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

Διπλωματική Εργασία

Μεταπτυχιακού Διπλώματος Ειδίκευσης

ΘΕΜΑ:

«Προστασία της Ιδιωτικότητας σε περιπτώσεις υπεργολαβίας υπηρεσιών πληροφορικής σε τρίτους φορείς»

Ονοματεπώνυμο Σπουδαστή:

Κωνσταντίνος Ι. Βίλλιος, ΜΤΕ0903

«ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΕ ΠΕΡΙΠΤΩΣΕΙΣ ΥΠΕΡΓΟΛΑΒΙΑΣ ΥΠΗΡΕΣΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΕ ΤΡΙΤΟΥΣ ΦΟΡΕΙΣ»

ΚΩΝΣΤΑΝΤΙΝΟΣ Ι. ΒΙΛΛΙΟΣ

<u>Επιτροπή Κρίσης</u>

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

Επιβλέπων Διπλωματικής: Κώστας Λαμπρινουδάκης, Επίκουρος Καθηγητής

ΠΕΙΡΑΙΑΣ 2012

Περίληψη

Στη σημερινή εποχή, η προστασία της ιδιωτικότητας διαδραματίζει ένα σημαντικό ρόλο. Ειδικά όταν συζητάμε για προσωπικά και ευαίσθητα δεδομένα και μάλιστα όταν τα χειρίζονται τρίτοι φορείς θα πρέπει να είμαστε πολύ επιφυλακτικοί και να παίρνουμε όλα εκείνα τα μέτρα προστασίας που θα καθορίσουν τη προστασία τους και να εξασφαλίζουν τη δυνατότητα να προστατεύονται από κακόβουλες επιθέσεις ή διαρροή από αμέλεια στις περιπτώσεις ανάθεσης έργων και υπηρεσιών πληροφορικής σε υπεργολάβους και μάλιστα για εργασίες μέσα στον ίδιο τον οργανισμό. Οι οικονομικοί και υγειονομικοί οργανισμοί έχουν πολλά δεδομένα που πρέπει να προστατεύονται σε τέτοιες περιπτώσεις και θα πρέπει εξασφαλιστεί κατά το μέγιστο δυνατό η διασφάλισή τους.

Λέξεις – Κλειδιά

Προσωπικά δεδομένα, ευαίσθητα δεδομένα, κακόβουλες επιθέσεις, υπεργολαβία, υγειονομικοί οργανισμοί, οικονομικοί οργανισμοί

Abstract

Nowadays, the protection of privacy conducts an important role. Especially when we are dealing with personal and sensitive data and even more when those data are being manipulated by other entities, we have to be extremely cautious and take all the available countermeasures so we can be sure that our data will be protected in the case of giving away projects to subcontractors. Economical and health organizations maintain a large amount of data that must be protected in such cases.

Keywords

Personal data, sensitive data, malicious attacks, subcontractor, health organizations, economical organizations

Πρόλογος

Η παρούσα διπλωματική εργασία εκπονήθηκε και υλοποιήθηκε από τον διπλωματούχο Κωνσταντίνο Βίλλιο από το Αίγιο Αχαΐας.
Ευχαριστώ πολύ τον καθηγητή μου Κωνσταντίνο Λαμπρινουδάκη για την ιδέα εκπόνησης της εργασίας αυτής και την πολύτιμη βοήθεια του καθ' όλη την διάρκεια της συγγραφής της, καθώς και τους καθηγητές μου Σωκράτη Κάτσικα και Χρήστο Ξενάκη για την συμμετοχή τους στην εξέτασή της. Επίσης ιδιαίτερη αναφορά θέλω να κάνω στον συμφοιτητή μου και συνοδοιπόρο Νικόλαο Λάμπρου για την στήριξη του και την πίστη του σε εμένα ώστε να καταφέρουμε να αναπτύξουμε την εταιρεία μας, μια ελληνική start up και να προσφέρουμε στο χώρο των υπηρεσιών διαδικτύου μαζί με όλα όσα μάθαμε μέσα από το μεταπτυχιακό μας. Τέλος, ευχαριστώ όλους τους φίλους και συναδέλφους μου για την βοήθεια και συμπαράστασή τους

Πειραιάς, Σεπτέμβριος 2012

Digitally signed by Konstantinos Villios
Date: 2012.09.27 10:06:41 +03'00'

.....

