ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
«ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗΣ ΔΙΟΙΚΗΣΗΣ
ΚΑΙ ΑΣΦΑΛΕΙΑΣ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

Διπλωματική Εργασία

Μεταπτυχιακού Διπλώματος Ειδίκευσης

ΘΕΜΑ:

«Θέματα Ασφάλειας σε Ανοιχτού Κώδικα Πλατφόρμες Ηλεκτρονικών Καταστημάτων»

Ονοματεπώνυμο Σπουδαστή:

Νικόλαος Γ. Λάμπρου, ΜΤΕ/0914

ΝΙΚΟΛΑΟΣ Γ. ΛΑΜΠΡΟΥ

Επιτροπή Κρίσης

Σωκράτης Κάτσικας Καθηγητής	Κώστας Λαμπρινουδάκης Επίκουρος Καθηγητής	Χρήστος Ξενάκης Επίκουρος Καθηγητής
……	……	……..

Επιβλέπων Διπλωματικής: Κώστας Λαμπρινουδάκης, Επίκουρος Καθηγητής

ΠΕΙΡΑΙΑΣ 2012

Περίληψη

Η ραγδαία ανάπτυξη της τεχνολογίας και των επικοινωνιών έχουν καταστήσει το ηλεκτρονικό εμπόριο όχι μόνο εφικτό, αλλά αναγκαίο και εκθετικά αναπτυσσόμενο. Τα λειτουργικά έξοδα έχουν μειωθεί, η ταχύτητα των συναλλαγών έχει αυξηθεί και η αγορά πλέον δεν έχει τους περιορισμούς των φυσικών καταστημάτων. Η εγκαθίδρυση όμως του ηλεκτρονικού εμπορίου ως έναν αποτελεσματικό και πλέον διαδεδομένο τρόπο αγορών, έχει στρέψει την προσοχή των κακόβουλων οντοτήτων προς την εξαπάτηση των χρηστών του ηλεκτρονικού εμπορίου. Στο παρόν κείμενο θα εντοπιστούν οι πρακτικές ασφάλειας που θα πρέπει να εφαρμόζουν τα συστήματα ηλεκτρονικού εμπορίου.

Λέξεις – Κλειδιά
Ηλεκτρονικό εμπόριο, ηλεκτρονικές συναλλαγές, προδιαγραφές ασφάλειας, κύκλος ζωής ασφάλειας, ευαίσθητα δεδομένα

Abstract

The rapid development of technology and communications has established e-commerce not only viable but essential. Operational costs are lowered, transaction speeds are faster and there are no restrains that physical stores carry. The very fact that e-commerce is becoming an effective and popular way of doing business, have attracted the attention of malicious entities who are trying to deceive e-commerce users. Below, several security guidelines that e-commerce systems should adopt, are mentioned.

Keywords

E-commerce, e-transactions, security requirements, security life cycle, sensitive data

Πρόλογος

Η παρούσα διπλωματική εργασία εκπονήθηκε από τον διπλωματούχο Λάμπρου Νικόλαο από τη Χαλκίδα Ευβοίας.
Ευχαριστώ πολύ τον καθηγητή μου Κωνσταντίνο Λαμπρινουδάκη για την στήριξη και την πολύτιμη βοήθεια του καθ' όλη την διάρκεια της συγγραφής της, καθώς και τους καθηγητές μου Σωκράτη Κάτσικα και Χρήστο Ξενάκη για όλα όσα με δίδαξαν τόσο σε προπτυχιακό όσο και σε μεταπτυχιακό επίπεδο. Επίσης, ιδιαίτερη αναφορά θέλω να κάνω στον συμφοιτητή μου Βίλλιο Κωνσταντίνο για την στήριξη του ώστε να καταφέρουμε να αναπτύξουμε την εταιρεία μας και να προσφέρουμε στο χώρο των υπηρεσιών διαδικτύου με τη βοήθεια όλων όσων μας δίδαξε το μεταπτυχιακό μας. Τέλος, ευχαριστώ την οικογένεια μου για την έμπρακτη βοήθεια στα φοιτητικά μου χρόνια. Η παρούσα διπλωματική εργασία αφιερώνεται στη μνήμη της αδερφής μου.

Πειραιάς, Δεκέμβριος 2012

Λάμπρου Νικόλαος
Πτυχιούχος Ψηφιακών Συστημάτων Πανεπιστημίου Πειραιά
Διπλωματούχος Τεχνοοικονομικής Διοίκησης και Ασφάλειας Ψηφιακών Συστημάτων Πανεπιστημίου Πειραιά

Πίνακας Περιεχομένων

Κεφάλαιο 1^{ο} – Το Ηλεκτρονικό Εμπόριο

Δε θα συναντήσει κανείς έναν κοινά αποδεκτό ορισμό για το ηλεκτρονικό εμπόριο στη σχετική βιβλιογραφία, καθώς κατά καιρούς έχουν παρατεθεί πολλοί ορισμοί ανάλογα με την σκοπιά από την οποία εξετάζεται ο όρος ηλεκτρονικό εμπόριο. Με έναν απλό ορισμό, το ηλεκτρονικό εμπόριο είναι η αγοραπωλησία προιόντων και υπηρεσιών μέσω του διαδικτύου, αλλά και κάθε μορφή επιχειρηματικής συναλλαγής που γίνεται με ηλεκτρονικά μέσα.

Συνοψίζοντας, ένας πιθανός ορισμός θα μπορούσε να είναι ο ακόλουθος:

«Το ηλεκτρονικό εμπόριο αποτελεί μια ολοκληρωμένη συναλλαγή που πραγματοποιείται μέσω του διαδικτύου χωρίς να είναι απαραίτητη η φυσική παρουσία των συμβαλλόμενων μερών, δηλαδή του πωλητή και του αγοραστή, οι οποίοι μπορούν να βρίσκονται ακόμα και σε διαφορετικές χώρες. Είναι οποιαδήποτε συναλλαγή που ενέχει διαδικτυακή δέσμευση για αγορά ή πώληση αγαθών και υπηρεσιών, διακίνηση πληροφοριών, υποστήριξη πελατών και πολλές άλλες διαδικασίες και υπηρεσίες που εμπλέκονται στη διαδικασία της αγοραπωλησίας.»

1.1 Πλεονεκτήματα Ηλεκτρονικού Εμπορίου

Τα πλεονεκτήματα του ηλεκτρονικού εμπορίου μπορούν να συνοψιστούν ως εξής: το ηλεκτρονικό εμπόριο αυξάνει τις πωλήσεις και μειώνει τα λειτουργικά έξοδα. Μια επιχείρηση μπορεί να χρησιμοποιήσει το ηλεκτρονικό εμπόριο για να προσεγγίσει πολλές διαφορετικές αγορές ακόμα και αν αυτές είναι διασκορπισμένες γεωγραφικά.

Όπως ακριβώς το ηλεκτρονικό εμπόριο μπορεί να αυξήσει τις ευκαιρίες πώλησης ενός πωλητή, το ίδιο μπορεί να κάνει για τις ευκαιρίες αγοράς ενός αγοραστή. Το ηλεκτρονικό εμπόριο αυξάνει την ταχύτητα και την ευστοχία με την οποία οι επιχειρήσεις ανταλλάσουν πληροφορίες, γεγονός το οποίο μειώνει τα κόστη και για τις δύο πλευρές της συναλλαγής.

Το ηλεκτρονικό εμπόριο δίνει στους αγοραστές μεγαλύτερο εύρος επιλογών σε αντίθεση με το συμβατικό εμπόριο, διότι μπορούν να διαλέξουν από πολλά διάφορα προιόντα και υπηρεσίες από πολλούς διαφορετικούς παροχείς. Επίσης, το ηλεκτρονικό εμπόριο μπορεί να παρέχει προιόντα και υπηρεσίες σε απομακρυσμένες περιοχές που διαφορετικά δε θα ήταν δυνατόν να διοχετευθούν.

1.2 Μειονεκτήματα Ηλεκτρονικού Εμπορίου

Το ηλεκτρονικό εμπόριο, όμως, έχει και μειονεκτήματα. Μερικά αγαθά, όπως για παράδειγμα τα τρόφιμα ή αντικείμενα μεγάλης αξίας όπως είναι τα κοσμήματα, είναι δύσκολο να ελεγχθούν από τον αγοραστή απομακρυσμένα. Επίσης, μερικές φορές είναι δύσκολο να υπολογιστούν τα λειτουργικά κόστη, μιας και το ηλεκτρονικό εμπόριο βασίζεται σε τεχνολογίες που αλλάζουν ραγδαία μέσα στο χρόνο.

Πολλές επιχειρήσεις αντιμετωπίζουν κοινωνικά και νομικά προβλήματα, ενώ οι αγοραστές από τη μεριά τους είναι φοβισμένοι στην ιδέα να χρησιμοποιήσουν τεχνολογίες που δεν είναι εξοικειωμένοι για τις αγορές τους. Αν και γίνονται προσπάθειες ενημέρωσης για την ασφαλή χρησιμοποίηση του ηλεκτρονικού εμπορίου από τους αγοραστές, αυτοί έχουν ενδοιασμούς σχετικά με το πόσο ασφαλές είναι να χρησιμοποιήσουν τους αριθμούς των πιστωτικών τους καρτών στο διαδίκτυο.

Το βασικό εμπόδιο όμως είναι η ασφάλεια. Οι συναλλαγές μεταξύ πωλητών και αγοραστών αποτελούνται από ζήτηση πληροφοριών, ζήτηση εκτιμήσεων κόστους, παραγγελίες, πληρωμές και υποστήριξη μετά την αγορά. Πολλές φορές είναι δύσκολο να διατηρηθεί ο υψηλός βαθμός εμπιστοσύνης για την αυθεντικότητα και εμπιστευτικότητα αυτών των συναλλαγών όταν γίνονται μέσω του διαδικτύου. Η υποκλοπή των συναλλαγών και ιδιαίτερα των αριθμών των πιστωτικών καρτών αλλά και άλλα ευαίσθητα δεδομένα κατά τη διάρκεια που αυτά μεταδίδονται στο διαδίκτυο, συχνά είναι το μεγαλύτερο εμπόδιο για την εμπιστοσύνη του κοινού στο ηλεκτρονικό εμπόριο.

