του δικτύου (scan) με την εγκατάσταση μιας συσκευής παράλληλα με την εφαρμογή η οποία εκτελούσε εσωτερικό έλεγχο.

Ένα άλλο στοιχείο που έπαιξε σημαντικό ρόλο στην επιλογή της συγκεκριμένης εταιρίας είναι ο διαχωρισμός της διαχείρισης από τον παρακολούθηση του δικτύου. Οι περισσότερες επιχειρήσεις ήθελαν απλά να διαχειρίζονται το περιβάλλον της εταιρίας Α το οποίο η εταιρία δεν μπορούσε να επιτρέψει. Αυτό που ήθελαν ήταν ένας συνεργάτης που θα μπορούσε να παρακολουθεί το δίκτυο και επιλεκτικά να διαχειρίζεται κάποιες συσκευές.

Αποτελέσματα: Το προσωπικό της εταιρίας έχει τώρα το χρόνο και την ικανότητα να επικεντρωθεί σε στρατηγικά θέματα ασφαλείας. «Πάντα υπάρχουν θέματα», δήλωσε ο μάνατζερ της εταιρείας, «Η ασφάλεια είναι ένας κινούμενος στόχος. Τώρα μπορούμε να δεχτούμε κάποιους από τους κινδύνους που γνωρίζουμε σήμερα και να κατανείμουμε ξανά του πόρους μας ώστε να επικεντρωθούμε στην εσωτερική ασφάλεια. Μπορούμε να εξετάσουμε νέες τεχνολογίες, με τις οποίες παλιότερα δεν είχαμε χρόνο να ασχοληθούμε. Μπορούμε, επίσης, να χρησιμοποιήσουμε το εκπαιδευμένο, σε θέματα ασφάλειας, προσωπικό ώστε να μάθουμε πως χτίζεται η ασφάλεια σε προχωρημένα project IT τα οποία περιλαμβάνουν κινητές και ασύρματες εφαρμογές. Επειδή κάποιος έξυπνα εξετάζει τα log της εταιρίας και εκτελεί ελέγχους, οι μηχανικοί μας έχουν το χρόνο να ασχοληθούν με πράγματα τα οποία ούτε θα είχαμε προσέξει στο παρελθόν».

Η εταιρία-πάροχος, αρχικά, ήλεγχε τις πύλες ίντερνετ της εταιρίας Α στις Ηνωμένες Πολιτείες. Το σύστημα του πελάτη δεχόταν επιθέσεις συνέχεια. Η εταιρία-πάροχος τους προειδοποιούσε τακτικά λέγοντας τους τι συμβαίνει και παρέχοντας τους πληροφορίες σχετικά με τις IP διευθύνσεις που διέπραξαν τις επιθέσεις. Επιπλέον, ήλεγχε τα logs του συστήματος όπως επίσης τα firewalls, τα IDSs και τους routers. Ενώ παλιότερα η εταιρία Α βασιζόταν μόνο στα firewall και τα IDSs, τώρα αν κάποιο από αυτά δεν καταφέρει να σταματήσει την επίθεση, είναι σίγουρο ότι η εταιρία-πάροχος θα την εντοπίσει. Σύμφωνα με τον μάνατζερ της εταιρίας Α η συχνότητα των συναγερμών που έπρεπε να διαχειριστεί η εταιρία καθιστούσε δύσκολο τον εντοπισμό των πραγματικών προβλημάτων. Η εταιρία με την οποία συνεργάστηκαν τους βοήθησε να αλλάξουν τους κανόνες των firewall και των IDSs ώστε να είναι πιο αποτελεσματικά. Η αξία αυτού και μόνο ήταν τεράστια.

Όταν προέκυπτε κάποιο πρόβλημα η αντίδραση του παρόχου ήταν άμεση, δίνοντας μια λύση για το εκάστοτε πρόβλημα το συντομότερο δυνατόν. Επίσης, πλέον η εταιρία Α έχει τον έλεγχο του συνολικού κόστους που απαιτείται για τη διατήρηση της ασφάλειας του δικτύου της και μπορεί να υπολογίσει την αποτελεσματικότητα των επενδύσεων της σε μετρήσιμους όρους.

4.3 Case study 3: Deutsche Lufthansa AG

Η Lufthansa είναι μια από τις πιο επιτυχημένες αεροπορικές εταιρίες και είναι γνωστή για την αποτελεσματικότητά και την συνέπεια της [38]. Οι πύλες διαδικτύου Lufthansa.com και miles-and-more.com είναι παράγοντες κλειδιά για τις πωλήσεις της εταιρίας και για τις σχέσεις της εταιρίας με τους πελάτες. Οι πύλες δέχονται καθημερινά παραπάνω από οχτώ εκατομμύρια επισκέπτες, στους οποίους παρέχουν πληροφορίες για τις πτήσεις και τους δίνουν τη δυνατότητα να ψάξουν και να κάνουν κράτηση για την πτήση που τους ενδιαφέρει on-line. Η σχέση μεταξύ της εταιρίας και των πελατών της στηρίζεται σε μεγάλο βαθμό στις υπηρεσίες που προσφέρονται μέσω ίντερνετ.

Η Lufthansa δίνει πολύ μεγάλη σημασία στην ποιότητα και στην ασφάλεια κυρίως λόγω των ευαίσθητων δεδομένων των πελατών που διακινούνται μέσα από τις πύλες της. Την ευθύνη για τα υψηλότερα δυνατά στάνταρ ασφάλειας και την ομαλή και συνεχή λειτουργία των πυλών της, έχει το τμήμα ηλεκτρονικού εμπορίου και απευθείας πωλήσεων (E-commerce and Direct Sales Department) και είναι μια πολύ απαιτητική εργασία. Η πρόκληση δεν είναι απλώς η διαχείριση μεγάλου αριθμού επισκεπτών καθημερινά ή η τεχνική δυσκολία των πυλών. Είναι πιο πολύπλοκο λόγω του γεγονότος του ότι η εταιρία είναι καθημερινά στόχος πολλών επιθέσεων.

Από τότε που δημιουργήθηκαν οι πύλες το 1996, η Lufthansa χρησιμοποιεί κρυπτογράφηση SSL για να προστατέψει τις πληροφορίες των πελατών της, κυρίως όταν χρησιμοποιούνται πιστωτικές κάρτες. Αυτό σημαίνει ότι χρησιμοποιήθηκαν τα υψηλότερα δυνατά στάνταρ ασφάλειας. Παρόλο, όμως, που η λύση που είχε βρεθεί εκπληρώνει τις πολύ αυστηρές απαιτήσεις ασφάλειας της εταιρίας, η υλοποίηση της προκαλούσε πολύ μεγάλο φόρτο εργασίας στους διαχειριστές του συστήματος.

Στο παρελθόν τα πιστοποιητικά SSL των server παράγονταν μέσα από μια ποικιλία αρχών πιστοποίησης. Αυτή η διαδικασία δεν ήταν αυτοματοποιημένη και χρειαζόταν χρόνος και προσπάθεια και για να τα παραγγείλουν αλλά και για να τα εγκαταστήσουν. Ακόμα πιο πολύπλοκο το έκανε το γεγονός ότι δεν μπορούσε να επιτευχθεί καμία γρήγορη και περιεκτική επισκόπηση για τα διάφορα πιστοποιητικά και τις ημερομηνίες λήξης τους.

Ειδικοί σε θέματα διαδικτύου της Deutsche Lufthansa AG, δήλωσαν ότι παρόλο που υπήρχε η λύση για τις απαιτήσεις ασφάλειας της εταιρίας, δεν υπήρχε μια σαφής και γενική εποπτεία. Επίσης, η διαδικασία της παραγγελίας ήταν διαμοιρασμένη και ήταν δύσκολο να ελεγχθεί. Μπορούσε να πάρει μέχρι και πέντε μέρες μεταξύ του χρόνου παραγγελίας ενός πιστοποιητικού και του χρόνου εξουσιοδότησης του. Όσο η κίνηση στις πύλες αυξανόταν, τόσο αυξανόταν και η πολυπλοκότητα της δομής που απαιτούνταν για να υποστηριχτούν οι πύλες. Αυτό αύξησε το φόρτο εργασίας και έβαλε όρια στο υπάρχων σύστημα διαχείρισης πιστοποιητικών, το οποίο οδήγησε σε λάθη. Για να βεβαιώσει ότι οι διαχειριστές ασχολούνταν με πιο παραγωγικά πράγματα και για να μειώσουν το ρυθμό με τον οποίον τα λάθη γίνονταν, η Lufthansa έψαξε μια λύση η οποία θα απλοποιούσε και θα αυτοματοποιούσε τη διαδικασία της παραγωγής πιστοποιητικών για τους server. Αυτή ήταν η υιοθέτηση της υποδομή δημοσίου κλειδιού για SSL που διαχειρίζεται γνωστή εταιρία και η οποία παρέχει μια ολοκληρωμένη λύση διαχείρισης για πιστοποιητικά server.

Αποτελέσματα: Μέσω αυτής της διαδικασίας τα πιστοποιητικά παράγονται γρήγορα και αποτελεσματικά μέσα από μια απλοποιημένη και ευέλικτη διαδικασία παραγγελίας. Επιπρόσθετα, η εγκατάσταση των πιστοποιητικών μπορεί να γίνει μέσα σε λίγα λεπτά, το οποία σημαίνει ότι η όλη διαδικασία παίρνει λιγότερο από μια ώρα σε σχέση με τις πέντε μέρες που απαιτούνταν παλιότερα.

Επίσης, η υπηρεσία που υιοθετήθηκε προσέφερε στους διαχειριστές ολοκληρωμένες αναφορές για οποιοδήποτε πιστοποιητικό σε πολύ μικρό χρονικό διάστημα και δε

χρειαζόταν να προστεθεί κάποιο περαιτέρω λογισμικό. Την όλη διαδικασία μπορεί να διαχειριστεί ένας ίντερνετ browser.

Κάτι ακόμα πολύ σημαντικό είναι ότι ο πάροχος ήταν ο μοναδικός ο οποίος υποστηρίζει (backs) τα πιστοποιητικά του με ένα πρόγραμμα εγγύησης για την περίπτωση οικονομικής καταστροφής και η οποία υποβάλει τη διαδικασία εξουσιοδότησης των πιστοποιητικών για αποτίμηση σε μέλος τους σώματος λογιστών. Η Lufthansa δεν έψαχνε μόνο για έναν πάροχο του οποίου το προϊόν θα αγόραζε, αλλά για έναν συνεργάτη του οποίου η γνώση και η εμπειρία θα βοηθούσε στην εύρεση της καλύτερης λύσης και ο οποίος θα υποστήριζε την εταιρία όταν τον χρειαζόταν.

Η συγκεκριμένη υποδομή δημοσίου κλειδιού για SSL ξεπέρασε τις προσδοκίες της Lufthansa όχι μόνο σε όρους ασφάλειας, διαχειρισιμότητας και υποστήριξης αλλά και σε όρους κόστους. Εκτιμάται ότι το κόστος ανά πιστοποιητικό server μειώθηκε 20-25%. Αυτό οφείλεται στο μειωμένο κόστος ανά πιστοποιητικό αλλά και στη μείωση του φόρτου εργασίας όσον αφορά τη διαχείριση. Ακόμα πιο σημαντικό είναι ότι το επίπεδο ασφαλείας αυξήθηκε μέσω της εξάλειψης των λαθών που αφορούσαν ληγμένα πιστοποιητικά. Αυτό σημαίνει ότι τώρα οι πελάτες της μπορούν να την εμπιστευθούν ακόμα περισσότερο.

Κεφάλαιο 5: Εφαρμογή

5.1 Το περιβάλλον εφαρμογής

Ο Πανελλήνιος Ιατρικός Σύλλογος αποφασίζει να παρέχει στα μέλη του τη δυνατότητα να χρησιμοποιούν την τράπεζα πληροφοριών του μέσω του διαδικτύου καθώς, επίσης, και να επικοινωνούν μεταξύ τους αλλά και με το σύλλογο με ασφαλή τρόπο. Επιπλέον, θέλει να μπορούν τα μέλη να αποδεικνύουν με μοναδικό τρόπο την ταυτότητα τους κατά τη διάρκεια της επικοινωνίας τους με ασθενείς, ασφαλιστικά ταμεία, και οποιοδήποτε άλλο πρόσωπο ή φορέα. Σε όλες τις παραπάνω περιπτώσεις υπάρχει η ανάγκη αυθεντικοποίησης των χρηστών. Πρέπει να υπάρχει η δυνατότητα λήψης απόφαση για το κατά πόσο ο εκάστοτε χρήστης έχει πρόσβαση στην τράπεζα πληροφοριών και, αν ναι, αν έχει πρόσβαση σε ολόκληρη τη βάση δεδομένων ή σε ορισμένες μόνο πληροφορίες. Επίσης, σε περίπτωση παραβιάσεως του συστήματος θα μπορεί να ελεγχθεί ποιος είχε τελευταίος πρόσβαση σε αυτό και ποιες ήταν οι ενέργειες του. Επιπλέον, μέσω της αυθεντικοποίησης, μπορεί να εξασφαλιστεί η πρόσβαση σε ορισμένες υπηρεσίες από συγκεκριμένα και μόνο άτομα. Γενικότερα, η διαδικασία της αυθεντικοποιησης στο σύστημα του Συλλόγου θα αποτελέσει μια πρώτη γραμμή άμυνας απέναντι σε επίδοξους εισβολείς και θα παρέχει τη δυνατότητα απαγόρευσης πρόσβασης μη εξουσιοδοτημένων χρηστών, απαιτώντας κάθε φορά από τους χρήστες να επικυρώνουν την εξουσιοδότηση τους να χρησιμοποιούν το σύστημα [41].

Ο Ιατρικός Σύλλογος αποτελείται από επιμέρους παραρτήματα σε ορισμένες μεγάλες πόλεις (Αθήνα, Θεσσαλονίκη, Λάρισα, Βόλο, Πάτρα, Ηράκλειο). Μέσω της κεντρικής σελίδας των τοπικών συλλόγων, τα μέλη έχουν την δυνατότητα να ελέγχουν τους λογαριασμούς ηλεκτρονικού ταχυδρομείου και να έχουν πρόσβαση στην τράπεζα πληροφοριών του συλλόγου καθώς και σε πληροφορίες σχετικά με τη δράση και τις αποφάσεις του.

Ως απόρροια όλων των παραπάνω, ο Σύλλογος αναγνωρίζει την ανάγκη για τη δημιουργία δύο χιλιάδων πιστοποιητικών ψηφιακών πιστοποιητικών για τα μέλη του με

σκοπό την αυθεντικοποίηση των χρηστών και των δοσοληψιών μεταξύ τους. Ο Πανελλήνιος Σύλλογος, που διαχειρίζεται τις πληροφορίες όλων των τοπικών συλλόγων, αποφασίζει να αναθέσει ολόκληρη τη διαδικασία της δημιουργίας και εγκατάστασης των πιστοποιητικών σε εταιρία που ειδικεύεται στον τομέα. Η χρήση των πιστοποιητικών αφορά τη διαδικασία εισόδου στο σύστημα, την υπογραφή και κρυπτογράφηση ηλεκτρονικού ταχυδρομείου και τον έλεγχο προσπέλασης. Είναι σημαντική η διασφάλιση της μυστικότητας των προσωπικών δεδομένων των μελών τους, καθώς και η μη αποκάλυψη των δεδομένων του συλλόγου σε τρίτους μέσω της διαδικασίας πιστοποίησης της ταυτότητας των χρηστών. Αυτό που επιθυμείται να αποφευχθεί είναι η πλαστογράφηση διευθύνσεων δικτύου, η μη εξουσιοδοτημένη τροποποίηση πληροφοριών, η άρνηση παραλαβής ή αποστολής πληροφοριών, απειλές λόγω πλαστοπροσωπίας και υποκλοπή συνθηματικών. Ορισμένα μέλη (πρόεδροι τοπικών συλλόγων, υπεύθυνοι για τα πιστοποιητικά), θα έχουν περισσότερα δικαιώματα πρόσβασης. Ο ιατρικός σύλλογος δεν απασχολεί άτομα σχετικά με τον τομέα της πληροφορικής και της ασφάλειας. Απασχολεί, όμως, άτομα ικανά ως προς τη σύναψη μιας συμφωνίας και τη διαχείριση μιας σχέση με κάποια άλλη εταιρία από τα οποία λείπει το τεχνικό υπόβαθρο.