Κωνσταντίνος Ι. Βίλλιος

Πτυχιούχος Εφαρμογών Πληροφορικής στη Διοίκηση και Οικονομία ΤΕ
Διπλωματούχος Τεχνοοικονομικής Διοίκησης και Ασφάλειας Ψηφιακών Συστημάτων

Πίνακας Περιεχομένων

Εισαγωγή

Στην σύγχρονη εποχή, η χρήση πληροφοριακών συστημάτων είναι δεδομένη για κάθε οργανισμό. Η επανάσταση της συνδεσιμότητας είναι πλέον γεγονός. Η ελεύθερη ροή πληροφοριών, οι ευκολίες που παρέχει το διαδίκτυο έχουν ωθήσει μέχρι και τις μικρότερες επιχειρήσεις να επενδύσουν στην χρήση πληροφοριακών συστημάτων και διαδικτυακών εφαρμογών. Σαν αποτέλεσμα, στο μεγαλύτερο ποσοστό των οργανισμών η χρήση των πληροφοριακών συστημάτων είναι απολύτως αναγκαία για την επίτευξη των στόχων και της βασικής λειτουργικότητας τους. Έτσι, η παραμικρή δυσλειτουργία, διακοπή ή παράνομη διείσδυση στα συστήματα αυτά μεταφράζεται σε κόστος, είτε από άμεσες οικονομικές απώλειες, είτε από την αδυναμία του οργανισμού να λειτουργήσει αποδοτικά.

Εκτός από τις οικονομικές επιπτώσεις όμως, τα προβλήματα ασφαλείας πληροφοριακών συστημάτων γίνονται ακόμα πιο αισθητά σε συστήματα που περιέχουν ευαίσθητα δεδομένα ή επιτελούν «ευαίσθητες» και σημαντικές λειτουργίες.

Διάφορα παραδείγματα τέτοιων συστημάτων είναι:

- Συστήματα με οικονομικά δεδομένα
- Συστήματα με ευαίσθητα ιατρικά δεδομένα
- Συστήματα που περιέχουν ευαίσθητα προσωπικά δεδομένα

Είναι φανερό ότι η ρήξη της ασφάλειας τέτοιων πληροφοριακών συστημάτων μπορεί να προκαλέσει σοβαρότατα προβλήματα που απειλούν άμεσα την ανθρώπινη ζωή και την ασφάλεια σε τοπικό ή μεγαλύτερο επίπεδο.

Δεν υπάρχει λοιπόν αμφιβολία ότι η ασφάλεια των πληροφοριακών συστημάτων έχει τεράστια σημασία στην σύγχρονη κοινωνία και πρέπει να παίζει πρωτεύον ρόλο κατά την σχεδίαση, συντήρηση και χρήση τους.

Η ευθύνη για την προστασία των προσωπικών και ευαίσθητων δεδομένων ενός πληροφοριακού συστήματος ανήκει πάντα στον φορέα που τα έχει συλλέξει για κάποιο συγκεκριμένο σκοπό. Στις περιπτώσεις που συγκεκριμένες εργασίες αξιοποιούν τα δεδομένα αυτά και ο οργανισμός αναθέτει σε τρίτο εξωτερικό φορέα την υλοποίηση τους, είναι απαραίτητο να ληφθούν τα απαραίτητα μέτρα ώστε να συνεχίσουν να προστατεύονται.

Υπεργολαβία για έναν οργανισμό είναι όταν μια εργασία, λειτουργία ή διαδικασία γίνεται ανάθεση σε τρίτους. Επιπλέον, οι λειτουργίες που επιτελούνται από το τρίτο μέρος (υπεργολάβο) μπορεί να εκτελείται είτε στο χώρο του εργοδότη, είτε εκτός του χώρου.