Κεφάλαιο 2^{ο} – Τεχνολογίες Ηλεκτρονικού Εμπορίου

Για να μπορεί να λειτουργήσει και να υπάρξει το ηλεκτρονικό εμπόριο χρειάζονται αρκετές διαφορετικές τεχνολογίες. Η πιο προφανής είναι το διαδίκτυο. Εκτός από αυτό το σύνθετο σύστημα συνδεδεμένων δικτύων χρειάζονται πολλά λογισμικά και μηχανήματα έτσι ώστε να μπορέσει να διατηρηθεί η υποδομή του ηλεκτρονικού εμπορίου. Μερικά παραδείγματα είναι λογισμικά βάσεων δεδομένων, δρομολογητές δικτύου, συσκευές και λογισμικά κρυπτογράφησης και άλλα. Οι μέθοδοι οι οποίες χρησιμοποιούνται έτσι ώστε όλα αυτά τα στοιχεία να συνυπάρξουν και να υποστηρίξουν το ηλεκτρονικό εμπόριο αλλάζουν διαρκώς. Για το λόγο αυτό όλες οι επιχειρήσεις που προσβλέπουν στη χρησιμοποίηση του ηλεκτρονικού εμπορίου πρέπει να προσαρμόζονται συχνά ώστε να καλύπτουν τις ολοένα και αυξανόμενες ανάγκες.

2.1 Χαρακτηριστικά Τεχνολογιών Ηλεκτρονικού Εμπορίου

Παρακάτω αναφέρονται τα χαρακτηριστικά των τεχνολογιών του ηλεκτρονικού εμπορίου.

1. Ευκολία αυτόματων διαδικασιών: Ο αγοραστής μπορεί πλέον εύκολα να χρησιμοποιήσει πολλαπλές αυτόματες μεθόδους πληρωμών. Για παράδειγμα μπορεί να πληρώσει απευθείας με την πιστωτική του κάρτα, να χρησιμοποιήσει υπηρεσίες όπως του Paypal, να μεταφέρει το ποσό από το λογαριασμό του στο λογαριασμό του δικαιούχου μέσω του e-banking, να πληρώσει με αντικαταβολή και άλλα.
2. Αμεσότητα του αποτελέσματος: Οι πληρωμές γίνονται άμεσα μέσω των αυτοματισμών και την ικανότητα των συστημάτων που διαχειρίζονται την πληρωμή και των παρόχων αυτών των συστημάτων να διαχειρίζονται τη διαδικασία σε πραγματικό χρόνο.
3. Ευκολία στην προσβασιμότητα: Πλέον τα υπολογιστικά και τηλεπικοινωνιακά συστήματα και λογισμικά είναι αρκετά φθηνά, έτσι ώστε να μπορούν να τα αποκτήσουν μικρές επιχειρήσεις και ιδιώτες για να προσφέρουν μια σειρά από υπηρεσίες πληρωμών, οι οποίες παλιότερα ήταν διαθέσιμες μόνο σε μεγάλες επιχειρήσεις εν μέσω ιδιωτικών δικτύων.
4. Συνοδευόμενες πληροφορίες: Οι συνοδευόμενες πληροφορίες είναι αυτές, που αν και δεν έχουν να κάνουν απευθείας με τη συναλλαγή, προσφέρουν χρήσιμες πληροφορίες στους αγοραστές και πωλητές. Παλιότερα, οι πληροφορίες αυτές μπορούσαν να πιστοποιηθούν μόνο από τα δύο μέρη μιας συναλλαγής, ενώ με τη χρησιμοποίηση της τεχνολογίας και του ηλεκτρονικού

εμπορίου υπάρχει η ανάγκη εύρεσης μεθόδων που μπορούν να υποστηρίξουν την αυθεντικότητα των συνοδευόμενων πληροφοριών.

5. Νέα επιχειρηματικά μοντέλα: Πλέον δημιουργούνται νέα επιχειρηματικά μοντέλα που έχουν ως στόχο την εκμετάλλευση των νέων τεχνολογιών πληρωμών και συγκεκριμένα να επωφεληθούν από την απομυθοποίηση της εμπιστοσύνης των καταναλωτών στις τράπεζες. Όλες οι επιχειρήσεις που χρησιμοποιούν το ηλεκτρονικό εμπόριο προσπαθούν να κερδίσουν την εμπιστοσύνη του καταναλωτή και να άρουν τους φόβους του ως προς τη χρησιμοποίηση αυτού του εργαλείου.

Κεφάλαιο 3ο – Ευπάθειες και Απειλές Ηλεκτρονικού Εμπορίου

Οι πτυχές ασφάλειας του ηλεκτρονικού εμπορίου μπορούν να εξεταστούν υπό το πρίσμα της διαδρομής από τον καταναλωτή έως τον εξυπηρετητή που φιλοξενεί το σύστημα ηλεκτρονικού εμπορίου. Αναλογιζόμενοι κάθε σύνδεση στην αλυσίδα αυτή, τα αγαθά που πρέπει να προστατευθούν για να διασφαλιστεί το ηλεκτρονικό εμπόριο περιλαμβάνουν τους υπολογιστές των καταναλωτών, τα μηνύματα που ταξιδεύουν στο τηλεπικοινωνιακό κανάλι και τους εξυπηρετητές, λογισμικό και μηχανήματα. Το κανάλι είναι πολύ σημαντικό να προστατευθεί, αλλά αν δεν υπάρχουν μέτρα προστασίας των υπολογιστών και εξυπηρετητών, τότε δεν υπάρχει καμία ασφάλεια.

3.1 Απειλές Καταναλωτών

Μέχρι την εμφάνιση του εκτελέσιμου διαδικτυακού περιεχομένου, οι ιστοσελίδες ήταν κυρίως στατικές. Οι ευπάθειες τότε δεν ήταν πολλές, μιας και το μόνο που έκαναν αυτές οι σελίδες ήταν η εμφάνιση στατικού υλικού και συνδέσμων, όμως πλέον η κατάσταση έχει αλλάξει με τη χρήση του ενεργού περιεχομένου.

- Ενεργό Περιεχόμενο: Το ενεργό περιεχόμενο αναφέρεται σε προγράμματα που έχουν ενσωματωθεί διαφανώς στις ιστοσελίδες και προκαλούν μια δράση. Το ενεργό περιεχόμενο μπορεί να εμφανίζει κινούμενα γραφικά, αναπαραγωγή ήχου ή να εκτελεί διαδικτυακά προγράμματα δημιουργίας φύλλων εργασίας. Το πιο σύνηθες παράδειγμα στο ηλεκτρονικό εμπόριο είναι η δυνατότητα του χρήστη να προσθέσει κάποια προιόντα που θα ήθελε να αγοράσει στο μέλλον στη λίστα επιθυμίας του, έτσι ώστε να μπορεί να δει το τελικό ποσό μαζί με φόρους, διαχειριστικά κόστη και κόστη μεταφοράς. Οι πιο γνωστές τεχνολογίες για το σκοπό αυτό είναι τα Java Applets, ActiveX Controls, JavaScript και VBScript.

  Καθώς το ενεργό περιεχόμενο είναι ενσωματωμένο στις ιστοσελίδες, μπορεί να είναι εντελώς αόρατο στον χρήστη που περιηγείται στην ιστοσελίδα. Αυτό σημαίνει ότι κάποιος μπορεί να ενσωματώσει κακόβουλο ενεργό περιεχόμενο, μια τεχνική που αποκαλείται Δούρρειος Ίππος, με την οποία καθίσταται δυνατή η αυτόματη εκτέλεση κακόβουλου κώδικα που έχει ως σκοπό να προκαλέσει ζημιά.

  Η ενσωμάτωση ενεργού περιεχομένου σε ιστοσελίδες που σχετίζονται με το ηλεκτρονικό εμπόριο επιφέρει προβλήματα στην ασφάλεια των συστημάτων. Κακόβουλα λογισμικά μπορούν να συλλέξουν πληροφορίες όπως οι αριθμοί πιστωτικών καρτών, ονόματα χρηστών και κωδικοί οι οποίοι συχνά

αποθηκεύονται προσωρινά σε αρχεία cookies. Τα cookies χρησιμοποιούνται ώστε να θυμάται το σύστημα ηλεκτρονικού εμπορίου τις επιλογές του χρήστη, όπως το όνομα χρήστη, οι κωδικοί και τα περιεχόμενα της παραγγελίας. Κακόβουλο ενεργό περιεχόμενο που δρα με τη μορφή cookie μπορεί να υποκλέψει τα περιεχόμενα των αρχείων στη μεριά του καταναλωτή ή ακόμα και να σβήσει ορισμένα από αυτά.

- Κακόβουλο Λογισμικό: Παραδείγματα κακόβουλου λογισμικού είναι οι ιοί, τα σκουλήκια (worms) και οι Δούρριοι Ίπποι. Ο Δούρριος Ίππος είναι ένα πρόγραμμα το οποίο μπορεί να εκτελεί μια χρήσιμη διαδικασία, αλλά να έχει μη προβλέψιμο αποτέλεσμα. Ο ιός είναι ένα κομμάτι κώδικα το οποίο αντιγράφεται σε ήδη υπάρχονται εκτελέσιμα αρχεία και προκαλούν ανεπιθύμητα αποτελέσματα.