5.2 Διαδικασία επιλογής υπηρεσιών ασφάλειας outsourcing

Βάσει των παραπάνω χαρακτηριστικών και αναγκών ακολουθεί η διαδικασίας επιλογής των μερών της τεχνολογίας υποδομής δημοσίου κλειδιού-ΥΔΚ (Public Key Infrastructure-PKI) που θα ανατεθεί στον εξωτερικό συνεργάτη.

Αρχικά καθορίζεται ο τύπος πιστοποιητικών ως πιστοποιητικά πελάτη (Client SSL certificates) τα οποία μπορούν να χρησιμοποιηθούν και για την υπογραφή και κρυπτογράφηση μηνυμάτων ηλεκτρονικού ταχυδρομείου. Όσον αφορά στο είδος της πληροφορίας που θα παρέχουν, θα είναι πιστοποιητικά ταυτότητας, δηλαδή, θα ταυτοποιούν μια οντότητα, αλλά και πιστοποιητικά χαρακτηριστικών, τα οποία θα περιγράφουν τις ιδιότητες μιας οντότητας (δικαιώματα προσπέλασης, συμμετοχή της σε μια ομάδα χρηστών) [41].

Πολιτική ασφάλειας: Η πολιτική ασφάλειας, που θα ορίζει τις αρχές που πρέπει να ακολουθούνται για την ασφάλεια των πληροφοριών και τα διάφορα επίπεδα ελέγχου ανάλογα με το επίπεδο ευαισθησίας της κάθε πληροφορίας, θα πρέπει να γίνει σε συνεργασία με τον σύλλογο. Ο προμηθευτής των πιστοποιητικών δεν μπορεί να γνωρίζει τον τρόπο λειτουργίας του συλλόγου, αλλά ούτε και το επίπεδο πρόσβασης κάθε μέλους του. Από την άλλη, οι κανόνες για τη χρήση της κρυπτογραφίας και η διαδικασία δημιουργίας, κατοχύρωσης και πιστοποίησης των κλειδιών θα ανατεθούν σε εξωτερικό συνεργάτη [41]. Συγκεκριμένα ο πάροχος θα είναι υπεύθυνος για τις εξής λειτουργίες:

1. Δημιουργία ζεύγους κλειδιών,
2. Αντιστοίχηση του ζεύγους κλειδιών με την αιτούσα οντότητα,
3. Διανομή κλειδιών,
4. Αποθήκευση κλειδιού,
5. Ανάκτηση κλειδιού,
6. Ανάκαμψη κλειδιού σε περίπτωση απώλειας ή διακύβευσης της ασφάλειας του,
7. Τήρηση αρχείου αντιγράφου κλειδιών,
8. Ενημέρωση κλειδιού,
9. Έλεγχος αιτήσεων για διαδικασίες που αφορούν την πρόσβαση στα κλειδιά και
10. Καθορισμός δικαιωμάτων πρόσβασης του προσωπικού σε διαδικασίες διαχείρισης κλειδιών

Αρχή πιστοποίησης (Certification Authority-CA): Το βασικό μέρος της υποδομής δημοσίου κλειδιού, δηλαδή η αρχή πιστοποίησης, θα δοθεί και αυτό για outsourcing. Αυτό περιλαμβάνει [40], [41]:

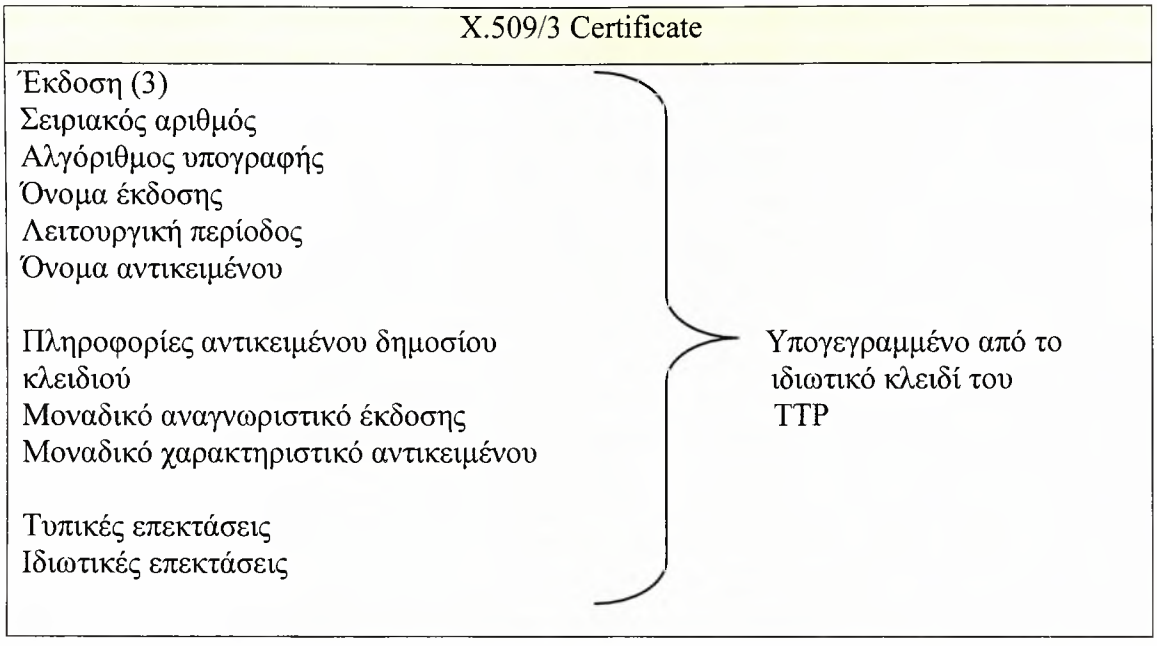
1. Τη δημιουργία πιστοποιητικών που συνδέουν την ταυτότητα ενός χρήστη με ένα δημόσιο κλειδί με τη βοήθεια των ψηφιακών υπογραφών.
2. Το προγραμματισμό της δημιουργίας λήξης των πιστοποιητικών.
3. Την αποθήκευση και την ανάκτηση του πιστοποιητικού.
4. Τη διασφάλιση για την ανάκληση των πιστοποιητικών όταν είναι απαραίτητο με τη δημοσίευση των λιστών ανάκλησης πιστοποιητικών (Certification Revocation Lists- CRLs).

5. Τη δημοσίευση πιστοποιητικού.
6. Την αρχειοθέτηση πιστοποιητικού.
7. Την επικοινωνία με άλλες εταιρίες Παροχής Υπηρεσιών Πιστοποίησης (Certificate Service Provider-CPS).

Η εταιρία-πάροχος θα δημιουργήσει την Αρχή Πιστοποίησης του Πανελλήνιου Ιατρικού Συλλόγου που θα διαχειρίζεται τα πιστοποιητικά του Συλλόγου. Ο πάροχος θα υπογράφει με το δικό του κλειδί το πιστοποιητικό της Αρχής Πιστοποίησης του Πανελλήνιου Ιατρικού Συλλόγου και, με τη σειρά της, η Αρχή Πιστοποίησης του Πανελλήνιου Ιατρικού Συλλόγου θα υπογράφει με το δικό της κλειδί τα πιστοποιητικά του Συλλόγου.

Η απόφαση του συλλόγου είναι να χρησιμοποιήσει τις υπηρεσίες μιας ήδη υπάρχουσας εμπορικής αρχής πιστοποίησης, κάποιου αναγνωρισμένου Παρόχου Υπηρεσιών Πιστοποίησης.

Η δημιουργία των πιστοποιητικών θα βασίζεται στο πρότυπο X.509, και πιο συγκεκριμένα την τρίτη έκδοση, και θα περιλαμβάνει [40]:



Πίνακας 7: Δομή Πιστοποιητικού

Αρχή Καταχώρησης (Registration Authority-RA): Το ρόλο του μεσολαβητή μεταξύ χρήστη και CA θα κρατήσει ο ίδιος ο σύλλογος και συγκεκριμένα, οι επιμέρους τοπικοί σύλλογοι. Για παράδειγμα, ο Ιατρικός Σύλλογος Θεσσαλονίκης θα είναι υπεύθυνος για την πιστοποίηση της ταυτότητας του χρήστη και θα μεταφέρει στο πανελλήνιο σύλλογο, έτοιμες, όλες τις αιτήσεις για τη δημιουργία πιστοποιητικών, ο οποίος με τη σειρά του θα τις μεταφέρει στην CA. Η διαδικασία της σύνδεσης ενός χρήστη με ένα πιστοποιητικό καθορίζει και το επίπεδο εμπιστοσύνης που παρέχεται από τα πιστοποιητικά. Ο μόνος υπεύθυνος για αυτό είναι ο ίδιος ο φορέας, αφού ο ίδιος αποφασίζει τα κριτήρια σύμφωνα με τα οποία κάποιος μπορεί να γίνει μέλος του συλλόγου και τα αποδεικτικά που χρειάζονται για αυτήν τη διαδικασία.

Σύστημα διανομής πιστοποιητικών: Μετά τη δημιουργία των πιστοποιητικών η CA είναι υπεύθυνη να παραδώσει τα πιστοποιητικά στον φορέα και αυτός με τη σειρά του να τα διανείμει στις επιμέρους RAs (τοπικοί σύλλογοι). Στη συνέχεια οι RAs είναι υπεύθυνες για τη διανομή των πιστοποιητικών στα μέλη των συλλόγων. Η διανομή θα γίνει μέσω ηλεκτρονικού ταχυδρομείου. Το μήνυμα θα περιέχει μια URL διεύθυνση όπου βρίσκεται το πιστοποιητικό, από όπου ο χρήστης μπορεί να το αποθηκεύσει στον τοπικό

του δίσκο. Εναλλακτικά, και για περιπτώσεις πιστοποιητικών υψηλού βαθμού εμπιστοσύνης, ο χρήστης θα μπορεί να παραλάβει το πιστοποιητικό του από τους επιμέρους συλλόγους, με χρήση κάποιου αποθηκευτικού μέσου [40].

Εφαρμογές της ΥΔΚ:

1. Ηλεκτρονικό ταχυδρομείο
2. Επικοινωνία μεταξύ Web Servers και Browsers

5.3 Διαδικασία επιλογής παρόχου

Κατά την αναζήτηση του παρόχου λαμβάνονται υπ'όψιν χαρακτηριστικά και ιδιότητες των εταιριών παροχής πιστοποίησης που αφορούν διάφορους τομείς.

Φήμη και εμπειρία: Το πιο σημαντικό ρόλο παίζει η φήμη και η εμπειρία της εταιρίας. Υπερέχουν πάροχοι με παράδοση στην έκδοση ψηφιακών πιστοποιητικών, με ήδη καταγεγραμμένες επιτυχίες και ισχυρούς οργανωτικούς πόρους. Για την εξακρίβωση των παραπάνω, θα μπορούσαν να γίνουν ερωτήσεις σε πελάτες που έχουν ήδη αναθέσει τη διαδικασία έκδοσης πιστοποιητικών στον εκάστοτε πάροχο και να καταγράφουν οι εμπειρίες και οι εντυπώσεις τους. Οι ερωτήσεις μπορεί να αφορούν το αν χρησιμοποιούν ακόμα τις υπηρεσίες του συγκεκριμένου παρόχου, γιατί επέλεξαν τον συγκεκριμένο πάροχο, αν υπήρξαν προβλήματα σε ολόκληρη τη διαδικασία και πως τα αντιμετώπισε ο πάροχος, πόσο καιρό κράτησε η διαδικασία δημιουργίας και εγκατάστασης των πιστοποιητικών και, τέλος, αν είναι ευχαριστημένοι από τη συνολική διαδικασία.

Οικονομική σταθερότητα: Στη φήμη και την εμπειρία, προστίθεται η οικονομική σταθερότητα της εταιρίας, καθώς αποτελεί ένδειξη της ικανότητας της να διατηρεί και να βελτιώνει τα συστήματα και το προσωπικό της, ώστε να μπορεί να υποστηρίζει τους πελάτες της.

Ενημέρωση (ενημερότητα): Δεύτερος βασικός παράγοντας, είναι η ικανότητα κάθε εταιρίας να μένει συνεχώς ενημερωμένη για τις τελευταίες εξελίξεις στον τομέα των

ψηφιακών πιστοποιητικών και σε παρεμφερή με αυτόν θέματα. Επίσης, σημαντικό θεωρείται το να έχει συμμετάσχει η εταιρία σε συνέδρια και να έχει καινοτομίες καταγεγραμμένες στο όνομα της.

Κόστος: Το κόστος των ψηφιακών πιστοποιητικών απασχολεί πολύ το συγκεκριμένο φορέα. Η ανάγκη για εξοικονόμηση χρημάτων είναι μεγάλη, αλλά μεγαλύτερη είναι η ανάγκη για λήψη υπηρεσιών υψηλής ποιότητας. Δίνεται περισσότερη βαρύτητα στην διατήρηση ενός υψηλού επιπέδου ασφάλειας από ότι στη μείωση του κόστους. Επιπλέον, εξετάζεται και η περίπτωση της αύξησης του κόστους για πιθανή μελλοντική αύξηση του αριθμού των πιστοποιητικών ή των υπηρεσιών που λαμβάνονται.

Χρόνος απόκρισης: Λόγω της ανάγκης για γρήγορη εγκατάσταση των πιστοποιητικών θα επιλεγούν εταιρίες που μπορούν να παραδώσουν τα πιστοποιητικά σε μικρό χρονικό διάστημα και των οποίων η εγκατάσταση διαρκεί λίγο. Επίσης, εξετάζεται η δυνατότητα απόκρισης (σε χρονικούς όρους) του προμηθευτή σε περίπτωση αύξησης του αριθμού των πιστοποιητικών από τον ιατρικό σύλλογο ή και σε περιπτώσεις ανάγκης για ανάκληση πιστοποιητικών.

Χρήση αναφορών: Ένα από τα χαρακτηριστικά που είναι επιθυμητό, είναι οι λεπτομερείς αναφορές, ώστε να είναι δυνατή η έκβαση συμπερασμάτων για την αποτελεσματικότητα των υπηρεσιών ψηφιακών πιστοποιητικών. Η συχνή ενημέρωση του φορέα μέσω είτε έντυπων είτε ηλεκτρονικών κειμένων για τις αλλαγές σε σχετικά θέματα κρίνεται απαραίτητη.

Διαθεσιμότητα: Εφόσον όλες οι πληροφορίες που αφορούν τα πιστοποιητικά αποθηκεύονται στην εταιρία παροχής τους, πολύ βασική είναι η ύπαρξη αντιγράφων ασφάλειας μέσα στην ίδια την εταιρία για την περίπτωση απώλειας τους, είτε λόγω φυσικής καταστροφής, είτε λόγω κάποιου χτυπήματος που πιθανόν δεχτεί. Έτσι, θα επιλεγούν εταιρίες που διαθέτουν τη δυνατότητα αυτή.