Στην παρούσα εργασία μελετώνται και αναλύονται όλα τα μέτρα εκείνα που θα καταστήσουν τα προσωπικά και ευαίσθητα δεδομένα των πληροφοριακών

συστημάτων των οργανισμών ασφαλή, για εργασίες από υπεργολάβους μέσα στον ίδιο τον οργανισμό. Και εφόσον μιλάμε για αναθέσεις έργων σε πληροφοριακά συστήματα νοσοκομειακών οργανισμών και τραπεζών, υπάρχουν ζητήματα ιδιωτικότητας για το πώς θα χειρίζονται τα δεδομένα στα οποία έχουν πρόσβαση ο υπεργολάβος και οι υπάλληλοι/ συνεργάτες του. Η ιδιωτικότητα είναι το απαράγραπτο δικαίωμα κάθε ατόμου να ασκεί έλεγχο στον τρόπο με τον οποίο οι προσωπικές του πληροφορίες τηρούνται, υποβάλλονται σε επεξεργασία, μοιράζονται ή διανέμονται και χρησιμοποιούνται από οποιαδήποτε άλλη οντότητα.

Κεφάλαιο 1^{ο} - Ασφάλεια και Αντιμετώπιση

1.1 Εισαγωγή

Στην δεκαετία του ’80, όταν τα πληροφοριακά συστήματα άρχισαν σιγά σιγά να διεισδύουν στις μεσαίες και μεγάλες επιχειρήσεις, οι άνθρωποι που ήξεραν να τα χειρίζονται ήταν λίγοι και εξειδικευμένοι. Τα φαινόμενα παραβίασης της ασφάλειας ήταν σχεδόν ανύπαρκτα. Κατά την διάρκεια της δεκαετίας του ’90 και μέχρι σήμερα, οι νέες τεχνολογίες οδήγησαν σε ευρεία χρήση των ηλεκτρονικών υπολογιστών με αποτέλεσμα ο αριθμός των παραβιάσεων ασφαλείας να ακολουθεί μια συνεχή εκθετική αύξηση.

1.2 Ιδιωτικότητα στην εποχή της τεχνολογίας

Με την πάροδο του χρόνου - και αναμφίβολα και υπό την επίδραση της εξέλιξης των νέων τεχνολογιών – γινόταν όλο και περισσότερο κατανοητό ότι η ιδιωτικότητα παρέχει αναγκαία αλλά και ανεπαρκή ωστόσο προστασία στο άτομο. Η τεχνολογική δυνατότητα διείσδυσης στη ζωή και στην επικοινωνία, στην προσωπικότητα και στις συνήθειες του χρήστη ανέδειξε και την διάσταση των κινδύνων που συνδέονται με την αναδυόμενη Κοινωνία της Πληροφορίας, καθώς ήδη η ποσοτική αύξηση συνεπέφερε την αύξηση της έντασης της προσβολής των δικαιωμάτων του ατόμου. [14]

1.3 Προστασία της Ιδιωτικότητας

Η προστασία του απορρήτου και των προσωπικών δεδομένων ως απαραίτητα συστατικά για την προστασία της ιδιωτικότητας στις περιπτώσεις που εξετάζουμε σχετίζονται με [14]:

- Απόλαυση συνταγματικών δικαιωμάτων
- Άσκηση συνταγματικών ελευθεριών
- Συμμετοχή στην ελεύθερη επικοινωνία στην πολιτική και κοινωνική ζωή

1.4 Αντιμετώπιση Προβλημάτων

Η αντιμετώπιση των προβλημάτων ασφαλείας, παρότι δεν είναι απλή υπόθεση, πρέπει να λαμβάνεται σοβαρά υπόψη. Η εισαγωγή πληροφοριακών συστημάτων σε ένα περιβάλλον μπορεί μεν να αυξάνει κατακόρυφα την παραγωγικότητα και το κέρδος, αλλά εισάγει νέους κινδύνους που αυξάνουν σημαντικά το ρίσκο και επομένως πρέπει οπωσδήποτε να αναγνωριστούν και να αντιμετωπιστούν ανάλογα. [13]