- Πλαστοπροσωπεία Εξυπηρετητή: Η πλαστοπροσωπεία εξαπατά το θύμα ώστε να πιστεύει ότι επικοινωνεί με τη σωστή οντότητα. Αν για παράδειγμα ένας χρήστης προσπαθεί να συνδεθεί σε έναν εξυπηρετητή, αλλά στην πραγματικότητα συνδέεται σε έναν άλλον ο οποίος λέει ότι είναι ο σωστός, τότε ο χρήστης έχει εξαπατηθεί. Οι επιθέσεις αυτές μπορεί να είναι παθητικές, δηλαδή ο κακόβουλος χρήστης να μην προσπαθεί να αυθεντικοποιήσει τον καταναλωτή αλλά να προκαλεί μια κατάσταση όπου ο καταναλωτής να μην μπορεί να συνδεθεί, αλλά τις περισσότερες φορές η επίθεση είναι ενεργητική, δηλαδή ο κακόβουλος χρήστης προσπαθεί με διάφορες «απαντήσεις» να κοροιδέψει τον καταναλωτή σχετικά με την πραγματική του ταυτότητα.

3.2 Απειλές Τηλεπικοινωνιακού Καναλιού

Το διαδίκτυο υπηρετεί ως μια ηλεκτρονική αλυσίδα που συνδέει τον καταναλωτή με τον εξυπηρετητή που φιλοξενεί το σύστημα ηλεκτρονικού εμπορίου. Τα μηνύματα που διοχετεύονται στο διαδίκτυο ακολουθούν ένα τυχαίο μονοπάτι από τον πηγαίο κόμβο στον κόμβο προορισμού και για το λόγο αυτό διέρχονται από έναν μεγάλο αριθμό ενδιάμεσων υπολογιστών στο δίκτυο πριν καταλήξουν στον προορισμό τους. Είναι προφανές ότι είναι αδύνατον να διασφαλιστεί ότι κάθε υπολογιστής μέσω του οποίου διέρχονται αυτά τα μηνύματα είναι ασφαλής και μη εχθρικός.

- Απειλές Εμπιστευτικότητας: Εμπιστευτικότητα είναι η αποφυγή της μη εξουσιοδοτημένης αποκάλυψης πληροφορίας. Ένα παράδειγμα παραβίασης της εμπιστευτικότητας είναι όταν ένας χρήστης συνδεθεί σε μια ιστοσελίδα η οποία περιέχει πεδία για το όνομα, τη διεύθυνση, την ηλεκτρονική διεύθυνση και άλλα. Όταν ο χρήστης συμπληρώσει τα πεδία και αποστείλει τη φόρμα τα δεδομένα στέλνονται στον εξυπηρετητή για επεξεργασία. Μια δημοφιλής μέθοδος αποστολής δεδομένων σε έναν εξυπηρετητή είναι η εισαγωγή τους

στο τέλος του συνδέσμου (url) μέσω HTTP ερωτήματος. Αν τώρα ο χρήστης για κάποιο λόγο δεν περιμένει για την απάντηση του εξυπηρετητή αλλά φύγει από την ιστοσελίδα και επισκευθεί μια άλλη μπορεί να συμβεί το εξής. Η δεύτερη ιστοσελίδα μπορεί να συλλέγει δεδομένα για διαφημιστικούς λόγους, όπως για παράδειγμα ο σύνδεσμος (url) από τον οποίο προήλθε ο επισκέπτης. Με τον τρόπο αυτό, οι κάτοχοι της δεύτερης ιστοσελίδας έχουν πλέον και τα προσωπικά στοιχεία του χρήστη που στο προηγούμενο βήμα πληκτρολόγησε στη φόρμα σύνδεσης της πρώτης ιστοσελίδας.

- Απειλές Ακεραιότητας: Μια απειλή ακεραιότητας υπάρχει όταν μια μη εξουσιοδοτημένη οντότητα μπορεί να μεταποιήσει μια σειρά από πληροφορίες ενός μηνύματος. Για παράδειγμα, υπάρχουν καταστάσεις όπου κακόβουλες οντότητες μπορούν να μιμηθούν γνωστές ιστοσελίδες (defacing). Με τον τρόπο αυτό οι χρήστες εξαπατούνται και καταχωρούν ευαίσθητα και προσωπικά δεδομένα σε ιστοσελίδες που ισχυρίζονται ότι είναι οι νόμιμες, αλλά δεν είναι. Αυτό μπορεί να γίνει για παράδειγμα με την χρησιμοποίηση κάποιας τρύπας ασφάλειας σε έναν εξυπηρετητή ονοματοδοσίας (DNS server) έτσι ώστε οι κακόβουλες οντότητες να αντικαταστήσουν τη διεύθυνση της ιστοσελίδας τους με αυτήν της νόμιμης, εξαπατώντας έτσι τους χρήστες. Οι απειλές ακεραιότητας μπορούν να μεταποιήσουν οικονομικά δεδομένα προκαλώντας έτσι σοβαρές επιπτώσεις στους καταναλωτές και στις επιχειρήσεις.

- Απειλές Διαθεσιμότητας: Η σημασία ύπαρξης των απειλών διαθεσιμότητας, που είναι γνωστές και ως απειλές καθυστέρησης ή άρνησης, είναι να διακόπτουν την ομαλή διαδικασία υπολογιστικής επεξεργασίας ή να αρνούνται την επεξεργασία ολοκληρωτικά. Αν λοιπόν ένα σύστημα ηλεκτρονικού εμπορίου υποστεί μια τέτοια επίθεση, αυτό θα έχει σοβαρά αρνητικά αποτελέσματα, καθώς θα προκληθεί η δυνανασχέτιση των χρηστών και τελικά τη φυγή τους από την ιστοσελίδα.

3.3 Απειλές Εξυπηρετητή Ηλεκτρονικού Εμπορίου

Ο εξυπηρετητής που φιλοξενεί το σύστημα ηλεκτρονικού εμπορίου είναι το τρίτο κομμάτι της αλυσίδας που συνδέει τον χρήστη με το σύστημα. Οι εξυπηρετητές έχουν ευπάθειες που μπορούν να εκμεταλευθούν οποιοιδήποτε κατέχουν τις γνώσεις και θέλουν να προκαλέσουν καταστροφή ή παράνομα να συλλέξουν ευαίσθητα και προσωπικά στοιχεία.

- Απειλές Εξυπηρετή Διαδικτύου: Το λογισμικό των συμβατικών εξυπηρετητών έχει σχεδιαστεί έτσι ώστε να απαντάει σε HTTP ερωτήματα. Όσο περισσότερο σύνθετο είναι το λογισμικό, τόσο μεγαλύτερη είναι η πιθανότητα

να περιέχει λάθη στον κώδικα (bugs) και τρύπες ασφάλειας τα οποία προκαλούν την ανεπιθύμητη απόκτηση πρόσβασης σε κακόβουλες οντότητες.

- Εξυπηρετητές Ηλεκτρονικού Εμπορίου: Οι εκυπηρετητές ηλεκτρονικού εμπορίου δρουν όπως οι απλοί εξυπηρετητές, απαντούν δηλαδή σε HTTP ερωτήματα αλλά επίσης και σε ερωτήματα από σενάρια CGI. Επίσης, χρησιμοποιούνται μια σειρά από λογισμικά, όπως ένας FTP εξυπηρετητής, ένας εξυπηρετητής ηλεκτρονικών μηνυμάτων, ένας εξυπηρετής για τη διαχείριση των συνδέσεων των χρηστών και λειτουργικά συστήματα. Όλα αυτά τα λογισμικά μπορεί να εμπεριέχουν τρύπες ασφάλειας και προγραμματιστικά λάθη τα οποία μπορει να εκμεταλευθούν οι κακόβουλοι χρήστες ώστε να αποκτήσουν πρόσβαση.

- Απειλές Βάσεων Δεδομένων: Τα συστήματα ηλεκτρονικού εμπορίου αποθηκεύουν τα δεδομένα των χρηστών τους σε βάσεις δεδομένων που βρίσκονται στον εξυπηρετητή. Αυτά τα δεδομένα είναι προσωπικά και συνήθως ευαίσθητα, οπότε οποιαδήποτε μη εξουσιοδοτημένη διαρρόη ή αλλαγή προκαλεί μεγάλη ζημιά στις επιχειρήσεις αλλά και στους ίδιους τους χρήστες. Ακόμη και σήμερα πολλές βάσεις δεδομένων αποθηκεύουν τα ονόματα χρηστών και κωδικούς πρόσβασης με μη ασφαλή τρόπο, ακόμα και μη κρυπτογραφημένα.

- Απειλές Διεπαφής Κοινής Πύλης (CGI): Η διεπαφή CGI χρησιμεύει στην μεταφορά των δεδομένων από έναν εξυπηρετητή σε άλλα προγράμματα, όπως είναι μια βάση δεδομένων. Τα CGI είναι προγράμματα και αυτό σημαίνει ότι αν δε χρησιμοποιηθούν σωστά, τότε μπορούν να προκαλέσουν προβλήματα ασφάλειας. Αν αποκτηθεί πρόσβαση σε αυτά τα προγράμματα, τότε μπορεί να προκληθούν σοβαρά προβλήματα όπως η απενεργοποίηση του συστήματος, η εκτέλεση άλλων προγραμμάτων που μπορεί να σβήσουν διάφορα αρχεία καθώς και η αποκάλυψη εμπιστευτικής πληροφορίας όπως είναι τα ονόματα χρηστών και οι κωδικοί πρόσβασης.

- Αποκάλυψη Κωδικών Πρόσβασης: Η πιο απλή απειλή εναντίον συστημάτων που βασίζονται σε κωδικούς πρόσβασης είναι το να μαντεύει κανείς αυτούς τους κωδικούς. Υπάρχουν διαδικασίες κατά τις οποίες αυτή η διαδικασία γίνεται αυτόματα (brute force attack, dictionary attack) και στοχεύουν για κωδικούς που συνήθως είναι αδύναμοι, δηλαδή περιέχουν μόνο λέξεις και όχι σύμβολα και αριθμούς.