Πιστοποίηση: Έλεγχος θα διεξαχθεί για το κατά πόσο οι υποψήφιοι πάροχοι πληρούν κριτήρια κατά ISO. Επίσης, αναζητούνται ανεξάρτητοι και έμπιστοι οργανισμοί, που βρίσκονται υψηλότερα στην ιεραρχία της διαδικασίας πιστοποίησης, οι οποίοι επικυρώνουν τις διαδικασίες που χρησιμοποιούνται από τον εκάστοτε πάροχο.

Στρατηγική: Αναζητούνται εταιρίες με καλά ορισμένες στρατηγικές και τεχνικές ανάκαμψης, για πιθανές μελλοντικές καταστάσεις, ώστε να είναι έτοιμες για την αντιμετώπιση οποιουδήποτε προβλήματος. Κρίνεται βασική η ικανότητα να μπορούν να απομονώνουν και να αποτιμούν τη ζημιά, αλλά και να μπορούν να κινηθούν γρήγορα, ώστε να αποκαταστήσουν πιθανές δυσλειτουργίες.

Προσωπικό: Σημαντικό κριτήριο είναι η στελέχωση της εταιρίας. Η ανάθεση μέρους της ασφάλειας του φορέα, προϋποθέτει την ύπαρξη ικανού και πλήρως καταρτισμένου προσωπικού. Για την εξακρίβωση αυτού θα μπορούσαν να ζητηθούν από κάθε εταιρία το επίπεδο εκπαίδευσης των υπαλλήλων της και ο χρόνος προϋπηρεσίας.

Αντικρουόμενα συμφέροντα: Ο πάροχος που θα επιλεγεί δεν πρέπει να έχει συγκρουόμενα συμφέροντα. Οι υπηρεσίες του πρέπει να είναι πολύ συγκεκριμένες και καλά ορισμένες, ώστε να μπορεί να έχει μεγαλύτερο βαθμό εξειδίκευσης σε αυτές. Η προσφορά πολλών υπηρεσιών ταυτόχρονα μπορεί να οδηγήσει τον πάροχο σε διλλήματα με συνέπεια τη δράση του σύμφωνα με το συμφέρον του.

Τεχνικές αποθήκευσης και ανάκτησης: Κριτήριο στην επιλογή του CSP αποτελεί η ικανότητα του να αποθηκεύει με ασφαλείς τρόπους τα πιστοποιητικά που έχει δημιουργήσει, με σκοπό να χρησιμοποιήσει την πληροφορία αυτή σε περιπτώσεις που ζητηθεί από τα μέλη της PKI ή σε περιπτώσεις προβλημάτων. Συγκεκριμένα, θα προτιμηθούν πάροχοι που διατηρούσαν δύο αντίγραφα της λίστας των πιστοποιητικών.

Τεχνικές ανάκλησης: Ο CSP πρέπει να έχει ανεπτυγμένες τεχνικές ανάκλησης, με τη δημιουργία και συχνή ανανέωση των Λιστών Ανακληθέντων Πιστοποιητικών (Certificate Revocation List-CRL). Οποιαδήποτε αλλαγή σε ένα πιστοποιητικό πρέπει να

αποθηκεύεται και όλοι οι χρήστες της PKI πρέπει να ενημερώνονται άμεσα. Σημαντική είναι η εξασφάλιση της έγκαιρης ενημέρωσης για τη λήξη κάποιου πιστοποιητικού.

Πιο συγκεκριμένα, από την εταιρία-πάροχο απαιτείται [40]:

- Πρόληψη, προστασία ή αποφυγή σφαλμάτων. Σφάλμα μπορεί να θεωρηθεί ένα μήνυμα που έχει υποστεί κρυφάκουσμα, παρεμπόδιση, τροποποίηση, αλλοίωση ή αποτυχία.
- Ανίχνευση σφαλμάτων τα οποία θα μπορούσαν να εγείρουν αμφισβητήσεις.
- Πραγματική διόρθωση σφαλμάτων.
- Πρόληψη, προστασία ή αποφυγή αμφισβητήσεων στο βαθμό που είναι επιτεύξιμο.
- Αποτελεσματική και αξιόπιστη επίλυση αμφισβητήσεων, στην περίπτωση που αυτές δεν είναι δυνατόν να προληφθούν. Δηλαδή ζητείται από την TTP να μπορεί να παρέχει στοιχεία για την επίλυση αμφισβητήσεων στα πλαίσια κάθε δοσοληψίας.
- Αποζημιώσεις σε περιπτώσεις καταστροφών, απωλειών ευκαιριών και απωλειών επιχειρηματικών δραστηριοτήτων.
- Μηχανισμοί διασφάλισης επιδόσεων σε αμφισβητούμενες δοσοληψίες μετά την επίλυση τους.
- Παρακολούθηση των χρηστών και των παρεχόμενων υπηρεσιών στην κατεύθυνση της λήψης ανάδρασης για τη βελτίωση του επιπέδου παροχής υπηρεσιών ασφάλειας και τη βελτίωση, γενικότερα, της ποιότητας των υπηρεσιών ασφάλειας και του επιπέδου εμπιστοσύνης που παρέχεται προς τους χρήστες.

ΣΥΜΦΩΝΗΤΙΚΟ ΔΙΑΧΕΙΡΙΣΗΣ ΥΠΗΡΕΣΙΩΝ

ΗΜΕΡΟΜΗΝΙΑ
Η παρούσα σύμβαση συνήφθη στις 01/10/2006

ΜΕΤΑΞΥ ΤΩΝ:
Της εταιρίας ABC της οποίας η έδρα βρίσκεται στην Αθήνα.

ΚΑΙ
Του Πανελλήνιου Ιατρικού Συλλόγου του οποίου η έδρα βρίσκεται στην Αθήνα (καλούμενου εφεξής «ο Πελάτης»)

ΕΠΕΙΔΗ
- Η Εταιρία ABC διαθέτει την εμπειρία και ασχολείται με την παροχή υπηρεσιών Ψηφιακών Πιστοποιητικών σε τρίτα μέρη πελάτες.
- Ο Πελάτης επιθυμεί η ABC να διαχειρίζεται και να διεκπεραιώνει λειτουργίες σχετικές με την έκδοση Ψηφιακών Πιστοποιητικών, όπως αυτές εξειδικεύονται λεπτομερώς στο παρόν και η ABC προτίθεται να παράσχει αυτές τις υπηρεσίες υπό τους όρους και τις συνθήκες του παρόντος Συμφωνητικού.

ΤΑ ΜΕΡΗ ΔΙΑ ΤΟΥ ΠΑΡΟΝΤΟΣ ΣΥΜΦΩΝΟΥΝ ΤΑ ΚΑΤΩΤΕΡΩ

1. ΔΙΑΡΚΕΙΑ
Οι υπηρεσίες θα ξεκινήσουν κατά την ημερομηνία έναρξης παροχής υπηρεσιών και υπό την αίρεση των διατάξεων περί πρόωρης λύσεως, όπως αυτές περιγράφονται στον όρο 10, θα παρέχονται για μια περίοδο ενός χρόνου πέρα από την οποία θα εξακολουθήσουν να παρέχονται, εκτός ή ώσπου να τερματιστούν κατόπιν εγγράφου καταγγελίας οποιουδήποτε των μερών, η οποία πρέπει να τάσσει προθεσμία δύο μηνών για τη λύση και που σε κάθε περίπτωση δεν μπορεί να γίνει πριν περάσει η αρχική περίοδος του ενός χρόνου (Η Διάρκεια) .

2. ΟΙ ΥΠΗΡΕΣΙΕΣ
- Υπό τους όρους του παρόντος Συμφωνητικού και υπό την προϋπόθεση πληρωμής της αμοιβής, η Εταιρία ABC συμφωνεί να παρέχει προς τον Πελάτη τις υπηρεσίες Ψηφιακών Πιστοποιητικών με αφετηρία την ημερομηνία έναρξης παροχής υπηρεσιών.
- Η Εταιρία ABC δεν θα είναι υπεύθυνη για την παροχή υπηρεσιών που δεν περιγράφονται λεπτομερώς στο Παράρτημα Α. Στη δε περίπτωση κατά την οποία ο Πελάτης επιθυμεί να αναθεωρήσει τις υπηρεσίες, τότε θα εφαρμοσθούν οι όροι της παραγράφου 8 .

- Ο όρος της επαναθέσεως σε λειτουργία κατόπιν καταστροφής δεν αποτελεί τμήμα του παρόντος Συμφωνητικού, αλλά μπορεί να αποτελέσει αντικείμενο ξεχωριστού Συμφωνητικού.

3. ΑΜΟΙΒΗ

- Υπό την προϋπόθεση της παροχής των υπηρεσιών στα επίπεδα που περιγράφονται στο Παράρτημα Α και σε σχέση με το παρόν Συμφωνητικό, ο Πελάτης οφείλει να καταβάλει στην Εταιρία ΑΒC όσον αφορά την αρχική καθορισμένη περίοδο του ενός χρόνου το ποσό των ..... σύμφωνα με τους όρους του Παραρτήματος Β (Η Βασική Χρέωση), το οποίο υπόκειται σε τροποποίηση και σε πρόσθετες χρεώσεις όπως αυτές καθορίζονται κατωτέρω.
- Η πληρωμή της Βασικής Χρέωσης θα πραγματοποιείται μέσω μηνιαίων πάγιων τραπεζικών εντολών, για την μηνιαία αμοιβή (όπως καθορίζεται στο Παράρτημα Β).
- Η Εταιρεία ΑΒC διατηρεί το δικαίωμα να αυξήσει τις τιμές υπό τις κάτωθι προϋποθέσεις :

  - ✓ Με τουλάχιστον προ τριάντα ημερών έγγραφη ειδοποίηση προς τον Πελάτη και με αφετηρία την εκάστοτε επέτειο της ημερομηνίας Έναρξης Παροχής Υπηρεσιών, σε ποσοστό όχι, υπό φυσιολογικές συνθήκες, μεγαλύτερο από το ποσοστό αύξησης μεταξύ τ..... που δημοσιεύτηκε τελευταία πριν από την εκάστοτε επέτειο.
  - ✓ Στην περίπτωση κατά την οποία οι υπηρεσίες (ή μέρος αυτών) εκτελούνται από κάποιο άλλο μέρος πλην των υπαλλήλων της Εταιρίας ΑΒC και ο προμηθευτής αυξήσει τις χρεώσεις του προς την Εταιρία ΑΒC για τις υπηρεσίες ή μέρος αυτών.

  Κάθε αμοιβή καθώς και οποιοδήποτε άλλο σχετιζόμενο με το παρόν ποσό οφειλόμενο προς τα Εταιρία ΑΒC είναι καταβλητέο το αργότερο σε 28 ημέρες από την ημερομηνία έκδοσης του μηνιαίου τιμολογίου εκτός αν ορίζεται διαφορετικά στο παρόν Συμφωνητικό. Κάθε αμοιβή αδείας η οποία χρεώνεται δυνάμει του παρόντος είναι πληρωτέα το αργότερο σε 28 ημέρες από την ημερομηνία του τιμολογίου.

  Όλες οι ανωτέρω τιμές και χρεώσεις, καθώς και οποιαδήποτε άλλα ποσά οφείλονται σε οποιοδήποτε των μερών δυνάμει του παρόντος δεν περιλαμβάνουν τον Φ.Π.Α., ο οποίος θα χρεώνεται επιπλέον με βάση τα ισχύοντα ποσοστά κατά το χρόνο χρέωσης της παροχής.

- Αν η Εταιρία ΑΒC κληθεί από τον Πελάτη να προμηθεύσει προϊόντα ή υπηρεσίες πλέον των παρασχεθησών υπηρεσιών τότε, σύμφωνα με τους όρους της παραγράφου 8, θα δικαιούται να χρεώσει τον Πελάτη για τα ανωτέρω προϊόντα και τιμές με βάση τα ισχύοντα ποσοστά τιμών τιμοκαταλόγου, χρόνου και υλικών και με ξεχωριστούς όρους και συνθήκες οι

οποίες θα θεωρηθούν κατάλληλες και να προσθέσει το ποσό των εν λόγω χρεώσεων στις χρεώσεις που γίνονται δυνάμει του παρόντος. Αν πρόσθετα προϊόντα ή υπηρεσίες απαιτηθούν σε φυσιολογικό βαθμό ως αποτέλεσμα συνθηκών για τις οποίες η Εταιρία ΑΒC δεν μπορεί να θεωρηθεί υπεύθυνη, τότε η Εταιρία ΑΒC προτού επιβάλλει τις αντίστοιχες χρεώσεις θα ενημερώνει τον Πελάτη παίρνοντας την έγγραφη συναίνεση του και υπό τον όρο πάντοτε ότι η Εταιρία ΑΒC δεν θα έχει καμιά ευθύνη από οποιοδήποτε αντίθετο αποτέλεσμα προκληθεί στις παρεχόμενες υπηρεσίες εξαιτίας της αρνήσεως του Πελάτη προς τα ανωτέρω.

- Στην περίπτωση κατά την οποία ο Πελάτης επιθυμεί την παροχή υπηρεσιών (ή μέρους αυτών) πριν από την συμφωνημένη ημερομηνία έναρξης αυτών, τότε θα ειδοποιήσει εγγράφως την Εταιρία ΑΒC, τουλάχιστον επτά ημέρες πριν από την επιθυμητή ημερομηνία και θα καταβάλει μια επιπλέον αμοιβή ως προκαταβολή για την περίοδο παροχής αυτών των υπηρεσιών με βάση τα όσα θα συμφωνηθούν πριν την έναρξη της παροχής μεταξύ των μερών.
- Η Εταιρία ΑΒC μπορεί να χρεώσει κατά καιρούς ετήσιο τόκο υπερημερίας σε ποσοστό 2.5 % πέραν του ισχύοντος τραπεζικού τόκου για κάθε ανεξόφλητη πληρωμή, ο οποίος θα υπολογίζεται από την ημερομηνία λήξης της προθεσμίας καταβολής και θα περιλαμβάνει όλα τα έξοδα συμπεριλαμβανομένων των δικαστικών καθώς και των εξόδων εκτέλεσης.

4. ΕΚΤΕΛΕΣΗ ΥΠΗΡΕΣΙΩΝ

Η Εταιρία ΑΒC θα παρέχει τις καθοριζόμενες στο Παράρτημα Α Υπηρεσίες με τις δέουσες ικανότητες, επιμέλεια και προσοχή και σε σχέση με τα επίπεδα απόδοσης τα οποία καθορίζονται στο Συμφωνηθέν Επίπεδο Παρεχομένων Υπηρεσιών το οποίο περιγράφεται στο Παράρτημα Α Εξυπακούεται ότι τυχόν διαφοροποιήσεις από πρόσωπα που δεν ανήκουν στο εξουσιοδοτημένο προσωπικό της Εταιρίας ΑΒC ή σε προστηθέντες της και οι οποίες επηρεάζουν τις παρεχόμενες υπηρεσίες, θα αγνοούνται.

Προγραμματισμένες διακοπές κατά τη διάρκεια του χρόνου παροχής των υπηρεσιών θα ισχύουν μόνο κατόπιν εγγράφου συμφωνίας με τον Πελάτη. Αυτές οι διακοπές θα προγραμματίζονται μόνο όταν κατά τη γνώμη της Εταιρίας ΑΒC κριθούν απαραίτητες για τη διατήρηση ή τη βελτίωση των υπηρεσιών και μόνο όπου κριθούν ότι θα έχουν την ελάχιστη επίδραση στις υπηρεσίες.