Ο κλάδος της ασφάλειας πληροφοριακών συστημάτων έχει να προσφέρει ευτυχώς μια πληθώρα από αντίμετρα (εργαλεία, μεθόδους, έλεγχους, πολιτικές ασφαλείας) για την αντιμετώπιση κάθε είδους προβλήματος. Η ενσωμάτωση όμως όλων αυτών σε κάθε οργανισμό δεν είναι καθόλου απλή υπόθεση. Αντιθέτως, ο διαφορετικός τρόπος λειτουργίας καθώς και η διαφορετική ανάθεση πόρων για θέματα ασφαλείας δημιουργούν εντελώς διαφορετικές συνθήκες, μοναδικές για κάθε οργανισμό. Η ενσωμάτωση της ασφάλειας λοιπόν δεν πρέπει να θεωρηθεί ως μια απλή διαδικασία, καθώς πρέπει κάθε φορά να λαμβάνονται υπόψη όλοι οι παράγοντες ώστε η ασφάλεια να μην γίνετε εμπόδιο στην λειτουργία του οργανισμού, αλλά να τον υπηρετεί.

Κεφάλαιο 2^{ο} – Υπεργολαβία και Δεδομένα

2.1 Τι σημαίνει υπεργολαβία

Υπεργολαβία για έναν οργανισμό είναι όταν οποιαδήποτε εργασία, λειτουργία ή διαδικασία που θα μπορούσε να εκτελεστεί από τους υπαλλήλους στο πλαίσιο ενός οργανισμού ή εταιρείας, γίνεται ανάθεση σε τρίτους για σημαντικό χρονικό διάστημα. Επίσης οι λειτουργίες που επιτελούνται από το τρίτο μέρος (υπεργολάβο) εκτελούνται είτε στο χώρο του εργοδότη, είτε εκτός του χώρου.

2.2 Η ταυτότητα του υπεργολάβου

Οι υπεργολάβοι των πληροφοριακών συστημάτων σε υγειονομικούς και οικονομικούς οργανισμούς μπορεί να είναι εταιρείες πληροφορικής και νέων τεχνολογιών καθώς και εταιρείες που σχετίζονται με την ανάπτυξη και ανάλυση πληροφοριακών συστημάτων. Επίσης μπορεί να είναι και ανεξάρτητα άτομα που σχετίζονται με οποιοδήποτε τρόπο με τον υπεργολάβο.
Θα μπορούσαμε να διακρίνουμε τις ακόλουθες περιπτώσεις [9, 14]:

- Κατάχρηση της ιδιωτικότητας από αμέλεια
- Κατάχρηση της ιδιωτικότητας από πρόθεση με τα ακόλουθα κυρίως κίνητρα:
    - Περιέργεια
    - Οικονομικό όφελος
    - Πρόκληση
    - Κατασκοπεία

2.3 Κατηγορίες Εργασιών Υπεργολάβου

Οι υπεργολάβοι των πληροφοριακών συστημάτων σε υγειονομικούς και οικονομικούς οργανισμούς μπορεί να είναι εταιρείες πληροφορικής και νέων τεχνολογιών καθώς και εταιρείες που σχετίζονται με την ανάπτυξη και ανάλυση πληροφοριακών συστημάτων. Επίσης μπορεί να είναι και ανεξάρτητα άτομα που σχετίζονται με οποιοδήποτε τρόπο με τον υπεργολάβο.

2.4 Κατηγορίες Δεδομένων

- ✓ **Δεδομένα προσωπικού χαρακτήρα**, είναι κάθε πληροφορία που αναφέρεται στο φυσικό πρόσωπο που αναφέρονται τα δεδομένα. Δεδομένα προσωπικού χαρακτήρα δεν είναι τα στατιστικά και συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν να προσδιορισθούν τα φυσικά πρόσωπα των δεδομένων [14].

- ✓ **Ευαίσθητα δεδομένα**, είναι τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων [14].

2.5 Επεξεργασία Δεδομένων

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα προστατεύεται από τον νόμο 2472/1997 και είναι κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από τον οποιοδήποτε φορέα, οργανισμό, φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση, η διαγραφή και η καταστροφή [14].