Κεφάλαιο 4^{ο} – Εφαρμογή Ασφάλειας Ηλεκτρονικού Εμπορίου

Στο κεφάλαιο αυτό θα δούμε τις βασικές στρατηγικές πτυχές που χρειάζεται να ακολουθήσει ένας οργανισμός που πρόκειται να αναπτύξει ένα σύστημα ηλεκτρονικού εμπορίου ώστε αυτό να είναι επιτυχημένο. Οι διάφορες σουίτες ασφάλειας όπως είναι τα κρυπτογραφημένα μηνύματα ηλεκτρονικού ταχυδρομείου ή τα ψηφιακά πιστοποιητικά παίζουν σημαντικό ρόλο στην προστασία των πολίτιμων δεδομένων αλλά για να είναι αποδοτική η ασφάλεια πρέπει να σχεδιαστεί και εφαρμοστεί σαν σύνολο. Θα μπορούσαμε να πούμε ότι τα βήματα είναι η σχεδίαση του μοντέλου του συστήματος, η αναγνώριση των στοιχείων που χρειάζονται ασφάλεια και η πιστοποίηση ότι τα στοιχεία αυτά θα είναι ασφαλή μετά από επιθέσεις. Η σχεδιασή του συστήματος και η αναγνώριση των στοιχείων προς προστασία είναι εφικτά, αλλά είναι αδύνατον να προβλευθούν όλες οι πιθανές ευπάθειες του συστήματος. Για το λόγο αυτό είναι καλό να γνωρίζουμε ότι δεν υπάρχει ο όρος απόλυτη ασφάλεια. Η ασφάλεια των συστημάτων πρέπει να αντιμετωπίζεται σαν μια διαρκής διαδικασία και όχι σαν ένα προιόν που δημιουργήθηκε μια φορά και έχει αφεθεί χωρίς επίβλεψη.

4.1 Κύκλος Ζωής Ασφάλειας

Είναι σημαντικό να γνωρίζουμε ότι η ασφάλεια συστημάτων όπως του ηλεκτρονικού εμπορίου, είναι μια διαδικασία δυναμική και όχι στατική. Χρειάζεται, λοιπόν, οι επιχειρήσεις να αναλύουν, σχεδιάζουν, επιβλέπουν και να προσαρμόζονται στις νέες ανάγκες διαρκώς. Παρακάτω αναλύονται τα βήματα αυτού του κύκλου ζωής.

- Προδιαγραφές Ασφάλειας και Ανάλυση Ρίσκου: Αυτό είναι το πρώτο βήμα στον κύκλο ζωής της ασφάλειας στο οποίο γίνεται συλλογή στοιχείων που αφορούν τα αγαθά της επιχείρησης που χρειάζονται προστασία, η ανάλυση τους ως προς το βαθμό επικινδυνότητας, η αναγνώριση των υπηρεσιών που απαιτούνται για την πρόσβαση αυτών των αγαθών και η πολιτική πρόσβασης των υπηρεσιών αυτών.

- Προδιαγραφή Πολιτικής Ασφάλειας: Σε αυτό το βήμα χρησιμοποιούνται τα ευρήματα από τις προδιαγραφές ασφάλειας και της ανάλυσης ρίσκου ως πρώτη ύλη ώστε να σχηματιστεί ένα σύνολο από πολιτικές ασφάλειας του ηλεκτρονικού εμπορίου. Συνήθως οι πολιτικές ασφάλειας αυτές, είναι γενικές οδηγίες προς τους τελικούς χρήστες και για το λόγο αυτό δεν περιέχουν τεχνικά χαρακτηριστικά του συστήματος και των τεχνολογιών και υπηρεσιων

που αυτό χρησιμοποιεί, πληροφορίες που θα μπορούσαν να φανούν χρήσιμες σε κακόβουλες οντότητες.

- Προδιαγραφή Δομής Ασφάλειας: Στο βήμα αυτό αναλύονται οι γενικές προδιαγραφές ασφάλειας και οι προδιαγραφες των πολιτικών ασφάλειας ώστε να δημιουργηθεί μια λίστα από εργαλεία ασφάλειας που χρειάζονται για την προστασία των αγαθών της επιχείρησης. Επίσης, η προδιαγραφή της δομής της ασφάλειας, προσφέρει μια γενική εικόνα για τον τρόπο χρήσης και την αναγκαιότητα των εργαλείων ασφάλειας που θα χρησιμοποιηθούν.

- Εφαρμογή Δομής Ασφάλειας: Στο βήμα αυτό η επιχειρήση προχωράει την εγκατάσταση και ρύθμιση των επιλεγμενων στο προηγούμενο βήμα εργαλείων ασφάλειας και γενικότερα της δομής ασφάλειας στο σύστημα του ηλεκτρονικού εμπορίου.

- Δοκιμές επί της Ασφάλειας: Σε αυτό το βήμα ο οργανισμός προχωράει στην πραγματοποίηση αρκετών δοκιμών ώστε να προσδιοριστεί η αποτελεσματικότητα της δομής ασφάλειας, η χρηστικότητα των μηχανισμών ελέγχου πρόσβασης αλλά και γενικότερα των μηχανισμών διαχείρισης του περιεχομένου και να δοκιμαστεί η αντοχή του συστήματος σε γνωστές ευπάθειες και απειλές.

- Επικύρωση Προδιαγραφών: Στο βήμα αυτό αναλύεται ο βαθμός στον οποίο έχουν υλοποιηθεί οι προδιαγραφές ασφάλειας του συστήματος ηλεκτρονικού εμπορίου του οργανισμού σε σχέση με τις αντίστοιχες πολιτικές ασφάλειας και της υλοποιημένης δομής ασφάλειας. Όταν αλλάζουν οι στόχοι και το διαχειριστικό περιβάλλον του οργανισμού καθώς και οι χρησιμοποιούμενες τεχνολογίες, τότε χρειάζονται νέες προδιαγραφές ασφάλειας και κατά συνέπεια η ενεργοποίηση του κύκλου ζωής της ασφάλειας από την αρχή του.

4.2 Προδιαγραφές Ασφάλειας

Όπως αναφέρθηκε παραπάνω, αυτό είναι το βήμα στο οποίο αναγνωρίζονται οι ανάγκες ασφάλειας που έχει μια επιχείρηση. Αυτές οι ανάγκες προκύπτουν από την αναγκαιότητα για την προστασία των παρακάτω θεμελιωδών στοιχείων ασφάλειας. Η σειρά με την οποία αναφέρονται δεν αντιστοιχούν σε καμία περίπτωση στο βαθμό αναγκαιότητας για την προστασία τους.

- Αυθεντικοποίηση: Η αυθεντικοποίηση είναι η δυνατότητα παραδοχής ότι μια ηλεκτρονική επικοινωνία έχει προέλθει πραγματικά από την οντότητα που έπρεπε. Στο ηλεκτρονικό εμπόριο η καλύτερη άμυνα για τέτοια προβλήματα είναι τα ψηφιακά πιστοποιητικά τα οποία έχουν προέλθει από έμπιστες οντότητες. Οποιοσδήποτε μπορεί να εκδώσει ψηφιακά πιστοποιητικά για τον εαυτό του, όμως οι έμπιστες οντότητες ζητάνε στοιχεία για την πραγματική ταυτότητα του παραλήπτη του πιστοποιητικού και ερευνούν την εγκυρότητα αυτών των στοιχείων προτού προβούν στην έκδοση του ψηφιακού πιστοποιητικού.

- Ιδιωτικότητα: Στο ηλεκτρονικό εμπόριο η ιδιωτικότητα είναι η δυνατότητα διασφάλισης ότι η πληροφορία είναι προσπελάσιμη και μπορεί να μεταβληθεί μόνο από εξουσιοδοτημένους χρήστες. Γενικά, αυτό επιτυγχάνεται με την κρυπτογράφηση. Τα ευαίσθητα δεδομένα, όπως είναι οι αριθμοί πιστωτικών καρτών, κρυπτογραφούνται πριν μεταδοθούν μέσω του διαδικτύου. Πληροφορίες που έχουν κρυπτογραφηθεί με δυνατό αλγόριθμο και μήκος κλειδιού μπορεί να αναχαιτιστούν από κακόβουλες οντότητες αλλά δεν μπορούν να αποκρυπτογραφηθούν μέσα σε εύλογο χρονικό διάστημα. Πάλι, τα ψηφιακά πιστοποιητικά μπορούν να χρησιμοποιηιούν εδώ για την εγκατάσταση μιας ασφαλούς σύνδεσης (HTTPS) με έναν εξυπηρετητή. Επίσης, για μεγαλύτερη ασφάλεια, τα ευαίσθητα δεδομένα μπορούν να παραμένουν σε κρυπτογραφημένη μορφή ακόμα και όταν απλά φυλάσσονται σε κάποια βάση δεδομένων.

- Εξουσιοδότηση: Οι μηχανισμοί εξουσιοδότησης δίνουν τη δυνατότητα σε έναν άνθρωπο ή ένα υπολογιστικό σύστημα να αποφασίσουν αν κάποιος έχει το δικαίωμα να ζητήσει ή να εποδεχτεί μια ενέργεια ή μια πληροφορία. Η εξουσιοδότηση είναι άρρηκτα συνδεδεμένη με την αυθεντικοποίηση. Αν ένα σύστημα μπορεί με ασφάλεια να πιστοποιήσει ότι μια ζήτηση για μια πληροφορία ή μια υπηρεσία έχει προέλθει από γνωστή οντότητα, τότε το σύστημα μπορεί να ανατρέξει στους εσωτερικούς κανόνες του ώστε να διαπιστωθεί αν αυτή η οντότητα έχει επαρκή δικαιώματα για να προχωρήσει η ενέργεια η οποία ζητήθηκε. Για παράδειγμα αν ένας εξυπηρετητής διαθέτει πόρους που είναι περιορισμένης και ελεγχόμενης πρόσβασης, τότε μπορεί να ζητήσει από τον χρήστη ένα ψηφιακό πιστοποιητικό από τον φυλλομετρητή του ώστε να πιστοποιηθεί ο χρήστης και να αποφασιστεί αν πρέπει να λάβει πρόσβαση.