5. ΔΙΚΑΙΩΜΑΤΑ ΠΡΟΣΒΑΣΗΣ

Υπό τον όρο της έγκαιρης προηγούμενης ειδοποίησης, η Εταιρία ΑΒC θα παρέχει πρόσβαση σε εξουσιοδοτημένο προσωπικό του Πελάτη ή σε εξουσιοδοτημένα τρίτα μέρη, στο δωμάτιο μηχανικού περιβάλλοντος στις εγκαταστάσεις του κέντρου δεδομένων της, με σκοπό τον έλεγχο της λειτουργίας και διατήρησης του περιβάλλοντος, σύμφωνα με τους όρους του παρόντος Συμφωνητικού αλλά και τις οδηγίες κατασκευαστή κάθε αντίστοιχου συστήματος.

Πρόσβαση στο σύστημα ή τα δεδομένα του Πελάτη θα απαγορεύεται σε υπαλλήλους και προστηθέντες της Εταιρίας ΑΒC ή σε τρίτους,

Πρόσβαση στο μηχανικό περιβάλλον του Πελάτη θα απαγορεύεται σε επαγγελματικό προσωπικό της Εταιρία ΑΒC ή τους προστηθέντες αυτού, οι οποίοι επιτελούν έργο για λογαριασμό του Πελάτη.

Στις περιπτώσεις όπου οι υπάλληλοι και προστηθέντες του Πελάτη έχουν πρόσβαση στις εγκαταστάσεις κέντρου δεδομένων της Εταιρίας ΑΒC και/ή στο σύστημα της Εταιρίας ΑΒC, ο Πελάτης θα αποζημιώνει την Εταιρία ΑΒC για κάθε προκληθείσα ζημιά, η οποία είναι αποτέλεσμα πράξης, παραλείψεως ή σφάλματος των υπαλλήλων και προστηθέντων του Πελάτη.

Στις περιπτώσεις που σε κάποιον εκ των συμβαλλομένων επιτραπεί η πρόσβαση στους χώρους εργασίας του αντισυμβαλλόμενου, οι υπάλληλοι και οι προστήθεντες του εκάστοτε συμβαλλόμενου υποχρεούνται να συμμορφώνονται με τις οδηγίες και τις σύννομες εντολές που θα προέρχονται από εξουσιοδοτημένο προσωπικό του αντισυμβαλλόμενου και να υπακούν σε όλες τους κείμενους κανονισμούς που αφορούν στη διεκπεραίωση των εργασιών ή στην συμπεριφορά του προσωπικού στους ανωτέρω χώρους.

Η Εταιρία ΑΒC θα καταβάλλει κάθε δυνατή προσπάθεια να διασφαλίσει την ασφαλή προστασία των δεδομένων έναντι πρόσβασης από μη εξουσιοδοτημένα πρόσωπα συμπεριλαμβανομένης της απόδοσης των κωδικών πρόσβασης που επιτρέπουν στο εξουσιοδοτημένο προσωπικό την απόκτηση πρόσβασης στο σύστημα.

Τα μέρη θα πρέπει να συμμορφώνονται εκατέρωθεν, με τις αντίστοιχες υποχρεώσεις τους, απορρέουσες από το Νόμο Προστασίας Δεδομένων του 1984 σε σχέση με τα δεδομένα.

6. ΥΠΑΛΛΗΛΟΙ

Τα μέρη αναγνωρίζουν ότι η Μεταβίβαση Κανονισμών Υποχρεώσεων (Προστασία Εργαζομένων) θα έχει εφαρμογή στη μεταφορά προσωπικού στην Εταιρία ΑΒC σύμφωνα με το παρόν Συμφωνητικό και υπό την προϋπόθεση ότι οι Υπάλληλοι θα θεωρούνται ως τέτοιοι της Εταιρίας ΑΒC με αφετηρία την Ημερομηνία Έναρξης Παροχής των Υπηρεσιών υπό τους όρους και τις συνθήκες που είναι τουλάχιστον, στο σύνολο τους, τόσο ικανοποιητικές όσο αυτές που απολαμβάνουν κατά τη συγκεκριμένη χρονική στιγμή από τον Πελάτη (με την εξαίρεση των παροχών που αφορούν στην συνταξιοδότηση) και οι οποίες αναγνωρίζουν στους υπαλλήλους το δικαίωμα συνεχούς απασχόλησης στην Εταιρία ΑΒC για την ίδια χρονική περίοδο που απασχολούντο στον Πελάτη. Στην περίπτωση που οι υπάλληλοι (ή κάποιοι από αυτούς) αρνηθούν να δεχθούν τις ανωτέρω Συμβάσεις Εργασίας με την Εταιρία ΑΒC από την Ημερομηνία Έναρξης Παροχής των Υπηρεσιών, η Εταιρία ΑΒC θα δικαιούται να τερματίσει το παρόν

Συμφωνητικό σύμφωνα με τα οριζόμενα στον όρο 10.

Ο Πελάτης αναλαμβάνει την υποχρέωση να αποζημιώσει και να προστατεύσει την Εταιρία ABC από και έναντι κάθε απαιτήσεως ή αξιώσεως από οποιονδήποτε υπάλληλο σε σχέση με απαλλαγή καθηκόντων λόγω υπεράριθμου θέσεων εργασίας, άδικη ή λανθασμένη απόλυση, σεξουαλική ή φυλετική διάκριση ή άλλης οι οποίες προέκυψαν πριν από την Ημερομηνία Έναρξης Παροχής Υπηρεσιών.

Η Εταιρία ABC αναλαμβάνει την υποχρέωση να αποζημιώνει και να προστατεύει τον Πελάτη από και έναντι κάθε ζημιάς, δαπάνης, ευθύνης και εξόδων προκυπτουσών σε σχέση και ως αποτέλεσμα κάθε ευθύνης ή υποχρέωσης της Εταιρίας ABC σε οποιονδήποτε υπάλληλο σε σχέση με την εργασία τους μετά την Ημερομηνία Έναρξης Παροχής των Υπηρεσιών.

Ο Πελάτης θα πληρώνει στους υπαλλήλους όλες τις παροχές που καταγράφονται κατά την Ημερομηνία Έναρξης Παροχής των Υπηρεσιών συμπεριλαμβανομένων όλων των επιδομάτων, προκαθορισμένων ή μη, αλλά υπό την εξαίρεση απορρεόντων δικαιωμάτων διακοπών και επιδομάτων αδείας, των οποίων όμως πλήρη στοιχεία θα έχουν δοθεί στην Εταιρία ABC πριν από την Ημερομηνία Έναρξης Παροχής των Υπηρεσιών.

Ο παρόν όρος αντιπροσωπεύει το σύνολο των υποχρεώσεων των μερών σε σχέση με τους υπαλλήλους και συγκεκριμένα, αλλά χωρίς όριο, η Εταιρία ABC δεν θα έχει καμιά ευθύνη έναντι του Πελάτη για ή σε σχέση με οποιοδήποτε προσωπικό απασχολούμενο από τον Πελάτη το οποίο δεν είναι υπάλληλοι και ο Πελάτης θα αποζημιώνει την Εταιρία ABC για κάθε αξίωση ή απαίτηση από οποιουδήποτε μέρος του προσωπικού ενάντια στην Εταιρία ABC σε σχέση με την εργασία τους στον Πελάτη ή την παύση αυτής.

7. ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Κάθε μέρος αναλαμβάνει την υποχρέωση:

- Κατά τη διάρκεια του παρόντος να χρησιμοποιεί το ίδιο επίπεδο προστασίας ώστε να αποτρέπει την αποκάλυψη πληροφοριών που αφορούν στη εργασία και τις υποθέσεις έκαστου των μερών ή πελατών αυτών η οποία θα έχει αποκτηθεί ή ληφθεί κατά τη διάρκεια παροχής των υπηρεσιών (η πληροφορία) και θα προστατεύεται με τον ίδιο τρόπο προστασίας μιας όμοιας πληροφορίας εκτός εάν:
  - ✓ η πληροφορία ήταν ήδη με νόμιμο τρόπο γνωστή ή κατέστη μ' αυτό τον τρόπο γνωστή στο άλλο μέρος εντελώς ανεξάρτητα από την ανάμειξη τους στο συμφωνητικό.
  - ✓ Η πληροφορία δημοσιοποιηθεί ανεξάρτητα από την λανθασμένη χρήση ή αποκάλυψη της από το άλλο μέρος.
  - ✓ Η αποκάλυψη ή χρήση της είναι απαραίτητη για την καλή εκτέλεση

και/ή τη νόμιμη άσκηση των δικαιωμάτων του άλλου μέρους σύμφωνα με το παρόν συμφωνητικό.

- ✓ Η πληροφορία δημιουργήθηκε από το άλλο μέρος ανεξάρτητα χωρίς να σχετίζεται με την παροχή των υπηρεσιών.

- Να χρησιμοποιεί την πληροφορία αποκλειστικά σε σχέση με την εφαρμογή του παρόντος και όχι προς ίδιον όφελος έκαστου των μερών ή προς όφελος τρίτου μέρους.

8. ΑΛΛΑΓΕΣ ΣΤΙΣ ΑΠΑΙΤΗΣΕΙΣ ΤΩΝ ΠΑΡΕΧΟΜΕΝΩΝ ΥΠΗΡΕΣΙΩΝ

Στη περίπτωση κατά την οποία ο πελάτης επιθυμεί να διαφοροποιήσει τις υπηρεσίες καθ' οποιονδήποτε τρόπο (οι τροποποιηθείσες υπηρεσίες) τότε θα κάνει ανάλογη έγγραφη πρόταση στην Εταιρία ΑΒC.

Η Εταιρία ΑΒC δεν θα έχει καμιά υποχρέωση να αποδεχθεί ή να εφαρμόσει τις ανωτέρω τροποποιηθείσες υπηρεσίες και διατηρεί το δικαίωμα να αυξήσει την αμοιβή της ως όρο αποδοχής ή εφαρμογής αυτών.

Η Εταιρία ΑΒC θα έχει για μία περίοδο οχτώ ημερών από την παραλαβή της ανωτέρω εγγράφου προτάσεως μία αποκλειστική επιλογή καθορισμού της παροχής των τροποποιηθεισών υπηρεσιών.

Στη περίπτωση κατά την οποία τα μέρη δεν συμφωνήσουν εγγράφως τους όρους με τους οποίους η Εταιρία ΑΒC θα παρέχει τις τροποποιηθείσες υπηρεσίες τότε ο πελάτης θα δικαιούται να τις αναθέσει σε ένα τρίτο μέρος υπό την προϋπόθεση ότι: η Εταιρία ΑΒC δεν θα έχει καμιά υποχρέωση να αποκαλύψει εμπιστευτικές πληροφορίες στο ανωτέρω τρίτο μέρος ή να επιτρέψει σ' αυτό να κάνει χρήση των περιουσιακών στοιχείων ή του συστήματος άλλη από αυτή που παρέχεται από την Εταιρία ΑΒC στον πελάτη για τη χρήση των υπηρεσιών και η Εταιρία ΑΒC δεν θα είναι υπεύθυνη για καμιά τροποποιηθείσα υπηρεσία εκτελεσθείσα από τρίτο μέρος ή από την επίδραση αυτής ή τη συμβατότητα αυτής με τις παρεχόμενες από την Εταιρία ΑΒC υπηρεσίες.

Σε περίπτωση οποιασδήποτε χειροτερεύσεως στις Υπηρεσίες ως αποτέλεσμα των Τροποποιημένων Υπηρεσιών, ο Πελάτης θα αποζημιώνει την Εταιρία ΑΒC για τις σχετικές συνέπειες και θα εξακολουθεί να είναι υπεύθυνος για την πληρωμή των Χρεώσεων και να εκπληρώνει τις λοιπές του υποχρεώσεις που απορρέουν από τη Σύμβαση.

9. ΑΝΑΦΟΡΑ ΚΑΙ ΣΥΜΒΟΥΛΕΣ

Τα μέρη θα έχουν τακτικές συναντήσεις ανά μήνα για να συζητούν τη λειτουργία και την παροχή των Υπηρεσιών. Για τις ανωτέρω συναντήσεις θα τηρούνται πρακτικά και αντίγραφα αυτών θα κυκλοφορούν μεταξύ αμφοτέρων των μερών.

Η Εταιρία ΑΒC θα παρέχει, διατηρεί και λειτουργεί κατάλληλες διαδικασίες για να μετρά τη διαθεσιμότητα, χρόνο ανταπόκρισης και ετήσια απόδοση.

10. ΛΗΞΗ (ΚΑΤΑΓΓΕΛΙΑ)

Η παρούσα Σύμβαση θα λήγει σε κάθε μια εκ των κατωτέρω περιπτώσεων:

- Εάν κάποιο από τα μέρη δώσει ειδοποίηση προς το άλλο εγγράφως ότι το δεχόμενο μέρος έχει προβεί σε ουσιαστική παράβαση των υποχρεώσεών του που απορρέουν από την παρούσα και το δεχόμενο μέρος αποτύχει να την επανορθώσει εντός 4 ημερών.
- Εάν κάποιο από τα μέρη δώσει ειδοποίηση προς το άλλο μέρος εγγράφως ως αποτέλεσμα του ότι το άλλο μέρος έχει πραγματοποιήσει συνάντηση με τους πιστωτές του ή αν γίνει πρόταση σχετικά με το άλλο μέρος για εκούσια διευθέτηση κατά το Τμήμα Ι της Πράξης περί Αφερεγγυότητας του 1986 ή αν γίνει πρόταση σχετικά με το άλλο μέρος για οποιαδήποτε άλλη σύνθεση, σχήμα ή διευθέτηση με τους πιστωτές (ή εκχώρηση προς όφελος αυτών) ή καταστεί αδύνατο να καταβάλει τα χρέη του κατά την έννοια του Τμήματος 123 της Πράξης περί Αφερεγγυότητας του 1986 ή αν θεματοφύλακας, διαχειριστής περιουσίας εν χρεοκοπία ή παρόμοιος αξιωματούχος διορισθεί σχετικά προς ή επί οιουδήποτε μέρους των επιχειρήσεων ή των περιουσιακών στοιχείων του άλλου μέρους ή αν μία αίτηση υποβληθεί ή μία συνάντηση πραγματοποιηθεί προς τον σκοπό λήψεως αποφάσεως ή άλλα μέτρα ληφθούν για τη λύση του άλλου μέρους ή για την έκδοση διαταγής διαχειρίσεως (για σκοπό άλλον από αυτόν της συγχωνεύσεως ή αναδιαρθρώσεως).
- Εάν ο Πελάτης δεν καταβάλει τις Χρεώσεις ή άλλα ποσά οφειλόμενα προς την Εταιρεία ABC ή προς κάποιο άλλο μέρος σύμφωνα με τους όρους της παρούσας Συμβάσεως, τα οποία ποσά παραμένουν ανεξόφλητα μετά την αντίστοιχη ημέρα καταβολής, η Εταιρία ABC θα δικαιούται να διακόψει τις Υπηρεσίες ή να καταγγείλει την παρούσα Σύμβαση ή το σχετικό μέρος των Υπηρεσιών χωρίς ευθύνη του με προηγούμενη έγγραφη ειδοποίηση προ 5 ημερών προς τον Πελάτη.
- Εάν η Εταιρία ABC για οποιοδήποτε λόγο, μειώσει το επίπεδο των, λαμβανομένων από τον Πελάτη, υπηρεσιών χωρίς προηγούμενη έγγραφη ειδοποίηση.