2.6 Μελέτες Περίπτωσης και δεδομένα

Στα πλαίσια της εργασίας έχουμε δυο μελέτες-περίπτωσης:

Οι **υγειονομικοί οργανισμοί** χρησιμοποιούν ευαίσθητα δεδομένα και αυτό έχει ως αποτέλεσμα να απαιτούνται περισσότερα μέτρα προστασίας από ότι θα παίρναμε αν δεν ήταν ευαίσθητα τα δεδομένα. Η νομοθεσία είναι πολύ αυστηρή περί επεξεργασία των δεδομένων και θα πρέπει να τηρούνται αυστηροί κανόνες ασφάλειας.

Οι **οικονομικοί οργανισμοί** χρησιμοποιούν δεδομένα προσωπικού χαρακτήρα. Όμως θα πρέπει να λάβουμε υπόψη μας ότι γίνεται και καταγραφή χώρου με τη μέθοδο της βιντεοσκόπησης κάτι που συνιστά να υπάρχει ξεχωριστή μέθοδος επεξεργασίας των συγκεκριμένων δεδομένων για να μην παραβιάζεται η κείμενη νομοθεσία.

Κεφάλαιο 3^{ο} – Ευπάθειες και Απειλές

3.1 Ορισμοί

- ✓ **Απειλή** είναι οτιδήποτε μπορεί να προκαλέσει παραβίαση της διαθεσιμότητας, ακεραιότητας ή εμπιστευτικότητας σε ένα πληροφοριακό σύστημα [9, 14]
- ✓ **Ευπάθεια** είναι η αδυναμία ή το ελάττωμα στο υλικό, λογισμικό ή στην αρχιτεκτονική ενός συστήματος καθώς και στις διαδικασίες ασφάλειας του πληροφοριακού συστήματος με σκοπό να παραβιάσει τη διαθεσιμότητα, ακεραιότητα ή την εμπιστευτικότητα του [9, 14]

3.2 Συνηθισμένες Ευπάθειες και απειλές

Σύμφωνα με τις περιπτώσεις-μελέτης της παρούσας εργασίας και με το εγχειρίδιο χρήσης της CRAMM εντοπίζουμε τις παρακάτω ευπάθειες και απειλές στα πληροφοριακά συστήματα υγειονομικών και οικονομικών οργανισμών [11, 12, 13, 14]:

- *Masquerading of User Identity:*
  Η χρήση ονόματος χρήστη και κωδικού πρόσβασης ενός άλλου ατόμου μπορεί να προκαλέσει την κλοπή, μετατροπή ή διαγραφή των προσωπικών πληροφοριών του χρήστη. Επίσης, κάποιος που δεν έχει δικαίωμα μπορεί να χρησιμοποιήσει τα προγράμματα του οργανισμού, προκαλώντας μη διαθεσιμότητα. Τέλος, η χρήση κωδικού ενός διαχειριστή μπορεί να προκαλέσει πολύ σοβαρότατες απώλειες σε όλο το σύστημα.

- *Communications Interception:*
  Η υποκλοπή των επικοινωνιών μεταξύ χρήστη και εξυπηρετητή μπορεί να οδηγήσει σε υποκλοπή των προσωπικών δεδομένων του χρήστη και των κωδικών πρόσβασης και άλλων ευαίσθητων ή όχι δεδομένων του συστήματος

- *Communications Failure:*
  Η αποτυχία των επικοινωνιών προκαλεί μη διαθεσιμότητα του προσωπικού χώρου των χρηστών, και ακόμη χειρότερα την μη διαθεσιμότητα του συστήματος.

- *Introduction of Damaging or Disruptive Software:*
  Η εισαγωγή επιβλαβούς λογισμικού όπως ιούς, δούρειους ίππους, σκουλήκια (worms), λογικές βόμβες κτλ. μπορεί να οδηγήσει στην καταστροφή των δεδομένων των χρηστών, την αλλοίωση ή την υποκλοπή τους.

- *Technical Failure of Host:*

Η απειλή αυτή καλύπτει τις περιπτώσεις βλάβης του υλικού (hardware). Μπορεί να οδηγήσει σε καταστροφή των δεδομένων που υπάρχουν στο πληροφοριακό σύστημα και σε μη διαθεσιμότητα της αντίστοιχης υπηρεσίας.