- Ακεραιότητα: Ακεραιότητα της πληροφορίας υπάρχει όταν διασφαλίζεται ότι η επικοινωνία δεν έχει αλλαχθεί ή τροποποιηθεί. Όταν κάποιος παραλαμβάνει ευαίσθητες πληροφορίες στο διαδίκτυο, επιθυμεί όχι μόνο να διασφαλίσει ότι προέρχονται από τον αναμενόμενο αποστολέα (αυθεντικοποίηση) αλλά και ότι οι πληροφορίες δε θα έχουν αναχαιτιστεί από κακόβουλη οντότητα κατά

τη μετάδοση και δε θα έχουν τροποποιηθεί. Ένας τρόπος ο οποίος χρησιμοποιείται για αυτόν τον λόγο είναι τα ψηφιακά πιστοποιητικά που υπογράφουν τα μηνύματα. Για παράδειγμα ένας χρήστης υπογράφει το ηλεκτρονικό του μήνυμα και το στέλνει στον παραλήπτη. Η υπογραφή του αποστολέα περιλαμβάνει μια ακολουθία χαρακτήρων, μοναδική για αυτό το μήνυμα. Όταν ο παραλήπτης ανοίξει το μήνυμα τότε το λογισμικό του θα δημιουργήσει μια νέα ακολουθία χαρακτήρων για το μήνυμα αυτό και τη συγκρίνει με αυτή που είχε έρθει στο αρχικό μήνυμα. Ακόμα και ένας χαρακτήρας να είχε αλλάξει από το αρχικό μήνυμα, τότε οι δύο αυτές ακολουθίες δε θα ταίριαζαν και το λογισμικό του παραλήπτη θα τον ενημέρωνε ότι το αρχικό μήνυμα είχε αλοιωθεί.

- Μη Αποποίηση: Η μη αποποίηση είναι η δυνατότητα διασφάλισης ότι όταν κάποιος αιτείται και εκτελεί μια ενέργεια, να μην μπορεί να ισχυριστεί ότι δεν την έκανε ποτέ. Για παράδειγμα η μη αποποίηση δίνει το δικαίωμα σε κάποιον να αποδείξει νομικά ότι μια οντότητα έστειλε ένα συγκεκριμένο email ή εκτέλεσε μια αγορά σε μια ιστοσελίδα. Οι ψηφιακές υπογραφές δίνουν και εδώ τη λύση, καθώς ο χρήστης που έχει εγκατεστημένη μια ψηφιακή υπογραφή μπορεί να κάνει κινήσεις που ισοδυναμούν με την χρήση της κανονικής ιδιόχειρης υπογραφής του.

4.3 Πολιτκή Ασφάλειας

Μια πολιτική ασφάλειας είναι εξαιρετικά χρήσιμη καθώς ορίζει τις προδιαγραφές για κάθε πτυχή του συστήματος (άνθρωποι, τεχνολογία, νομικά ζητήματα) και πως αυτά αλληλεπιδρούν μεταξύ τους. Η πολιτική ασφάλειας μιας επιχείρησης ορίζει τη θέση της ως προς την προστασία των φυσικών και ηλεκτρονικών αγαθών της. Ξεχωρίζει τα φυσικά και τα αγαθά του πνεύματος που είναι πολύτιμα για τη συνεχόμενη επιτυχία της εταιρείας και ορίζει πως αυτά θα πρέπει να προστατευθούν.

Μια πολιτική ασφάλειας μπορεί να συμπεριλάβει ζητήματα όπως:

- Σε τι τύπους υπηρεσιών μπορούν να έχουν πρόσβαση οι χρήστες (HTTP, FTP, SMTP)
- Τι διαβαθμίσεις ασφάλειας υπάρχουν σχετικά με τις πληροφορίες της επιχείρησης και ποιες από αυτές τις βαθμίδες πρέπει να υποστούν κρυπτογράφηση πριν από τη μετάδοση τους
- Τι πληροφορίες πελατών αποθηκεύονται, πόσο ευαίσθητες είναι αυτές και πως προβλέπεται να προστατευθούν

- Ποιοί υπάλληλοι έχουν απομακρυσμένη πρόσβαση στο εταιρικό δίκτυο
- Ρόλοι και ευθύνες προισταμένων και υπαλλήλων στην εφαρμογή και τήρηση της πολιτικής ασφάλειας
- Πως θα αντιμετωπιστούν τυχόν παραβιάσεις ασφάλειας
- Ποιος έχει πρόσβαση στον εταιρικό εξυπηρετητή
- Ποια είναι η διαδικασία ώστε να αποφασιστεί σε ποιον θα δοθεί πρόσβαση

Η πολιτική ασφάλειας θα πρέπει να περιέχει λεπτομέρεις ως προς το πως θα εφαρμοστεί και πως δημιουργούνται προσωπικές ευθύνες για την εφαρμογή και τήρηση της. Επίσης, για να είναι αποτελεσματική, χρειάζεται να δοκιμάζεται και αναθεωρείται συχνά ώστε να κρίνονται τα μέτρα ασφάλειας ως προς την καταλληλότητα τους. Αυτό συμβαίνει γιατί υπάρχουν ραγδαίες αλλαγές στην τεχνολογία και μπορεί να υπάρχουν και αλλαγές στον τρόπο λειτουργίας της επιχείρησης, ζητήματα τα οποία μπορεί να έχουν επιπτώσεις πάνω στην εφαρμοσμένη ασφάλεια.

4.4 Δομή Ασφάλειας

Η δομή ασφάλειας είναι η εφαρμογή της πολιτικής ασφάλειας, δηλαδή οι τεχνολογίες που επιλέχθηκαν για την προστασία του συστήματος ηλεκτρονικού εμπορίου καθώς και οι κανόνες με τους οποίους λειτουργούν αυτές οι τεχνολογίες. Μερικά παραδείγματα περιλαμβάνουν:

- Εφαρμογή «παλαίωση» και λήξη των κωδικών πρόσβασης
- Εφαρμογή κανόνων για την πολυπλοκότητα των κωδικών πρόσβασης
- Φιλτράρισμα απαγορευμένων εξερχόμενων συνδέσεων από το τείχος προστασίας
- Καταγραφή σε αρχείο κάθε φυσικής πρόσβασης στα δωμάτια που βρίσκονται οι εξυπηρετητές
- Εφαρμογή κανόνων ως προς το ποιος ενημερώνει και διαβάζει τα αρχεία καταγραφής και κάθε πότε ελέγχονται οι αναφορές από το τείχος προστασίας

Τελικά, όμως, για να είναι αποτελεσματική η δομή ασφάλειας, πρέπει να εφαρμοστεί από όλους. Θα πρέπει να υπάρχουν τιμωρίες για τυχόν παραβιάσεις της πολιτικής ασφάλειας από του εργαζόμενους και συνεργάτες της επιχείρησης.

4.5 Δοκιμές Ασφάλειας

Η ανάγκη για δοκιμές στην ασφάλεια ενός οργανισμού προκύπτει από δύο βασικούς παράγοντες. Ο πρωταρχικός παράγοντας είναι ότι είναι πάρα πολύ σημαντικό να μετριέται ο βαθμός στον οποίο η δομή ασφάλειας εφαρμόζει την πολιτική ασφάλειας και τις προδιαγραφές ασφάλειας του οργανισμού. Η εφαρμογή της δομής ασφάλειας χρειάζεται ανθρώπινες παρεμβάσεις, οπότε είναι σημαντικό να γίνονται έλεγχοι για να μηδενιστούν οι περιπτώσεις ανθρώπινου λάθους. Ο δεύτερος παράγοντας είναι ο βαθμός ευπάθειας της εφαρμοσμένης δομής ασφάλειας σε νέες απειλές και κινδύνους. Τα τελευταία χρόνια παρατηρείται εκθετική αύξηση στο ρυθμό εμφάνισης νέων απειλών και για το λόγο αυτό η ασφάλεια ενός οργανισμού θα πρέπει να δοκιμάζεται και να αναθεωρείται για να μπορεί να αντιμετωπίσει τις νέες απειλές. Οι δοκιμές ασφάλειας μπορούν να αποτελούνται από:

- Επαλήθευση των προδιαγραφών ασφάλειας όπως είναι η τοποθεσία των αγαθών, ο μηχανισμός ελέγχου πρόσβασης για τα αγαθά, υπάρχουσες υπηρεσίες συστήματος και οι μηχανισμοί ελέγχου πρόσβασης αυτών, η συνδεσιμότητα μεταξύ της επιχείρησης και μεταξύ της επιχείρησης και του εξωτερικού κόσμου

- Επαλήθευση των ρυθμίσεων των εργαλείων ασφάλειας που επιλέχθηκαν στη δομή ασφάλειας

- Επαλήθευση για οποιοδήποτε κενό μεταξύ της προτεινόμενης δομής ασφάλειας και της εφαρμοσμένης δομής ασφάλειας

- Επαλήθευση των περιορισμών της προτεινόμενης δομής ασφάλειας ως προς γνωστές ευπάθειες

Διακρίνουμε λοιπόν δύο πτυχές στις δοκιμές ασφάλειας, ο έλεγχος συμμόρφωσης και οι δοκιμές διείσδυσης. Στον έλεγχο συμμόρφωσης ελέγχεται αν η δομή ασφάλειας που έχει εφαρμοστεί ταυτίζεται με την πολιτική ασφάλειας του οργανισμού. Στις δοκιμές διείσδυσης ελέγχεται αν η υπάρχουσα δομή ασφάλειας ενός οργανισμού είναι επαρκής για την αντιμετώπιση των πιθανών απειλών ασφάλειας. Για το σκοπό αυτό υπάρχουν πάρα πολλά αυτοματοποιημένα ή μερικώς αυτοματοποιημένα εργαλεία ασφάλειας. Τα εργαλεία αυτά προσπαθούν να διεισδύσουν στο δίκτυο του οργανισμού και δημιουργούν αναφορές για τις ευπάθειες που υπάρχουν σε αυτό. Τα ευρήματα του σταδίου αυτού χρησιμοποιούνται για την αναβάθμιση της δομής ασφάλειας και πολιτικής ασφάλειας του οργανισμού. Στη συνέχεια, η φάση των δοκιμών ξεκινάει ξανά, πράγμα που μας κάνει να καταλάβουμε ότι όλες οι διαδικασίες για την ασφάλεια ενός οργανισμού είναι δυναμικές και πρέπει να επαναλαμβάνονται ανα τακτά χρονικά διαστήματα.