11. ΣΥΝΕΠΕΙΕΣ ΤΗΣ ΚΑΤΑΓΓΕΛΙΑΣ

Με τη λήξη ή την καταγγελία της παρούσας Συμβάσεως με οποιοδήποτε τρόπο αυτή προέλθει:

- Η Εταιρία ABC θα επιστρέψει στον Πελάτη μόλις του ζητηθεί όλα τα στοιχεία, έγγραφα ή δεδομένα που προέκυψαν ως αποτέλεσμα της παροχής των Υπηρεσιών.
- Με τη λήξη ή την καταγγελία της παρούσας Συμβάσεως, για οποιοδήποτε λόγο, όλες οι ανεξόφλητες Χρεώσεις και τα άλλα ποσά που οφείλονται στην Εταιρία ABC θα πρέπει να καταβληθούν αμέσως.
- Η Εταιρία ABC, με την έγγραφη ειδοποίηση του Πελάτη, θα παρέχει την προσήκουσα βοήθεια έναντι των ισχυουσών τιμών χρεώσεως «χρόνου και υλικών» για την επιλογή κατάλληλων εναλλακτικών υπηρεσιών που θα

- αγορασθούν ώστε να συνεχίσουν να εκτελούνται όπως κατά την ημέρα της καταγγελίας.
- Η Εταιρία ABC, με την έγγραφη ειδοποίηση του Πελάτη, θα παρέχει την προσήκουσα βοήθεια έναντι των ισχυουσών τιμών χρεώσεως «χρόνου και υλικών» στο βαθμό που είναι αναγκαίο για να δυνηθεί ο Πελάτης να μετακινήσει τα Δεδομένα ή οποιοδήποτε μέρος αυτών που παραμένουν στην κυριότητα του Πελάτη, σε εναλλακτικές τοποθεσίες.
- Η Εταιρία ABC θα είναι υπεύθυνη με δικό της κίνδυνο και δαπάνη για την ανάκτηση οποιουδήποτε τμήματος των Περιουσιακών Στοιχείων, των Δεδομένων και του Συστήματος, κυριότητος της Εταιρίας ABC, που ευρίσκονται στις εγκαταστάσεις του Πελάτη κατά την καταγγελία ή τη λήξη.
- Ο Πελάτης θα είναι υπεύθυνος με δικό του κίνδυνο και δαπάνη για να μετακινήσει τα Περιουσιακά Στοιχεία, τα Δεδομένα ή το Σύστημα ή οποιοδήποτε τμήμα αυτών, επί των οποίων η κυριότητα ή ο νόμιμος τίτλος δεν έχει μεταβιβαστεί στην Εταιρία ABC ή τα οποία επαναγοράζονται ή επανεκχωρούνται και τα οποία ευρίσκονται στις εγκαταστάσεις της Εταιρίας ABC.
- Η Εταιρία ABC θα έχει το δικαίωμα να παρακρατεί τη νομή και κατοχή των Περιουσιακών Στοιχείων που δεν ευρίσκονται υπό την κυριότητα της Εταιρίας ABC και να ασκεί προνόμιο επί των Περιουσιακών Στοιχείων σχετικά με κάθε ανεξόφλητες Χρεώσεις ή άλλα ποσά που οφείλονται στην Εταιρία ABC, υπό τους όρους της παρούσας Συμβάσεως.

12. ΠΕΡΙΟΡΙΣΜΟΙ ΤΗΣ ΕΥΘΥΝΗΣ

Η ευθύνη της Εταιρίας ABC προς τον Πελάτη για απώλεια ή ζημιά ή πρόκληση βλάβης σε περιουσία σχετικά με οποιαδήποτε μεμονωμένη απαίτηση ή σειρά απαιτήσεων σχετιζομένων με την ίδια ενέργεια, παράλειψη η από περιστάσεις απορρέουσες από αμέλεια της Εταιρίας ABC, εσφαλμένη παράσταση, παράβαση συμβατικής υποχρεώσεως ή σφάλμα, σε καμιά περίπτωση δεν θα υπερβαίνει το μεγαλύτερο μεταξύ του ..... ή του ποσού που είναι ίσο με το σύνολο του ποσού ή των ποσών που είναι καταβλητέα από τον Πελάτη σύμφωνα με τη σύμβαση ή τις συμβάσεις (εάν υπάρχουν) με τις οποίες σχετίζεται η ευθύνη.

13. ΑΠΑΓΟΡΕΥΣΗ ΠΡΟΣΛΗΨΗΣ ΕΡΓΑΖΟΜΕΝΩΝ

- Ο Πελάτης κατά τη διάρκεια και για περίοδο 6 μηνών μετέπειτα από τη λήξη της Συμφωνίας, δεν μπορεί να προσλάβει οποιονδήποτε από το προσωπικό της Εταιρίας ABC ή συμβούλους που έχουν αναμιχθεί στην παροχή των Υπηρεσιών ή την εκτέλεση της παρούσας Συμβάσεως.
- Σε περίπτωση κατά την οποία ο Πελάτης διαπιστωθεί ότι έχει παραβεί τον ανωτέρω υπό-όρο, τότε αυτός θα καταβάλει στην Εταιρία ABC ως ρευστοποιημένες ζημιές ένα ποσό ίσο με το ήμισυ του τελικού μικτού ετήσιου μισθού του προσώπου που απασχολήθηκε ή προσλήφθηκε.
- Ο Πελάτης δια του παρόντος αναγνωρίζει και συμφωνεί ότι οι φόρμουλες που περιγράφονται στην παράγραφο 13 αποτελούν εύλογο προσδιορισμό εκ

μέρους της Εταιρίας ΑΒC των δαπανών που θα προκληθούν από την απώλεια του προσώπου που απασχολήθηκε η προσελήφθηκε.

14. ΠΑΡΑΔΟΣΗ ΥΠΗΡΕΣΙΩΝ

Η Εταιρία ΑΒC οφείλει να παραδώσει τις Υπηρεσίες στον Πελάτη, όπως αυτές περιγράφονται στο Παράρτημα Α, κατά την ημερομηνία έναρξης παροχής υπηρεσιών. Σε αντίθετη περίπτωση, η Εταιρία ΑΒC θα υποχρεωθεί να πληρώσει πρόστιμο, το οποίο δε θα ξεπερνάει το 1/30 του μηνιαίου ποσού που καταβάλει ο Πελάτης στην Εταιρία ΑΒC. Σε περίπτωση που ο Πελάτης ζητήσει την παροχή πρόσθετων υπηρεσιών, που δεν προβλέπονται στην παρούσα Σύμβαση, η ημερομηνία παράδοσης τους θα καθοριστεί στο καινούριο Συμφωνητικό που θα γίνει μεταξύ των μερών για τις επιπρόσθετες υπηρεσίες.

15. ΔΙΑΦΟΡΑ – ΛΟΙΠΟΙ ΟΡΟΙ

- Ουδεμία μεταβολή, τροποποίηση ή προσθήκη στην παρούσα Σύμβαση θα είναι έγκυρη, εκτός αν γίνει εγγράφως και υπογραφεί από τους δεόντως εξουσιοδοτημένους εκπροσώπους αμφοτέρων των μερών.
- Η ακυρότητα ή μη εκτελεστότητα οποιουδήποτε μέρους της παρούσας Συμβάσεως δεν θα κωλύει την πλήρη συνέχιση του υπολοίπου μέρους.
- Ουδέν μέρος δύναται να εκχωρήσει ή να ορίσει υπεργολάβο για ολόκληρη ή για μέρος της παρούσας Συμβάσεως χωρίς την προηγούμενη έγγραφη συναίνεση του άλλου μέρους. Οποιαδήποτε απόπειρα εκχωρήσεως ή ορισμού υπεργολάβου για ολοκλήρωση ή για μέρος της παρούσας Συμβάσεως χωρίς την τοιαύτη προηγούμενη έγγραφη συναίνεση είναι άκυρη.
- Οι αναφορές σε Όρους ή Παραρτήματα θα θεωρούνται ως αναφορές στους όρους και τα παραρτήματα της παρούσας Συμβάσεως.

Παράρτημα Α: Καθορισμός των Υπηρεσιών

1. Υπηρεσίες διαχείρισης κλειδιών

- *Δημιουργία Ζεύγους κλειδιών*

Η Εταιρία ΑΒC θα είναι υπεύθυνη για τη δημιουργία ζευγών κλειδιών. Θα δημιουργούνται δύο ζεύγη κλειδιών, ένα για την δημιουργία ψηφιακών υπογραφών και ένα για την κρυπτογράφηση δεδομένων. Το μήκος του κλειδιού θα είναι τουλάχιστον 1024 bits ενώ ο αλγόριθμος κρυπτογράφησης θα αποφασίζετε από την Εταιρία ΑΒC με βάση προκαθορισμένα πρότυπα και το νομοθετικό πλαίσιο στην Ελλάδα και την Ευρωπαϊκή Ένωση, ενώ θα πρέπει να λαμβάνεται υπ'όψιν η δεδομένη υπολογιστική ισχύς. Ο χρόνος ισχύος ενός κλειδιού θα πρέπει να υπολογίζεται βάση του γεγονότος ότι η υπολογιστική ισχύς διπλασιάζεται κάθε δεκαοχτώ μήνες.

- *Αντιστοίχηση του ζεύγους κλειδιών με την αιτούσα οντότητα*

Η Εταιρία ΑΒC, μέσω της Αρχής Πιστοποίησης του Πανελλήνιου Ιατρικού Συλλόγου, είναι υπεύθυνη για την αντιστοίχηση του κάθε ζεύγους κλειδιών με μία μοναδική οντότητα και τη δημιουργία του μοναδικού αναγνωριστικού της. Η Εταιρία ΑΒC οφείλει να διατηρήσει τη μυστικότητα του ιδιωτικού κλειδιού, ενώ σε αντίθετη περίπτωση θα υποστεί τις συνέπειες του όρου 11.

- *Διανομή κλειδιών* [40]

Η Εταιρία ΑΒC πρέπει να εξασφαλίζει ότι η μεταβολή των κλειδιών δεν είναι δυνατή κατά τη διάρκεια της διανομής και ότι δεν είναι πιθανή η ανάγνωση τους από μία τρίτη, μη εξουσιοδοτημένη, οντότητα. Η μετάδοση των κλειδιών θα γίνεται με έξυπνες κάρτες, οι οποίες θα αποστέλλονται με συμβατική συστημένη αλληλογραφία στον Πελάτη.

- *Αποθήκευση κλειδιού*

Η αποθήκευση των ιδιωτικών κλειδιών, έτσι ώστε τα κλειδιά να προστατεύονται από κλοπή, μετατροπή ή κατάχρηση, αποτελεί αρμοδιότητα της Εταιρίας ΑΒC. Εάν ο Πελάτης κάνει μια αίτηση αποθήκευσης ενός κλειδιού, η Εταιρία ΑΒC οφείλει να επιβεβαιώσει των αίτηση αποθήκευσης. Σε περίπτωση αποτυχίας, πρέπει να ενημερώσει εγγράφως τον πελάτη εντός μιας εργάσιμης ημέρας και να περιμένει έγγραφη απάντηση από τον Πελάτη. Σε περίπτωση επιτυχίας οφείλει να στείλει έγγραφη επιβεβαίωση αποθήκευσης. Εάν, για οποιοδήποτε λόγο, η λίστα με τα αποθηκευμένα κλειδιά υποκλαπεί ή καταστραφεί, η Εταιρία ΑΒC οφείλει μέσα σε δύο ημέρες να δημιουργήσει καινούρια ζεύγη κλειδιών και να τα διανείμει στον Πελάτη με τον τρόπο που περιγράφεται στην παρούσα Σύμβαση.

- *Ανάκτηση κλειδιού*

Εάν ο πελάτης αιτηθεί την ανάκτηση του δημοσίου κλειδιού κάποιον εκ των οντοτήτων του, η Εταιρία ΑΒC οφείλει να το παραδώσει σε δύο ώρες από τη στιγμή που έγινε η αίτηση.

- *Ανάκαμψη κλειδιού σε περίπτωση απώλειας ή διακύβευσης της ασφάλειας του*

Σε περιπτώσεις όπου:

1. Ο χρήστης χάσει το ιδιωτικό κλειδί του που απαιτείται για την

αποκρυπτογράφηση σημαντικών πληροφοριών

2. Ο Πελάτης έχει την εξουσία να έχει πρόσβαση σε προστατευόμενες πληροφορίες, αλλά το κλειδί είναι διαθέσιμο μόνο σε ένα μέλος το οποίο δεν είναι παρών
3. Μία απόφαση δικαστηρίου απαιτεί πρόσβαση σε εμπιστευτικές πληροφορίες

και μόνο σε αυτές τις περιπτώσεις, η Εταιρία ΑΒC οφείλει να ανακτήσει το κλειδί από τα αντίγραφα ασφάλειας και μόνο κατόπιν αυθεντικοποίησης της αίτησης, επιβεβαίωσης πλήρους εξουσιοδότησης και νομικά δικαιολογημένης αίτησης. Το κλειδί επιστρέφεται στον αιτηθέντα μέσω έξυπνης κάρτας, όπως προβλέπεται στη Σύμβαση για τη διανομή κλειδιών. Η αυθεντικοποίηση της αίτησης θα γίνεται σύμφωνα με τα όσα ορίζονται στην παράγραφο *Έλεγχος αιτήσεων για διαδικασίες που αφορούν την πρόσβαση στα κλειδιά*, της Συμβάσεως αυτής.

- *Τήρηση αρχείου αντιγράφου κλειδιών*

Η Εταιρία ΑΒC οφείλει να διατηρεί αντίγραφα τόσο των ιδιωτικών όσο και των δημόσιων κλειδιών με τις διαδικασίες αποθήκευσης και ανάκτησης, όπως αυτές αναφέρονται παραπάνω στη Σύμβαση αυτή. Σε περίπτωση φυσικής καταστροφής του αντιγράφου, η Εταιρία ΑΒC δεν φέρει καμία ευθύνη, ενώ σε περίπτωση κλοπής του αντιγράφου από ιδιοκτησία της Εταιρίας ΑΒC, η Εταιρία ΑΒC οφείλει να ενημερώσει τον Πελάτη εντός τριών ωρών από την κλοπή και μέσα σε δύο μέρες να δημιουργήσει και να παραδώσει νέα ζεύγη κλειδιών.

- *Ενημέρωση κλειδιού*

Σε περίπτωση λήξης ενός πιστοποιητικού ή σχετικής έγγραφης αίτησης από τον Πελάτη, η Εταιρία ΑΒC πρέπει να ενημερώσει ή να ανανεώσει ένα κλειδί εντός δύο ημερών. Επίσης η Εταιρία ΑΒC οφείλει να ενημερώνει περιοδικά τα κλειδιά. Η περίοδος ενημέρωσης θα είναι ανάλογη της διάρκειας ζωής ενός κλειδιού και δε θα ξεπερνά τους τέσσερις μήνες με εξαιρέσεις περιπτώσεις όπου το κλειδί χρησιμοποιήθηκε για να υπογραφεί ψηφιακά ένα κείμενο, το οποίο πρέπει να παραμείνει έγκυρο για μεγαλύτερο χρονικό διάστημα.