Συμπεράσματα

Είναι σίγουρο ότι το ηλεκτρονικό εμπόριο αναπτύσσεται με ραγδαίους ρυθμούς. Πολλές τεχνολογίες έχουν συνυπάρξει ώστε να μπορέσουν τα συστήματα ηλεκτρονικού εμπορίου να αναπτυχθούν και να χαρίσουν τόσο στους τελικούς χρήστες όσο και στις επιχειρήσεις που τα διατηρούν μια λειτουργική αλλά προπαντός ασφαλή εμπειρία αγοραπωλησιών. Για το λόγο αυτό είναι επιτακτική η ανάγκη ανάπτυξης ολοκληρωμένου σχεδίου ασφάλειας για τα συστήματα αυτά. Τα σχέδια αυτά είδαμε ότι βασίζονται στη λογική του κύκλου ζωής. Αυτό σημαίνει ότι υπάρχουν συγκεκριμένα βήματα και στάδια τα οποία πρέπει να γίνονται με τη σωστή σειρά, ώστε να επιτευχθεί το καλύτερο αποτέλεσμα ως προς την ασφάλεια. Τέλος, χρειάζεται συνεχής έλεγχος και παρακολούθηση έτσι ώστε να βελτιώνονται συνεχώς οι μηχανισμοί και οι κανόνες ασφάλειας. Συνοπτικά, λοιπόν, για να πετύχει ένα σύστημα ηλεκτρονικού εμπορίου θα πρέπει να ακολουθηθούν τα εξής βήματα:

- Προδιαγραφές Ασφάλειας και Ανάλυση Ρίσκου
- Προδιαγραφή Πολιτικής Ασφάλειας
- Προδιαγραφή Δομής Ασφάλειας
- Εφαρμογή Δομής Ασφάλειας
- Δοκιμές επί της Ασφάλειας
- Επικύρωση Προδιαγραφών

Με τη σωστή κατανόηση των αναγκών μιας επιχείρησης και των πόρων για την ασφάλεια της πληροφορίας, είναι σίγουρο ότι τα συστήματα ηλεκτρονικού εμπορίου θα ωριμάσουν και θα μπορέσουν να αποτελέσουν πλεονέκτημα και για τις δύο μεριές των ηλεκτρονικών συναλλαγών των συστημάτων αυτών, δηλαδή του τελικού χρήστη και των επιχειρήσεων που διατηρούν αυτά τα συστήματα.

Βιβλιογραφία

[1] Rayport J. & Jaworski B., "E-commerce", Boston 2001

[2] Whiteley D., "E-commerce Strategy Technologies and Applications, London 2000

[3] Anthony D. Miyazaki & Anna Fernadez, "Consumer Perceptions of Privacy and Security Risks for Online Shopping, The Journal of Consumer, 2001

[4] Burns S., "Unique characteristics of E-commerce technologies and their effects upon payment systems, 2002

[5] Mazumdar C., Barik M. S., Das S., Roy J., Barkat M. A., "Final technical report for project development of validated security processes and methodologies for web based enterprises, 2003

[6] Schneider G. P., Perry J. T., "Electronic Commerce", Cambridge 2001

[7] Dr. Nada M. A. Al-Slamy, "E-Commerce security", 2008

[8] Theresa A. Kraft, Ratika Kakar, "E-Commerce Security", University of Michigan 2009

[9] Someswar Kesh, Sam Ramanujan, Sridhar Nerur, "A framework for analyzing e-commerce security", 2002

Παράρτημα Α' - Ερωτηματολόγιο

Ασφάλεια Ηλεκτρονικού Εμπορίου

0% 100%

Γενικές Ερωτήσεις

Γενικές ερωτήσεις για την ασφάλεια του συστήματος Ηλεκτρονικού Εμπορίου.

* **Χρησιμοποιείτε κάποιο σύστημα Ηλεκτρονικού Εμπορίου;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι

* **Τι σύστημα Ηλεκτρονικού Εμπορίου χρησιμοποιείτε;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

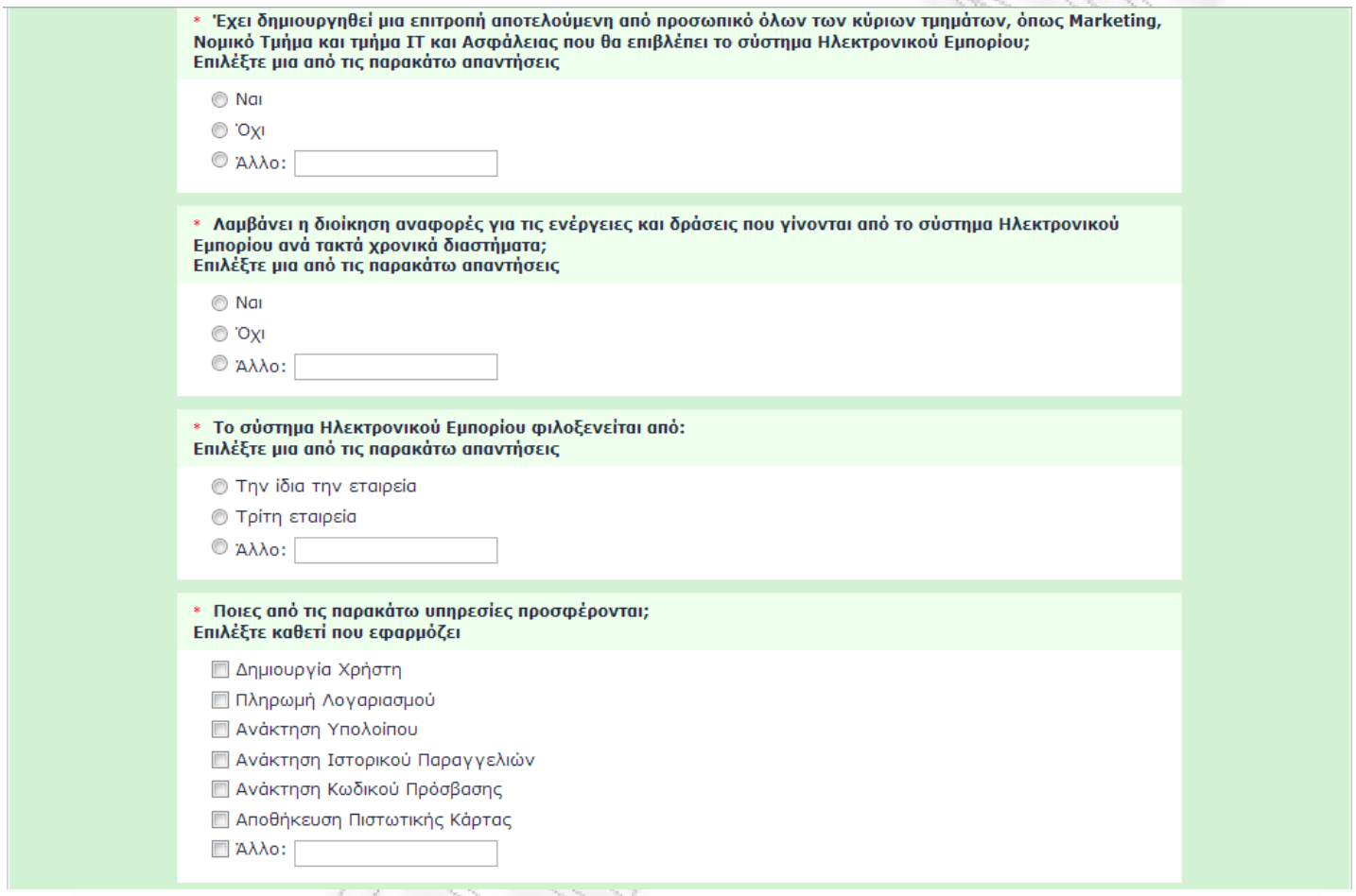
- Εσωτερική ανάπτυξη συστήματος
- Επί πληρωμή σύστημα τρίτης εταιρείας
- Σύστημα ανοιχτού κώδικα
- Άλλο:

* **Έχουν αναπτυχθεί επαρκής πολιτικές και διαδικασίες για τις ενέργειες που γίνονται από το σύστημα Ηλεκτρονικού Εμπορίου;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι

* **Υπάρχει ειδικό τμήμα ή προσωπικό που ασχολείται μόνο με το σύστημα Ηλεκτρονικού Εμπορίου;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ειδικό τμήμα
- Ειδικό προσωπικό
- Άλλο:



* **Έχει δημιουργηθεί μια επιτροπή αποτελούμενη από προσωπικό όλων των κύριων τμημάτων, όπως Marketing, Νομικό Τμήμα και τμήμα ΙΤ και Ασφάλειας που θα επιβλέπει το σύστημα Ηλεκτρονικού Εμπορίου;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- ○ Ναι
- ○ Όχι
- ○ Άλλο:

* **Λαμβάνει η διοίκηση αναφορές για τις ενέργειες και δράσεις που γίνονται από το σύστημα Ηλεκτρονικού Εμπορίου ανά τακτά χρονικά διαστήματα;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- ○ Ναι
- ○ Όχι
- ○ Άλλο:

* **Το σύστημα Ηλεκτρονικού Εμπορίου φιλοξενείται από:**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- ○ Την ίδια την εταιρεία
- ○ Τρίτη εταιρεία
- ○ Άλλο:

* **Ποιες από τις παρακάτω υπηρεσίες προσφέρονται;**
Επιλέξτε καθετί που εφαρμόζει

- ☐ Δημιουργία Χρήστη
- ☐ Πληρωμή Λογαριασμού
- ☐ Ανάκτηση Υπολοίπου
- ☐ Ανάκτηση Ιστορικού Παραγγελιών
- ☐ Ανάκτηση Κωδικού Πρόσβασης
- ☐ Αποθήκευση Πιστωτικής Κάρτας
- ☐ Άλλο:

Ασφάλεια Ηλεκτρονικού Εμπορίου

0% 100%

Ανάλυση Ρίσκου

Γενικές ερωτήσεις που αφορούν στην ανάλυση ρίσκου.