Σε περιπτώσεις διακύβευσης ενός κλειδιού, η Εταιρία ΑΒC πρέπει να ενημερώσει τον Πελάτη εντός τριών ωρών από τη στιγμή επιβεβαίωσης της διακύβευσης και να ανανεώνει το κλειδί εντός δύο ημερών. Σε αντίθετη περίπτωση και εάν ο προκληθεί οποιουδήποτε είδους ζημιά στον Πελάτη λόγω καθυστέρησης ενημέρωσης από την Εταιρία ΑΒC, η Εταιρία ΑΒC θα είναι υποχρεωμένη να αποζημιώσει τον Πελάτη για τη ζημιά που έπαθε. Εάν το διακυβευθέν κλειδί είναι το κλειδί της Εταιρίας ΑΒC, τότε η Εταιρία ΑΒC οφείλει να αποσύρει και να αντικαταστήσει το πιστοποιητικό της Αρχής Πιστοποίησης του Πανελλήνιου Ιατρικού Συλλόγου που έχει υπογραφεί από αυτό το κλειδί. Αν χαθεί το κλειδί της Αρχής Πιστοποίησης του Πανελλήνιου Ιατρικού Συλλόγου, πρέπει να αποσυρθούν και να αντικατασταθούν όλα τα πιστοποιητικά που έχουν υπογραφεί από το κλειδί αυτό.

Τα παλαιότερα ζεύγη κλειδιών θα διατηρούνται από την Εταιρία ABC για την αντιμετώπιση πιθανών διενέξεων μεταξύ χρηστών που αφορούν σε παλαιότερα έγγραφα.

- *Έλεγχος αιτήσεων για διαδικασίες που αφορούν την πρόσβαση στα κλειδιά*

Η Εταιρία ABC οφείλει να ελέγχει τα παρακάτω σε περιπτώσεις αποδοχής και ελέγχου αιτήσεων που αφορούν την ενημέρωση, ανανέωση, επαναφορά και ανάκαμψη των κλειδιών:

1. Αν ο αιτών είναι ιδιοκτήτης του κλειδιού
2. Αν ο αιτών είναι εξουσιοδοτημένος να αποκτήσει πρόσβαση στο κλειδί
3. Ότι ο αιτών έχει υπογράψει ψηφιακά την αίτηση και ότι έχει κατάλληλα αυθεντικοποιηθεί
4. Ότι οι λόγοι για την πρόσβαση στο κλειδί βρίσκονται σε συμφωνία με τους κανόνες και την πολιτική της Εταιρίας ABC

- *Καθορισμός δικαιωμάτων πρόσβασης του προσωπικού σε διαδικασίες διαχείρισης κλειδιών*

Η Εταιρία ABC οφείλει να ενημερώνει τον Πελάτη για τους ρόλους και τα δικαιώματα και τις υποχρεώσεις κάθε υπαλλήλου εφόσον αυτό ζητηθεί.

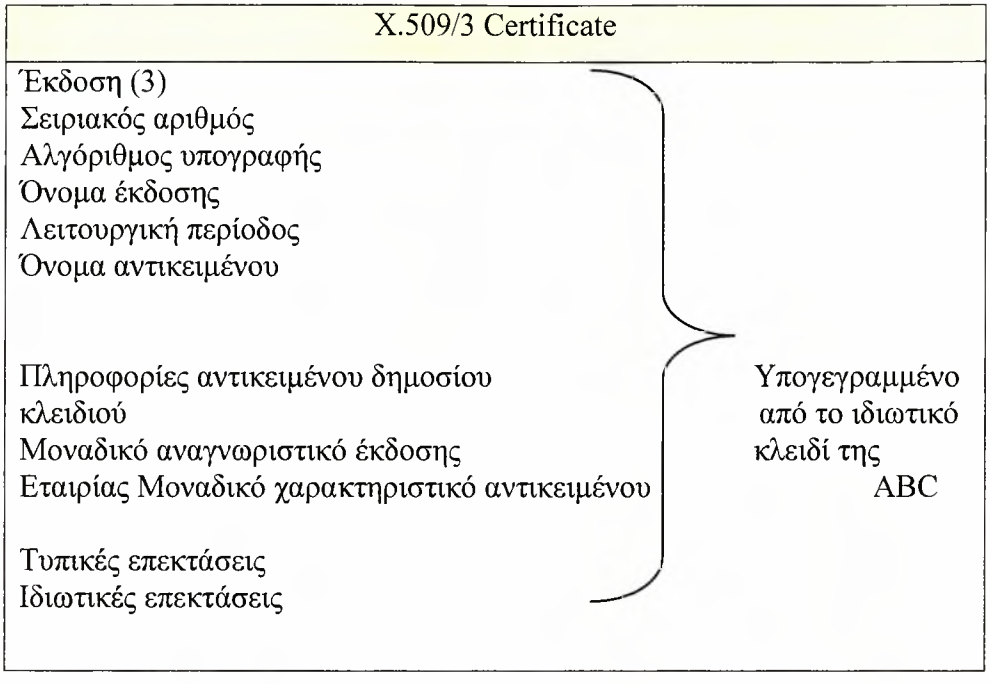
2. Υπηρεσίες διαχείρισης πιστοποιητικών

- *Δημιουργία Πιστοποιητικών*

Η Εταιρία ABC δε φέρει καμία ευθύνη για την αντιστοίχηση των πιστοποιητικών με την κάθε οντότητα. Η διαδικασία εγγραφής και επιβεβαίωσης των μελών του Πελάτη καθώς και η ευθύνη της σωστής αντιστοίχησης βαραίνει αποκλειστικά και μόνο των Πελάτη.

Μετά τη δημιουργία των πιστοποιητικών αυτά θα υπογράφονται από το ιδιωτικό κλειδί της εταιρίας ABC, η οποία θα αναλαμβάνει την ευθύνη για την αυθεντικοποίηση των πληροφοριών που αναγράφονται στο κάθε πιστοποιητικό.

Η δημιουργία των πιστοποιητικών θα βασίζεται στο πρότυπο X.509, και πιο συγκεκριμένα την τρίτη έκδοση, και θα περιλαμβάνει [40]:



- *Διανομή πιστοποιητικών*

Μετά τη δημιουργία των πιστοποιητικών η Εταιρία ABC οφείλει να τα παραδώσει στον Πελάτη. Η Εταιρία ABC δεν φέρει καμία ευθύνη για τη διαδικασία διανομής των πιστοποιητικών σε κάθε οντότητα. Η διαδικασία διανομής των πιστοποιητικών στα μέλη του Πελάτη δεν αποτελεί μέρος αυτής της Σύμβασης. Ο τρόπος παράδοσης των πιστοποιητικών από την Εταιρία ABC στον Πελάτη θα γίνεται μέσω του παγκόσμιου ιστού, με χρήση μηχανισμών αυθεντικοποίησης. Με χρήση ενός προκαθορισμένου συνθηματικού, ο Πελάτης θα μπορεί να έχει πρόσβαση στην περιοχή αποθήκευσης των πιστοποιητικών στην Εταιρία ABC και από εκεί να αποθηκεύει τα πιστοποιητικά σε δικό του χώρο.

- *Αποθήκευση και ανάκτηση πιστοποιητικού*

Κατά τη στιγμή δημιουργίας ενός πιστοποιητικού, η Εταιρία ABC αναλαμβάνει την αποστολή ενός αντιγράφου του πιστοποιητικού στην υπηρεσία καταλόγου. Η Εταιρία ABC αναλαμβάνει επίσης τη διατήρηση αντιγράφων των πιστοποιητικών για περιπτώσεις όπου χρειάζεται η ανάνηψη ενός πιστοποιητικού που έχει χαθεί ή για την επίλυση διαφορών ή για περιπτώσεις που ο Πελάτης ζητήσει πληροφορίες για τα πιστοποιητικά. Στην τελευταία περίπτωση, η Εταιρία ABC δεσμεύεται να δώσει τις πληροφορίες που ζητήθηκαν από τον πελάτη εντός μίας ημέρας από τη στιγμή που έγινε η έγγραφη αίτηση.

Ο Πελάτης δύναται να χρησιμοποιήσει το πρωτόκολλο υπερκειμένου (HTTP) ως το μέσο διασύνδεσης με την υπηρεσία καταλόγου, όπου η τελευταία θα λειτουργεί ως μέσω διασύνδεση της οντότητας με την αποθήκευση

πιστοποιητικών. Ο Πελάτης θα διαθέτει ένα συνθηματικό ώστε να αυθεντικοποιείται και επιβεβαιώνεται η δυνατότητα πρόσβασης στις υπηρεσίες καταλόγου.

- *Ανάκληση πιστοποιητικού*

Ακύρωση πιστοποιητικού μπορεί να συμβεί για τους εξής λόγους:

1. Τερματισμός περιόδου εγκυρότητας
2. Διακύβευση ασφάλειας
3. Απώλεια ιδιωτικού κλειδιού και ανανέωση

Σε περίπτωση ακύρωσης, ο Πελάτης πρέπει να ενημερωθεί από την Εταιρία ΑΒC εντός δύο ωρών από την ακύρωση του πιστοποιητικού.

Η Εταιρία ΑΒC οφείλει να διατηρεί μια Λίστα Ανακληθέντων Πιστοποιητικών την οποία θα πρέπει να ενημερώνει σε τακτικά χρονικά διαστήματα. Οι διαδικασίες αποθήκευσης και ανάκτησης της Λίστας Ανακληθέντων Πιστοποιητικών γίνεται σύμφωνα με τις διαδικασίες αποθήκευσης και ανάκτησης των πιστοποιητικών που αναφέρονται παραπάνω στην παρούσα Σύμβαση. Η διανομή της Λίστας Ανακληθέντων Πιστοποιητικών θα γίνεται μέσω της υπηρεσίας καταλόγου. Προτού η Εταιρία ΑΒC διανείμει τη Λίστα στον Πελάτη όταν αυτή ζητηθεί, οφείλει να την υπογράψει με το ιδιωτικό της κλειδί.

❖ Διαδικασία αίτησης ανάκλησης

Στην περίπτωση που ο Πελάτης υποπτευθεί ότι κάποιο από τα ιδιωτικά κλειδιά έχει διακυβευτεί πρέπει να ενημερώσει την Εταιρία ΑΒC εντός μιας ημέρας. Ο Πελάτης πρέπει να υποβάλει έγγραφη αίτηση ανάκλησης του πιστοποιητικού προς την Εταιρία ΑΒC. Η Εταιρία ΑΒC οφείλει να ενεργοποιήσει όλες τις διαδικασίες που απαιτούνται για την ανάκληση του πιστοποιητικού, όπως αυτές αναφέρονται στην παράγραφο *Μηχανισμοί Ανάκλησης*. Μετά την ακύρωση του πιστοποιητικού, η Εταιρία ΑΒC πρέπει να δημοσιοποιήσει το γεγονός στον Πελάτη, είτε μέσω ηλεκτρονικής, είτε μέσω συμβατικής αλληλογραφίας.

Η αίτηση μπορεί να παραδίδεται είτε ηλεκτρονικά μέσω του διαδικτύου, είτε μέσω τηλεφώνου, είτε μέσω συμβατικής αλληλογραφίας.

Όταν η Εταιρία ΑΒC λάβει την αίτηση θα πρέπει να επικοινωνήσει τηλεφωνικά με τον Πελάτη εντός της ίδιας ημέρας που έγινε η αίτηση, ώστε να αυθεντικοποιηθεί η αίτηση.

❖ Μηχανισμοί Ανάκλησης

Η Εταιρία ΑΒC διατηρεί Λίστες Ανάκλησης Πιστοποιητικών, όπως αυτές περιγράφηκαν ανωτέρω, Ο Πελάτης έχει τη δυνατότητα να υποβάλει αίτηση και να λάβει απάντηση από την Εταιρία ΑΒC σχετικά με την ακύρωση ενός πιστοποιητικού.

Παράρτημα Β: Χρεώσεις

ΓΙΑ ΤΗΝ ΕΤΑΙΡΙΑ ΑΒC	**ΓΙΑ ΤΟΝ ΠΕΛΑΤΗ**
Υπογραφή :	Υπογραφή :
Όνομα :	Όνομα :
Τίτλος :	Τίτλος :
Ημερομηνία :	Ημερομηνία :

Πίνακας 8: Πρότυπο Συμφωνητικού Διαχείρισης Υπηρεσιών

Η δημιουργία της παραπάνω σύμβασης βασίστηκε στο πρότυπο Συμβάσεως Διασφάλισης Ποιότητας που περιέχεται στην εργασία "Outsourcing" της ομάδας Ε5 [7]. Διαφοροποιήθηκε ως προς τα εξής σημεία:

1. Τον τρόπο πληρωμής. Στο συμφωνητικό-πρότυπο δίνεται η δυνατότητα πληρωμής ολόκληρου του ποσού μέσα σε συγκεκριμένο χρονικό διάστημα, όπως επίσης απαιτείται και μια προκαταβολή.
2. Δεν χρησιμοποιήθηκε η παράγραφος **ΕΓΚΑΤΑΣΤΑΣΕΙΣ** που υπήρχε στο πρότυπο συμφωνητικό
3. Τα δικαιώματα πρόσβασης. Στο παρών Συμφωνητικό ο πάροχος δεν έχει δικαιώματα πρόσβασης στα Δεδομένα και το Σύστημα του Πελάτη.
4. Παραλήφθηκε εντελώς η παράγραφος **ΠΑΡΑΔΟΣΗ ΣΥΣΤΗΜΑΤΟΣ** του πρότυπου πιστοποιητικού και προστέθηκε η παράγραφος **ΠΑΡΑΔΟΣΗ ΥΠΗΡΕΣΙΩΝ**.
5. Παραλήφθηκε η παράγραφος **ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ** του πρότυπου συμφωνητικού.
6. Παραλήφθηκε η παράγραφος **ΑΠΟΖΗΜΙΩΣΕΙΣ** .
7. Στην παράγραφο **ΑΛΛΑΓΕΣ ΣΤΙΣ ΑΠΑΙΤΗΣΕΙΣ ΤΩΝ ΠΑΡΕΧΟΜΕΝΩΝ ΥΠΗΡΕΣΙΩΝ** έχουν παραληφθεί τα δικαιώματα του παρόχου
8. Παραλήφθηκε η παράγραφος **ΜΕΣΑ ΕΠΙΚΟΙΝΩΝΙΑΣ** .

9. Στο παρών συμφωνητικό διαφοροποιούνται οι όροι κάτω από τους οποίους μπορεί να λήξει το συμβόλαιο στη παράγραφο **ΛΗΞΗ**.
10. Στο παρών συμφωνητικό διαφοροποιούνται οι συνέπειες της λήξης της συνεργασίας στην παράγραφο **ΣΥΝΕΠΕΙΕΣ ΤΗΣ ΚΑΤΑΓΓΕΛΙΑΣ**.
11. Διαφοροποιούνται οι περιορισμοί της ευθύνης στην παράγραφο **ΠΕΡΙΟΡΙΣΜΟΙ ΤΗΣ ΕΥΘΥΝΗΣ**.
12. Διαφοροποιείται η παράγραφος **ΔΙΑΦΟΡΟΙ-ΛΟΙΠΟΙ ΟΡΟΙ**.
13. Προστέθηκε το **ΠΑΡΑΡΤΗΜΑ Α** στο οποίο περιγράφονται οι υπηρεσίες.
14. Προστέθηκε το **ΠΑΡΑΡΤΗΜΑ Β** το οποίο περιέχει τις χρεώσεις.

5.5 Αποτίμηση

Η ανάθεση ολόκληρης της διαδικασίας έκδοσης ψηφιακών πιστοποιητικών στην Εταιρία ABC θα μπορούσε να βοηθήσει σε μεγάλο βαθμό τον Πανελλήνιο Ιατρικό Σύλλογο.