* **Υπάρχουν πολιτικές, διαδικασίες και πρακτικές για τη διεξαγωγή ανάλυσης ρίσκου ώστε να αποκαλυφθούν οι εσωτερικές και εξωτερικές ευπάθειες και απειλές στο σύστημα Ηλεκτρονικού Εμπορίου;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- ΌΧΙ

Παρακαλώ καταχωρήστε τα σχόλιά σας εδώ:

* **Οι πολιτικές που υπάρχουν σχετίζονται με λειτουργικό ρίσκο, ρίσκο ασφάλειας, ρίσκο φήμης και νομικό ρίσκο;**
Επιλέξτε καθετί που εφαρμόζει

- Λειτουργικό Ρίσκο
- Ρίσκο Ασφάλειας
- Ρίσκο Φήμης
- Νομικό Ρίσκο
- Άλλο:

* **Έχει γίνει ανάλυση ρίσκου για τις ενέργειες και δράσεις του συστήματος Ηλεκτρονικού Εμπορίου;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι

* **Ξαναελέγχει η διοίκηση το ρίσκο που συνδέεται με τεχνολογικές και λειτουργικές αλλαγές στο σύστημα Ηλεκτρονικού Εμπορίου;**

Ασφάλεια Ηλεκτρονικού Εμπορίου

0% 100%

Νομικά Ζητήματα
Ερωτήσεις σχετικές με νομικά θέματα.

* **Είναι ενημερωμένο το νομικό τμήμα για σημαντικά θέματα όπως τα συμβόλαια Ηλεκτρονικού Εμπορίου και οι συνεργασίες;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι

* **Παρακολουθούνται διαρκώς οι αλλαγές στο νομικό δίκαιο και τροποποιούνται άμεσα και κατάλληλα οι πολιτικές και διαδικασίες του συστήματος Ηλεκτρονικού Εμπορίου;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

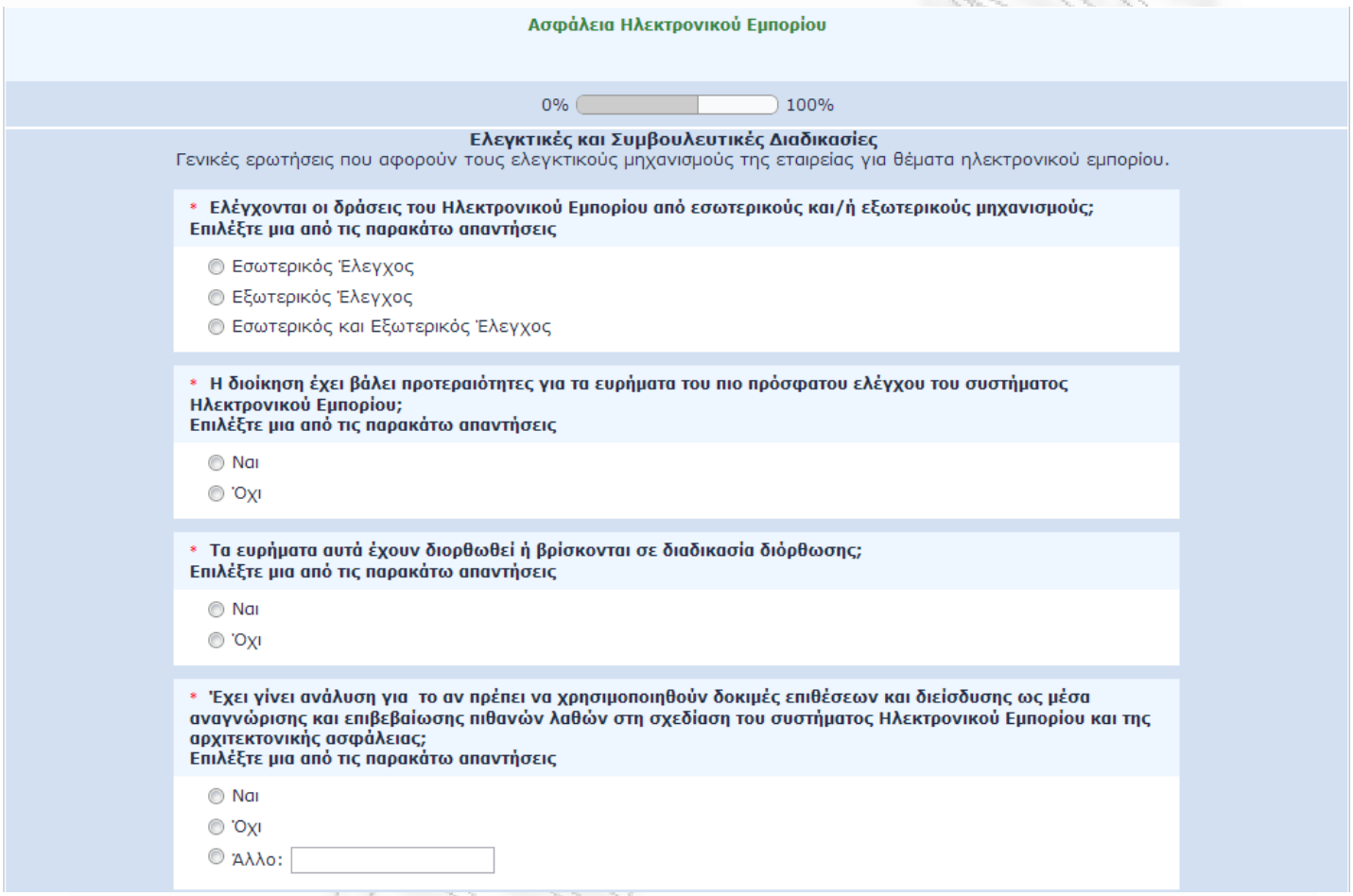
- Ναι
- Όχι
- Άλλο:

* **Υπάρχουν ειδικές διαδικασίες για τη διασφάλιση ότι οι συναλλαγές στο Ηλεκτρονικό Εμπόριο δεσμεύουν τον τελικό χρήστη και δεν μπορούν να αποποιηθούν;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι
- Άλλο:

* **Είναι ενήμερο το νομικό τμήμα για τις νομικές επιπλοκές που μπορεί να προκύψουν από χρήστες άλλων χωρών;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι



Ασφάλεια Ηλεκτρονικού Εμπορίου

0% 100%

Ελεγκτικές και Συμβουλευτικές Διαδικασίες

Γενικές ερωτήσεις που αφορούν τους ελεγκτικούς μηχανισμούς της εταιρείας για θέματα ηλεκτρονικού εμπορίου.

* **Ελέγχονται οι δράσεις του Ηλεκτρονικού Εμπορίου από εσωτερικούς και/ή εξωτερικούς μηχανισμούς;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Εσωτερικός Έλεγχος
- Εξωτερικός Έλεγχος
- Εσωτερικός και Εξωτερικός Έλεγχος

* **Η διοίκηση έχει βάλει προτεραιότητες για τα ευρήματα του πιο πρόσφατου ελέγχου του συστήματος Ηλεκτρονικού Εμπορίου;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