Κάποιοι, ίσως, ισχυριζόντουσαν ότι ο Σύλλογος έχει τη δυνατότητα παραγωγής των κλειδιών από μόνος του και ότι η ανάθεση σε τρίτους είναι περιττή. Ο Ιατρικός Σύλλογος, όμως, δεν είχε την απαραίτητη εμπειρία για να παράγει ένα αξιόπιστο και ασφαλές ζεύγος κλειδιών, ενώ η Εταιρία ABC μπορούσε να υποστηρίξει έναν επαγγελματικό τρόπο παραγωγής κλειδιών. Επιπρόσθετα, η Εταιρία ABC ήταν ενήμερη για όλες τις νομοθεσίες, σε κρατικό αλλά και διεθνές επίπεδο, που διέπουν τις διαδικασίες δημιουργίας Ψηφιακών Πιστοποιητικών, η αναζήτηση των οποίων θα ήταν ιδιαίτερα χρονοβόρα εάν αναλάμβανε ο Σύλλογος τη δημιουργία των Πιστοποιητικών.

Η Εταιρία ABC γνώριζε όλες τις τελευταίες εξελίξεις γύρω από το συγκεκριμένο θέμα, και θα ήταν έτοιμη για να αντιδράσει σε περιπτώσεις που κάτι πήγαινε στραβά. Το άρτια εκπαιδευμένο προσωπικό της ήταν συνεχώς σε εγρήγορση και έτοιμο για να αντιμετωπίσει πιθανά προβλήματα. Ο χρόνος ανταπόκρισης σε τέτοιες περιπτώσεις θα ήταν σίγουρα μικρότερος από τη διάρκεια αποκατάστασης κάποιου λάθους σε περίπτωση που η δημιουργία των πιστοποιητικών θα ήταν ευθύνη του συλλόγου.

Για να μπορέσει ο ιατρικός σύλλογος να αναλάβει ολόκληρη τη διαδικασία θα έπρεπε να αναζητήσει τουλάχιστον δύο άτομα που να γνωρίζουν καλά το αντικείμενο, να τους προσλάβει και να τους ανταμείβει κατάλληλα. Αυτό, σε όρους κόστους, σημαίνει αφιέρωση σημαντικού χρόνου στην αναζήτηση και την επιλογή των ατόμων, αλλά και αύξηση των εξόδων για τη μίσθωση αυτών. Όσον αφορά στο χρόνο, δεν ήταν εύκολο να αφιερωθεί πολύς χρόνος για κάτι τέτοιο, αλλά ούτε υπήρχαν εργαζόμενοι στον Ιατρικό Σύλλογο, με κατάλληλες γνώσεις για την επιλογή των νέων ατόμων. Υπολογίστηκε ότι ο μισθός τους, σε μηνιαία βάση, δε θα ήταν λιγότερος από 1500€ και σε αυτό το ποσό πρέπει να προστεθούν τα έξοδα ασφάλισης και τυχόν επιδόματα.

Όσον αφορά στο χρηματικό κόστος, πρέπει να συνυπολογιστεί σε αυτό και το κόστος απόκτησης των κατάλληλων εργαλείων για τη διαδικασία της δημιουργίας των Πιστοποιητικών. Τα χρήματα που θα εξοικονομούνταν με αυτόν τον τρόπο, θα μπορούσαν να χρησιμοποιηθούν σε άλλες δραστηριότητες τους Συλλόγου, όπως αγορά εργαλείου για καλύτερη γραμματειακή υποστήριξη.

Επίσης, μια τέτοια κίνηση θα δημιουργούσε ένα κλίμα εμπιστοσύνης μεταξύ των μελών του Συλλόγου και των διαδικασιών που ανατέθηκαν στην Εταιρία ABC. Τα μέλη γνωρίζοντας ότι μια εταιρία, τόσο αναγνωρισμένη όσο η ABC, έχει αναλάβει μέρος της προστασίας των ηλεκτρονικών συναλλαγών του Συλλόγου θα νοιώθουν μεγαλύτερη ασφάλεια. Συγκεκριμένα, υπολογίζεται ότι θα μπορούσε να αυξηθεί κατά 45% ο αριθμός των μελών που θα διαλέγουν να αποκτήσουν τις πληροφορίες που θέλουν μέσω διαδικτύου. Αυτό θα αποδέσμευσε τους υπαλλήλους του Συλλόγου, δημιουργώντας τους, έτσι, την ευκαιρία να ασχοληθούν με άλλες δραστηριότητες και να βελτιώσουν τον τρόπο λειτουργίας του Συλλόγου και τις υπηρεσίες που παρέχει.

Ως προς τα διαδικαστικά θέματα, αναμένεται να τηρηθούν όλοι οι, προβλεπόμενοι από το Συμφωνητικό Διαχείρισης Υπηρεσιών, όροι και να διατηρηθεί το προσυμφωνηθέν επίπεδο ποιότητας. Επίσης, υπάρχει η πεποίθηση ότι δε θα προκύψει σοβαρό πρόβλημα που να αφορά την ασφάλεια των προσωπικών δεδομένων των μελών του Συλλόγου και των δεδομένων που ανήκουν στο Σύλλογο.

Κεφάλαιο 6: Συμπεράσματα

Το outsourcing αποτελεί πλέον πρακτική για πολλές μικρές αλλά και μεγάλες επιχειρήσεις, αφού παρέχει τη δυνατότητα σε αυτές να επωφεληθούν "αγοράζοντας" εξειδικευμένες υπηρεσίες ασφάλειας. Κάθε φορά που ένας οργανισμός επιλέγει να δώσει κάποιες υπηρεσίες για outsourcing, καταφέρνει να χαμηλώσει το κόστος, να βελτιώσει τον ισολογισμό του, να μειώσει τους κινδύνους στους οποίους εκτίθεται, να βελτιώσει την παραγωγικότητα, να μειώσει τις ευθύνες των επιχειρηματιών και των εργαζομένων σε αυτόν και να επεκτείνει τις ικανότητες του. Αλλά, αν η τεχνική του outsourcing συνεχίσει να αναπτύσσεται τα επόμενα χρόνια με τους ρυθμούς που αναπτύσσεται μέχρι τώρα (από $28.7 δισεκατομμύρια το 2004 αναμένεται να φτάσει τα $70 δισεκατομμύρια μέχρι το 2011 [21]), θα πρέπει να δημιουργηθούν διαδικασίες προτυποποίησης ώστε να αποφεύγονται τυχόν παρατυπίες και να μειωθεί το κόστος ακόμα περισσότερο. Για να έχει αποτέλεσμα η προσπάθεια αυτή πρέπει να συνεργαστούν και οι δύο πλευρές (πελάτες-πάροχοι).

Για να ανακεφαλαιώσουμε, το outsourcing λειτουργεί καλύτερα όταν:

1. Υπάρχει στην αγορά πληθώρα προμηθευτών υψηλής ποιότητας υπηρεσιών ασφάλειας και κατά συνέπεια μεγάλος ανταγωνισμός μεταξύ τους.
2. Οι ικανότητες των προμηθευτών μπορούν να χρησιμοποιηθούν για να κερδίσει η εκάστοτε εταιρία ένα ανταγωνιστικό πλεονέκτημα.
3. Οι ικανότητες των ατόμων που εργάζονται στην εταιρία καθώς και οι πόροι της μπορούν να χρησιμοποιηθούν καλύτερα αλλού μέσα στην εταιρία ή να γίνουν μέρος της διαδικασίας του outsourcing.
4. Η εξωτερική σχέση θα μειώσει τους κινδύνους μια εταιρίας μέσα σε ένα μεταβαλλόμενο περιβάλλον.

Από την άλλη, το να κρατάς τις λειτουργίες αυτές ενδοεπιχειρισιακά λειτουργεί όταν:

1. Δεν υπάρχουν αποδεδειγμένα ικανοί προμηθευτές.
2. Το να συνεχίσουν να λειτουργούν ενδοεπιχειρησιακά οι δραστηριότητες της ασφάλειας προστατεύουν ένα σαφές ανταγωνιστικό πλεονέκτημα που θα χαθεί εάν επιλεγεί το outsourcing.

3. Το κόστος του outsourcing είναι πολύ υψηλό.
4. Δεν υπάρχει προσωπικό το οποίο μπορεί να επιβλέψει μια σχέση outsourcing.

Τελικά, όσο πιο μεγάλος είναι ένας οργανισμός, τόσο πιο ανθεκτικός γίνεται στην εισαγωγή του outsourcing. Αυτό συμβαίνει γιατί διαθέτει τους πόρους και τα μέσα (χρήματα, προσωπικό κ.τ.λ.) ώστε να ανταπεξέλθει στις απαιτήσεις της ασφάλειας ενός δικτύου. Σε αντίθεση, οι μικρότερες επιχειρήσεις δεν έχουν ούτε το προσωπικό αλλά ούτε και τα χρήματα για να ανταποκριθούν στο σύνολο των κινδύνων που ελλοχεύουν στην ολοένα και μεγαλύτερη εξάρτηση τους από το ίντερνετ. Για αυτό και καταφεύγουν στη λύση του outsourcing ευκολότερα. Αλλά, οι μικρές εταιρίες θα πρέπει να ακολουθούν ένα μοντέλο το οποίο είναι ευέλικτο, οικονομικά ανεκτό και ταιριάζει με τους επιχειρηματικούς τους στόχους.

Αν υλοποιηθεί σωστά μια τέτοια λύση μπορεί να αλλάξει προς το καλύτερο την λειτουργία μιας επιχείρησης και να προσθέσει αξία στις καθημερινές λειτουργίες της. Μια σχέση outsourcing, όταν επιλεγεί ένας έμπειρος και αξιόπιστος πάροχος, επιτρέπει στους πελάτες να απολαύσουν τα οφέλη ενός υψηλού επιπέδου ασφάλειας χωρίς να είναι αναγκασμένοι να υλοποιούν, να συντηρούν και να παρακολουθούν συνεχώς τα προϊόντα και τις πολιτικές ασφαλείας. Όπως επισημάνθηκε, όμως, ο σκοπός μιας εταιρίας που αξιολογεί την περίπτωση του outsourcing, δεν πρέπει να είναι μόνο η μείωση του κόστους. Παρόλο που η συνολική μείωση του κόστους πρέπει να λαμβάνεται υπ' όψιν, το χαμηλού κόστους outsourcing μπορεί να οδηγήσει σε χαμηλή ποιότητα υπηρεσιών.

Όπως είναι φυσικό, υπάρχει και η αρνητική πλευρά του outsourcing. Μπορεί να ακούγονται πολύ ελκυστικά όσα μπορούν να επιτευχθούν μέσα από το outsourcing αλλά από την άλλη τα να αναθέτεις την ασφάλεια του δικτύου σου σε άλλη εταιρία είναι επικίνδυνο. Για αυτό το σκοπό, προτείνεται ως πιθανή μελλοντική επέκταση του θέματος η ανάπτυξη τεχνικών που να διασφαλίζουν την ασφαλή επικοινωνία μεταξύ παρόχου και πελάτη, όπως, επίσης, και η έρευνα πάνω στο πως θα διασφαλιστεί η μυστικότητα των δεδομένων μιας επιχείρησης, όταν αυτά βρίσκονται στα χέρια του παρόχου των υπηρεσιών.

Επίσης, περαιτέρω έρευνα θα μπορούσε να γίνει στον τομέα της δημιουργίας ενός βέλτιστου συμβολαίου μεταξύ των δύο πλευρών που θα ικανοποιεί τις απαιτήσεις και τις ανάγκες τους και το οποίο θα λαμβάνει υπ' όψιν του διάφορες παραμέτρους, όπως η απόδοση, η εμπειρία, η αξιοπιστία, η φήμη κ.τ.λ.

Το μοντέλο που αναφέρεται στο κεφάλαιο 3 είναι μια πρώτη προσέγγιση του προβλήματος της δημιουργίας ενός βέλτιστου συμβολαίου. Το κόστος μετάβασης είναι πολύ σημαντικός παράγοντας στην περίπτωση της ασφάλειας δικτύων για δύο κυρίως λόγους. Πρώτον, γιατί όπως έχει ήδη αναφερθεί η ασφάλεια είναι περισσότερο τέχνη και όχι επιστήμη και δεύτερον, γιατί υπάρχει αυξημένη αβεβαιότητα σχετικά με τους κινδύνους η οποία αυξάνει τα κόστη συντονισμού. Οι επιθέσεις στο ίντερνετ μπορεί να είναι σπάνιες και να υπάρχει αδράνεια για μεγάλο χρονικό διάστημα. Μπορεί όμως μια περίοδος να είναι πολύ έντονη και γεμάτη από περιστατικά. Για αυτό σε μελλοντικές προσπάθειες ανάπτυξης τέτοιων μοντέλων προτείνεται να ληφθούν υπ' όψιν.

Τέλος, προτείνεται η δημιουργία ενός εργαλείου που θα αυτοματοποιεί τη διαδικασία δημιουργίας μιας Σύμβασης Διασφάλισης Ποιότητας. Το συγκεκριμένο εργαλείο θα δέχεται ως είσοδο τα δεδομένα κάθε περίπτωσης και η έξοδος του θα είναι ένα πρότυπο της Σύμβασης Ποιότητας (αν όχι η ίδια). Επίσης, θα μπορούσε να αναπτυχθεί ένα εργαλείο το οποίο να ελέγχει το κατά πόσο και οι δύο πλευρές τηρούν τους όρους της Σύμβασης.

Όσον αφορά τα ελληνικά δεδομένα, το outsourcing βρίσκεται σε πολύ πρώιμο στάδιο. Εν μέρει οφείλεται στην αργή διάδοση του ίντερνετ και γενικότερα των σύγχρονων τεχνολογιών. Η χρήση τους τώρα αρχίζει να διαδίδεται και, όπως είναι φυσικό, τώρα αρχίζουν να εντοπίζονται τα προβλήματα που προκύπτουν και μελλοντικά θα γίνουν προσπάθειες για να βρεθεί η καλύτερη λύση για αυτά. Ένας άλλος λόγος για την μικρή ανάπτυξη του outsourcing, είναι η έλλειψη ισχυρών νόμων που μπορούν να διασφαλίσουν μια τέτοιου είδους σχέση και κατ'επέκτασην η έλλειψη εμπιστοσύνης σε εταιρίες που διαθέτουν τέτοιες υπηρεσίες. Σημαντικό είναι, επίσης, το ότι δεν υπάρχουν αρκετές εταιρίες στην Ελλάδα που να κάνουν αυτήν τη δουλειά, πράγμα που δείχνει ότι

το έδαφος δεν είναι ακόμα ώριμο για την ανάπτυξη μιας τέτοιας βιομηχανίας. Αυτό έχει σαν αποτέλεσμα την έλλειψη ανταγωνισμού, τη διατήρηση των τιμών σε υψηλά επίπεδα και τη μικρή ενημέρωση πάνω σε αυτόν τον τομέα.

Κάνοντας μια σύγκριση και πάλι του outsourcing με την ιατρική φροντίδα, οι γιατροί και τα νοσοκομεία είναι ο μόνος τρόπος για να έχεις ικανοποιητική ιατρική φροντίδα. Παρομοίως, το outsourcing είναι ο μόνος τρόπος να διατηρηθεί ένα επαρκές και ικανοποιητικό επίπεδο ασφάλειας στα σημερινά δίκτυα των επιχειρήσεων.