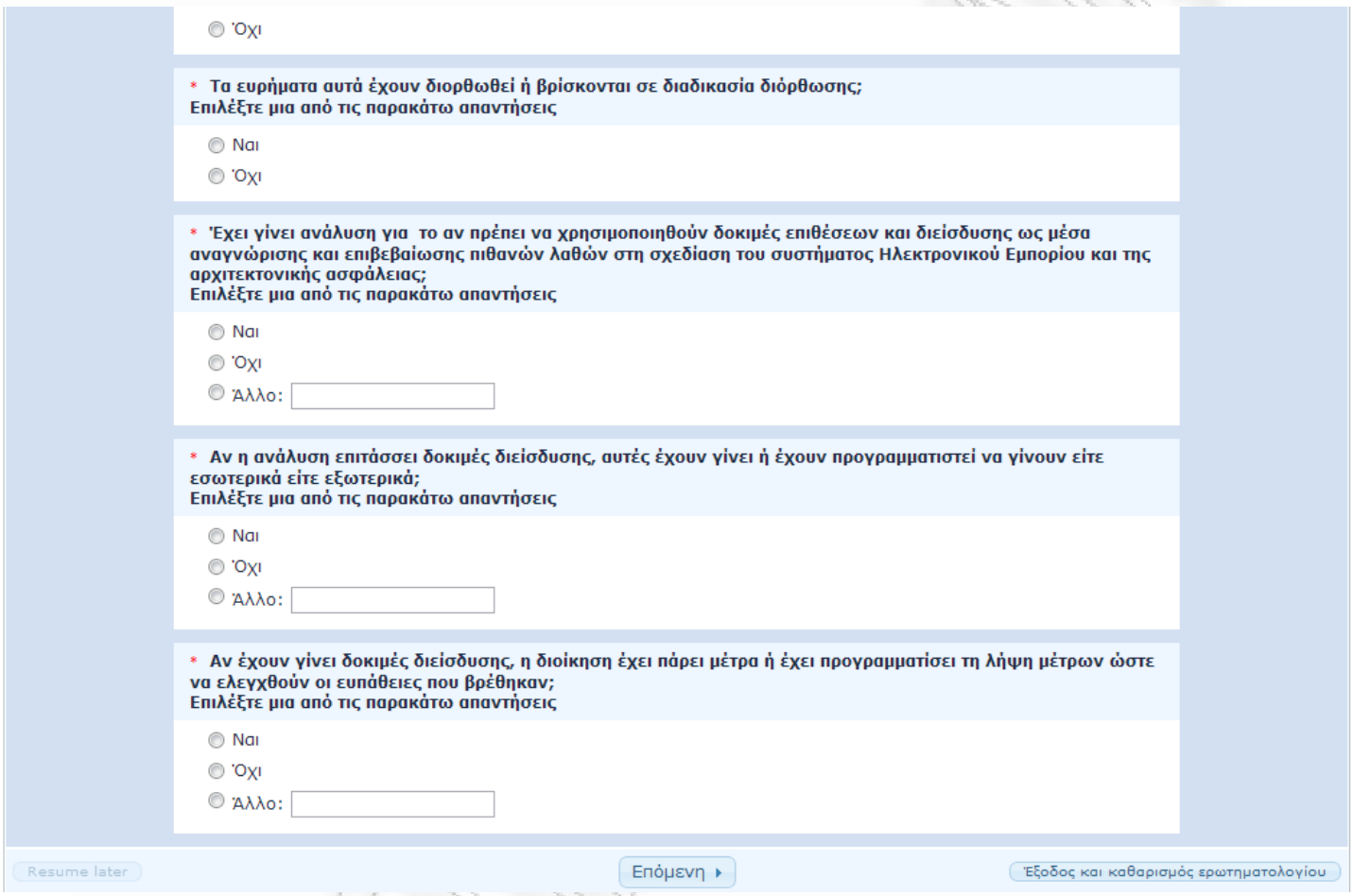
- Ναι
- Όχι

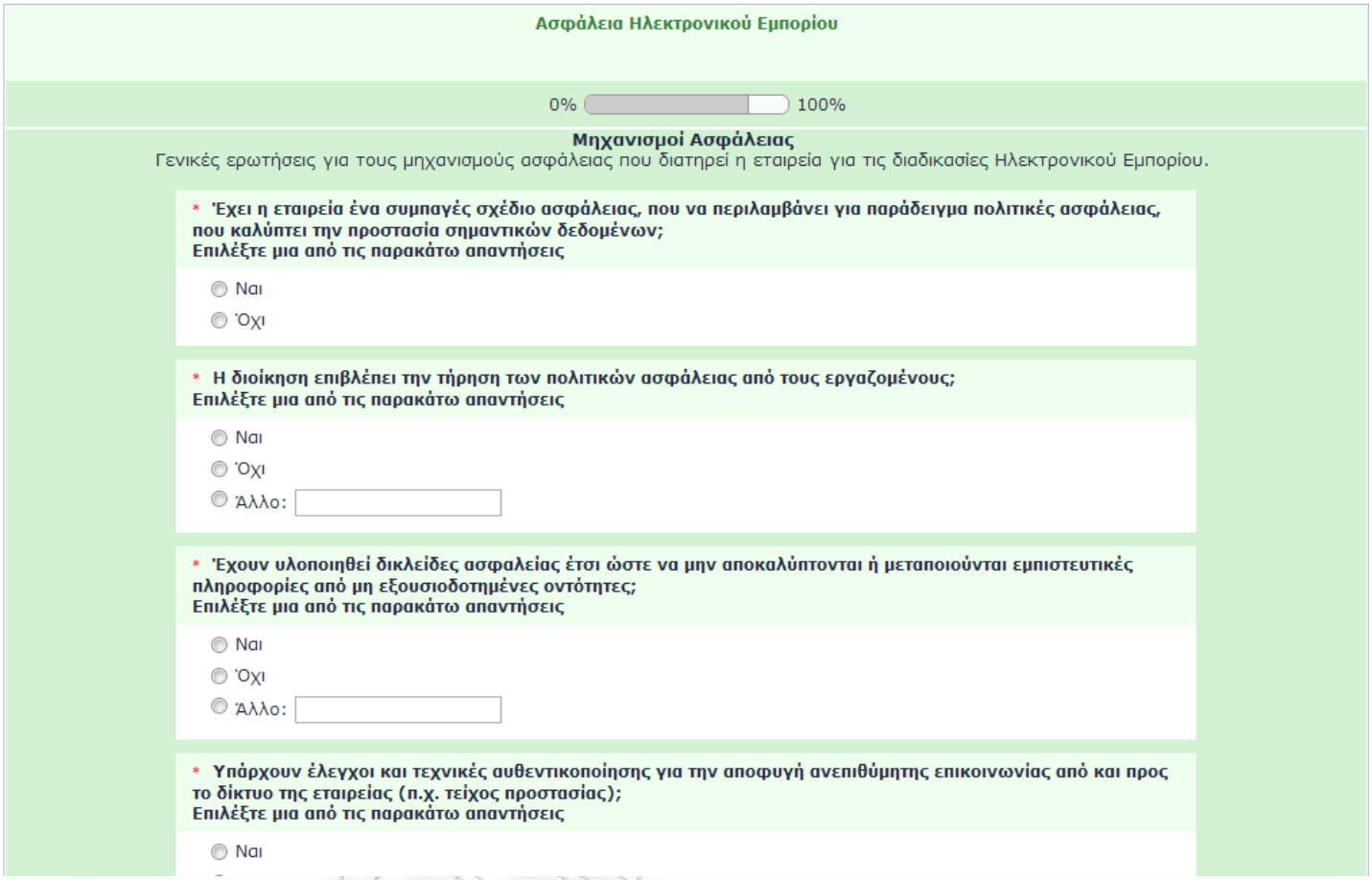
* **Τα ευρήματα αυτά έχουν διορθωθεί ή βρίσκονται σε διαδικασία διόρθωσης;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι

* **Έχει γίνει ανάλυση για το αν πρέπει να χρησιμοποιηθούν δοκιμές επιθέσεων και διείσδυσης ως μέσα αναγνώρισης και επιβεβαίωσης πιθανών λαθών στη σχεδίαση του συστήματος Ηλεκτρονικού Εμπορίου και της αρχιτεκτονικής ασφάλειας;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι
- Άλλο:


Όχι
* Τα ευρήματα αυτά έχουν διορθωθεί ή βρίσκονται σε διαδικασία διόρθωσης;
Επιλέξτε μια από τις παρακάτω απαντήσεις
Ναι
Όχι
* Έχει γίνει ανάλυση για το αν πρέπει να χρησιμοποιηθούν δοκιμές επιθέσεων και διείσδυσης ως μέσα αναγνώρισης και επιβεβαίωσης πιθανών λαθών στη σχεδίαση του συστήματος Ηλεκτρονικού Εμπορίου και της αρχιτεκτονικής ασφάλειας;
Επιλέξτε μια από τις παρακάτω απαντήσεις
Ναι
Όχι
Άλλο:
* Αν η ανάλυση επιτάσσει δοκιμές διείσδυσης, αυτές έχουν γίνει ή έχουν προγραμματιστεί να γίνουν είτε εσωτερικά είτε εξωτερικά;
Επιλέξτε μια από τις παρακάτω απαντήσεις
Ναι
Όχι
Άλλο:
* Αν έχουν γίνει δοκιμές διείσδυσης, η διοίκηση έχει πάρει μέτρα ή έχει προγραμματίσει τη λήψη μέτρων ώστε να ελεγχθούν οι ευπάθειες που βρέθηκαν;
Επιλέξτε μια από τις παρακάτω απαντήσεις
Ναι
Όχι
Άλλο:
Resume later
Επόμενη
Έξοδος και καθαρισμός ερωτηματολογίου



Ασφάλεια Ηλεκτρονικού Εμπορίου

0% 100%

Μηχανισμοί Ασφάλειας

Γενικές ερωτήσεις για τους μηχανισμούς ασφάλειας που διατηρεί η εταιρεία για τις διαδικασίες Ηλεκτρονικού Εμπορίου.

* **Έχει η εταιρεία ένα συμπαγές σχέδιο ασφάλειας, που να περιλαμβάνει για παράδειγμα πολιτικές ασφάλειας, που καλύπτει την προστασία σημαντικών δεδομένων;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι

* **Η διοίκηση επιβλέπει την τήρηση των πολιτικών ασφάλειας από τους εργαζομένους;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι
- Άλλο:

* **Έχουν υλοποιηθεί δικλείδες ασφαλείας έτσι ώστε να μην αποκαλύπτονται ή μεταποιούνται εμπιστευτικές πληροφορίες από μη εξουσιοδοτημένες οντότητες;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι
- Άλλο:

* **Υπάρχουν έλεγχοι και τεχνικές αυθεντικοποίησης για την αποφυγή ανεπιθύμητης επικοινωνίας από και προς το δίκτυο της εταιρείας (π.χ. τείχος προστασίας);**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι

* **Υπάρχουν έλεγχοι και τεχνικές αυθεντικοποίησης για την αποφυγή ανεπιθύμητης επικοινωνίας από και προς το δίκτυο της εταιρείας (π.χ. τείχος προστασίας);**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι
- Άλλο:

* **Υπάρχουν μηχανισμοί οι οποίοι θα αποσυνδέουν τους χρήστες του συστήματος Ηλεκτρονικού Εμπορίου ως αποτέλεσμα μη δραστηριότητας μετά από συγκεκριμένο χρονικό διάστημα;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι
- Άλλο:

* **Έχουν διαβαθμιστεί τα δεδομένα με βάση την ευαισθησία τους αλλά και τον αντίκτυπο που θα είχαν στην εταιρεία σε περίπτωση απώλειας τους;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι
- Άλλο:

* **Υπάρχουν κριτήρια με βάση τα οποία αποφασίζεται ο τρόπος κρυπτογράφησης των διάφορων τύπων ευαίσθητων δεδομένων που χρειάζονται παραπάνω προστασία;**
Επιλέξτε μια από τις παρακάτω απαντήσεις

- Ναι
- Όχι
- Άλλο:

Resume later | Υποβολή | Έξοδος και καθαρισμός ερωτηματολογίου