Παράρτημα Α

Υπηρεσίες ασφάλειας που προσφέρονται από τις εταιρίες-παροχείς [33]:

Ασφάλεια εφαρμογής/Αναθεώρηση κώδικα	Έλεγχος του κώδικα των εφαρμογών web για ευπάθειες και επισφαλής τεχνικές κωδικοποίησης
Αποτίμηση ευπαθειών και διαχείριση	Εκτέλεση τεστ διείσδυσης σε συστήματα για γνωστές ευπάθειες
Πιστοποιητικά	Αποτίμηση της συμμόρφωσης της εταιρείας με την κυβέρνηση, τη βιομηχανία, τις απαιτήσεις συνεργατών και πελατών και διανομή απόδειξης της συμμόρφωσης
Διαχείριση κινδύνων	Βοήθεια προς τους πελάτες για να πάρουν αποφάσεις σχετικά με τη μείωση των ευπαθειών είτε ελαχιστοποιώντας τους κινδύνους ή εφαρμόζοντας αποτελεσματικούς ως προς το κόστος ελέγχους
Υπηρεσίες Firewall	24x7 παρακολούθηση της κίνησης μέσα από το firewall
Υπηρεσίες VPN	Παρόμοιες με αυτές του firewall,συνήθως λειτουργούν επιπρόσθετα με τις υπηρεσίες firewall
Email anti-spam/antivirus	Έλεγχος του περιεχομένου (των email και των συννημένων) για πιθανό μοχθηρό κώδικα η για junk mails
Υπηρεσίες IDS	24x7παρακολούθηση της κίνησης του δικτύου, ανίχνευση και ανάλυση ανωμαλιών για πραγματικές επιθέσεις

Υπηρεσίες IPS	24x7 παρακολούθηση, μπλοκάρισμα απειλών πριν συμβεί οτιδήποτε
Παρακολούθηση ασφάλειας	Παρόμοια με τα IDS, μπορεί να συνδυάζει γεγονότα από πολλές διαφορετικές πηγές και να παρέχει σε βάθος ανάλυση
Ευφυΐα απειλής (threat intelligence)	Βασίζεται σε έρευνα του παρόχου σε γεγονότα του πραγματικού κόσμου, προσφέρει μια σειρά από χαρακτηριστικά τα οποία περιέχουν κάθε προειδοποίηση ανερχόμενης απειλής, την σοβαρότητα και τη διάσταση αυτής καθώς και άμεση επισήμανση και συμβουλές
Απάντηση σε περιστατικά και επιχειρηματολογία	Απαντήσεις σε περιστατικά βασιζόμενη σε 5 βασικές λειτουργίες: ανίχνευση, αποτίμηση, επιχειρηματολογία, περιεχόμενο και ανάκαμψη
Αυθεντικοποίηση	Επαλήθευση και επιβεβαίωση της ταυτότητας ατόμων που προσπελάζουν ευαίσθητες πληροφορίες ή που πραγματοποιούν μεγάλης αξίας συναλλαγές B2B
Διαχείριση ταυτότητας	Διαχείριση της αυθεντικοποίησης των χρηστών, των δικαιωμάτων πρόσβασης, περιορισμών πρόσβασης, του προφίλ των λογαριασμών, των κωδικών πρόσβασης και άλλων παρόμοιων χαρακτηριστικών
Διαβούλευση	Η πρακτική του να βοηθάς εταιρείες να βελτιώσουν το επίπεδο ασφάλειας μέσα από επαγγελματικές αναλύσεις
Υπηρεσία παρακολούθησης των logs	Η διαδικασία της παρακολούθησης και της

	δημιουργίας ημερολογίου με όλα τα γεγονότα που συνέβησαν, η ανάλυση και συσχέτιση αυτών καθώς και η αναφορά τους στην εταιρεία-πελάτη

Πίνακας 9: Υπηρεσίες outsourcing

Παράρτημα Β

Ερωτηματολόγιο που χρησιμοποιήθηκε για την αποτύπωση της κατάστασης στην Ελλάδα

- Έχετε δικό σας τμήμα πληροφορικής;
  Ναι Όχι

- Εάν ναι ο αριθμός των εργαζομένων που απασχολούνται σε αυτό είναι:
  1. 1-3
  2. 4-6
  3. 6-10
  4. 10 και άνω

- Υπάρχει κάποιος υπεύθυνος για την ασφάλεια του δικτύου της επιχείρησης σας?
  Ναι Όχι

- Εάν ναι είναι ένας ή παραπάνω;

- Πόσο σημαντικό είναι το δίκτυο σας για τη ζωτικότητα της επιχείρηση σας;
  1. Αδιάφορο
  2. Μέτριας Σημασίας
  3. Μέγιστης Σημασίας

- Γνωρίζεται ότι υπάρχουν εταιρείες που μπορούν να αναλάβουν την ασφάλεια του δικτύου σας:
  Ναι Όχι

- Εάν ναι πιστεύετε ότι η τιμή των υπηρεσιών που προσφέρονται σε σχέση με την ποιότητα αυτών είναι
  1. Καλή
  2. Ικανοποιητική
  3. Εξαιρετική

- Θα εμπιστευόσασταν την ασφάλεια του δικτύου σας σε κάποια άλλη εταιρεία?
  Ναι Όχι

- Εάν όχι δε θα το κάνατε γιατί:
  1. Δε θα εμπιστευόσασταν σε άλλους το δίκτυο σας
  2. Δεν πιστεύετε πως η υπάρχουσα νομοθεσία σας καλύπτει
  3. Δεν έχετε ακούσει ποτέ για κάτι τέτοιο
  4. Πιστεύετε ότι η συνάρτηση τιμής- ποιότητας δεν είναι γραμμική

- Εάν ναι θα εμπιστευόσασταν σε αυτούς :
  1. Ολόκληρο τον τομέα της ασφάλειας
  2. Μέρος αυτού

- Είναι εύκολο να εμπιστευθείτε κάτι τόσο σημαντικό όπως είναι η ασφάλεια του δικτύου σας ;
  1. Καθόλου
  2. Λίγο
  3. Αρκετά
  4. Πολύ

- Ποιες από τις παρακάτω υπηρεσίες-προϊόντα θα εμπιστευόσασταν σε μια εταιρεία που παρέχει ασφάλεια ;

1. Πιστοποιητικά (πελατών, servers)
2. VPN
3. Πολιτική ασφάλειας
4. Παρακολούθηση και έλεγχο του δικτύου
5. Ανάλυση των συναγερμών
6. Άλλο (παρακαλώ συμπληρώστε)

- Αναπτύσσετε κάποιες από τις παρακάτω υπηρεσίες-προϊόντα ενδοεπιχειρησιακά;
  1. Πιστοποιητικά
  2. VPN
  3. Πολιτική ασφαλείας
  4. Παρακολούθηση και έλεγχο του δικτύου
  5. Ανάλυση των συναγερμών
  6. Άλλο(παρακαλώ συμπληρώστε)

- Πιστεύετε ότι μια τέτοια κίνηση έχει πλεονεκτήματα ;
  Ναι Όχι

- Εάν ναι, μπορείτε να αναφέρετε κάποια από αυτά;

- Εάν όχι μπορείτε να αναφέρετε γιατί;

- Παρακάτω ακολουθεί μια λίστα με ορισμένα ενδεικτικά πλεονεκτήματα που προκύπτουν από την ανάθεση της ασφάλειας ενός δικτύου σε τρίτους.

1. Η ανάθεση της ασφάλειας του δικτύου σας σε κάποια άλλη εταιρεία μπορεί να αποδεσμεύσει το δικό σας προσωπικό
2. Το κόστος θα μειωθεί αισθητά
3. Το δίκτυο θα ελέγχετε 24 ώρες τη μέρα, 7 ημέρες την εβδομάδα, 365 ημέρες το χρόνο
4. Θα είστε πάντα ενημερωμένοι
5. Χρήση των πιο σύγχρονων τεχνολογικών μέσων και εφαρμογών
6. Πολύ λιγότερα περιστατικά θα φτάνουν σε εσάς ελευθερώνοντας το χρόνο σας
7. Περισσότερος ελεύθερος χρόνος σημαίνει μεγαλύτερη προσοχή στο αντικείμενο που αποτελεί τον πυρήνα της επιχείρησης σας
8. Μάθει από τους συνεργάτες της

Ποια από τα παραπάνω θεωρείτε σημαντικά και γιατί

Βιβλιογραφία

[1] "From the World of Security - A Word from the Experts: Why Outsource Security?" , Bruce Schneier, ENISA QUARTERLY, 03/2006, http://www.enisa.eu.int/

[2] "Task Support for Network Security Monitoring.", Stolze, M., R. Pawlitzek and S. Hild, Proceedings ACM SIGCHI 2003 Workshop on System Administrators are Users, too: Designing workspaces for managing Internet-Scale Systems, http://www.cs.berkeley.edu/~mikechen/chi2003-sysadmin/

[3] "Visual Problem-Solving Support for New Event Triage in Centralized Network Security Monitoring: Challenges, Tools and Benefits", Markus Stolze, René Pawlitzek, Andreas Wespi, 2003

[4] "The case for outsourcing", Bruce Schneeir, Supplement to IEEE Computer Magazine, 04/2002, http://csdl2.computer.org/persagen/DLAbsToc.jsp? resourcePath= /dl/mags/co/&toc=comp/mags/co/2005/04/r4toc.xml

[5] "Θεσμικό πλαίσιο και ηλεκτρονικό επιχειρείν στην Ελλάδα-Αλληλεπίδραση και προοπτικές", Τελικό παραδοτέο ομάδας εργασίας Δ1, Επιχειρησιακό πρόγραμμα «Η κοινωνία της πληροφορίας», Αθήνα, Ιούνιος 2003, www.ebusinessforum.gr

[6] "Decision Support: Design outsourcing relationships that yield long-term ROI", Joe Santana, TechRepublic, 2/9/2004, http://articles.techrepublic.com.com/5100-10878-5140217.html

[7] "Outsourcing", Τελικό παραδοτέο ομάδας εργασίας Ε1, Επιχειρησιακό πρόγραμμα «Η κοινωνία της πληροφορίας», Αθήνα, Δεκέμβριος 2003, www.ebusinessforum.gr

[8] Service Level Agreement, 28/12/2004, http://guide.darwinmag.com/technology/outsourcing/sla/index.html

[9] "Security Outsourcing Grabs Hold", Bill Brenner, CIO Decisions Magazine September 2005, www.counterpane.com

[10] "Don't lose control with outsourcing" Daniel Blum, Network World, 14/11/2005, www.networkworld.com

[11] ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management, http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html

[12] "Is security ripe for outsourcing", Jennifer Mears, Network World, 23/08/2004, www.networkworld.com

[13] "Intelligence and Control Services, The new age of information security", MOUNTAIN VIEW, CA. 06/10/2003 www.verisign.com

[14] "A market Driven approach to Healthcare IT", White Paper, Michael F. Corbett, Eclipsys Corporation, International Association of Outsourcing Professionals

[15] "University Hospital", Case Study, www.iss.com

[16] "Achieving network security", White Paper, 22/08/2003, www.att.com/

[17] "Should you outsource your network security", White Paper, 01/04, CIO magazine Volume 6, Number 1

[18] "Managed Network Security Services For Distributed Enterprises", White Paper, www.securepipe.com

[19] "More large companies are turning to service providers to handle their security", George V. Hulme, 26/05/2003, http://www.informationweek.com/story/showArticle.jhtml?articleID=1010023

[20] "Managed Security Services", Διαφήμιση, www.panurgy.com

[21] "Network Outsourcing Market Opportunities, Strategies, and Forecasts, 2005 to 2011", Network outsourcing Brochure, WINTERGREEN RESEARCH, INC.

[22] "Outsourcing 2005", Michael F. Corbett , Fortune 21/03/2005

[23] "Οδηγός για το επιτυχημένο outsourcing", 11/2003, www.ebussinessforum.gr

[24] "The case for outsourcing network security", Διαφήμιση, www.checkpoint.com

[25] "Weigh the risks before outsourcing security", Carl Weinschenk, TechRepublic, 31/3/2003, http://articles.techrepublic.com.com/5100-10878_11-5029745.html

[26] "Outsourcing: The next ten years", Michael F. Corbett, Executive Director, International Association of Outsourcing Professionals (IAOP) 2005, http://www.outsourcingprofessional.org/firmbuilder/articles/34/175/1172/

[27] "Outsourcing 2005, New directions, opportunities and challenges: a roundtable discussion", Cheryl Krivda, Business Week, 2005, www.businessweek.com

[28] "Intrusion Prevention, A Proactive Approach to Network", White Paper, www.verisign.com

[29] "Why enterprises outsource network security", Michael Suby Research Program Manager Stratecast Partners (a division of Frost & Sullivan), White Paper, www.verisign.com

[30] "Ψηφιακό Outsourcing για τεχνολογίες αιχμής με μικρό κόστος", Πρόγραμμα Δικτυωθείτε http://www.go-online.gr/ebusiness/specials/article.html?article_id=883

[31] Ψηφιακό κέντρο έρευνας, http://www.vrc.gr:8080/roadmaps/roadmaps/npd/page.html?page_id=88

[32] "Outsourcing Security Analysis with Anonymized Logs", Jianqing Zhang, Nikita Borisov, William Yurcik 01/09/2006

[33] "Outsourcing Internet Security: Economic Analysis of Incentives for Managed Security Service Providers", Wen Ding, William Yurcik, Xiaoxin Yin, National Center for Supercomputing Applications (NCSA) University of Illinois at Urbana-Champaign, The 1st Workshop on Internet and Network Economics 15-17/12/2005

[34] "Outsourcing Internet Security: The Effect of Transaction Costs on Managed Service Providers", Wen Ding, William Yurcik, National Center for Supercomputing Applications (NCSA), University of Illinois at Urbana-Champaign 18/11/2005

[35] "The Hidden Cost of IT Outsourcing *Sloan Management Rev",* Barthelemy J., Vol.42, No.3, pp. 60-69, 2001.

[36] "A Game Theoretic Economics Framework to understanding the Information Security outsourcing Market", Wen Ding, William Yurcik, National Center for Supercomputing Applications (NCSA), University of Illinois at Urbana-Champaign 10/06/2005

[37] "Outsourcing Network Security Protection: The Smart Option", White Paper, 04/2006, www.lucent.com

[38] "Deutsche Lufthansa AG. VeriSign Delivers Total PKI Certificate Management", Case study, www.verisign.com

[39] Theresa Grant, Security Councel, http://www.csoonline.com/counsel/session20/question2265.html

[40] "Ασφάλεια δικτύων υπολογιστών, Τεχνολογίες και Υπηρεσίες σε περιβάλλοντα Ηλεκτρονικού Επιχειρήν & Ηλεκτρονικής Διακυβέρνησης " Στέφανος Γκρίτζαλης, Σωκράτης Κ.Κάτσικας, Δημήτρη Γκρίτζαλη, Εκδόσεις Παπασωτηρίου, 2003

[41] "Ασφάλεια πληροφοριακών συστημάτων και δικτύων", Γ. Πάγκαλος, Ι. Μαυρίδη, Εκδόσεις Ανικούλα 2002

[42] "CS-02 Integrated Circuit Manufacturer: *Safeguarding a Global Network So Limited Internal Staff Can Focus on Strategic Issues*", Case study, Release v06.05.04 4.0, www.couterpane.com

[43] "CS-01 Regence Group: Maintaining 24/7 Monitoring of a Multi-Platform Network with Limited Internal Resources", Case study, Release v06.05.04 4.0, www.counterppane.com