- *System and Network Software Failure:*
  Η απειλή αυτή καλύπτει τις περιπτώσεις σφάλματος του λογισμικού που υπάρχει στο πληροφοριακό σύστημα. Μπορεί να οδηγήσει σε μη διαθεσιμότητα αλλά και τυχαία (accidental) αποκάλυψη απόρρητων δεδομένων.

- *Theft by Insiders:*
  Η κλοπή των δεδομένων με οποιοδήποτε τρόπο, μπορεί να οδηγήσει σε αποκάλυψη τους.

- *Wilful Damage by Insiders:*
  Η ζημιά με πρόθεση μπορεί να προκαλέσει φυσική καταστροφή υλικών στοιχείων, μη διαθεσιμότητα υπηρεσιών, καταστροφή ή αλλοίωση δεδομένων.

- *Fire:*
  Η φωτιά απειλεί να καταστρέψει δεδομένα ή με πρόσχημα το περιστατικό να μπορεί να δημιουργηθεί κενό ασφαλείας και να υπάρξει φυσική πρόσβαση στο πληροφοριακό σύστημα από μη επιτρεπόμενο άτομο

- *Power Failure:*
  Η διακοπή ρεύματος απειλεί με μη διαθεσιμότητα και με πρόσχημα το περιστατικό να μπορεί να δημιουργηθεί κενό ασφαλείας και να υπάρξει πρόσβαση στο πληροφοριακό σύστημα από μη εξουσιοδοτημένο άτομο

- *Air Conditioning Failure:*
  Η διακοπή λειτουργίας του συστήματος κλιματισμού στο φυσικό χώρου του πληροφοριακού συστήματος μπορεί να προκαλέσει την μη διαθεσιμότητα του και με πρόσχημα το περιστατικό να μπορεί να δημιουργηθεί κενό ασφαλείας και να υπάρξει φυσική πρόσβαση στο πληροφοριακό σύστημα από μη επιτρεπόμενο άτομο

- *Water Damage:*
  Η πλημμύρα μπορεί να προκαλέσει φυσική καταστροφή των υλικών στοιχείων, καταστροφή των δεδομένων, μη διαθεσιμότητα του πληροφοριακού συστήματος και με πρόσχημα το περιστατικό να μπορεί να δημιουργηθεί κενό ασφαλείας και να υπάρξει φυσική πρόσβαση στο πληροφοριακό σύστημα από μη επιτρεπόμενο άτομο.

Κεφάλαιο 4^{ο} – Μέτρα Προστασίας της Ιδιωτικότητας

Πρέπει να λάβουμε υπόψη μας αν η ζημιά που θα προκληθεί θα γίνει από πρόθεση ή αμέλεια διότι είναι πολύ σημαντικό να μπορεί να βρεθεί ο λόγος για τον οποίο παραβιάστηκε η ιδιωτικότητα, εφόσον υπάρχουν οι μηχανισμοί που να μπορούμε να το διερευνήσουμε. Αναφέρουμε ενδεικτικά μέτρα προστασίας στον παρακάτω πίνακα [1-21]:

Απειλές και Ευπάθειες	Μέτρα Προστασίας
Masquerading of User Identity	✓ Κανονισμός διαχείρισης κωδικών πρόσβασης για τις υπηρεσίες email, ftp, χρήσης υπολογιστών ✓ Κανονισμός μορφής των κωδικών πρόσβασης των συστημάτων ✓ Καταγραφή των συμβάντων μέσω log αρχείων ✓ Κανονισμός διαχείρισης ελέγχου πρόσβασης σε αρχεία που διαχειρίζονται οι οργανισμοί ✓ Κανονισμός διαχείρισης περιπτώσεων προς αποφυγή του φαινομένου social engineering (υποκλοπή μέσω ανθρώπινης εξαπάτησης) ✓ Προστασία των συστημάτων και ενημέρωση των υπαλλήλων του οργανισμού για το key logging
Communications Interception	✓ Προστασία από κακόβουλο λογισμικό ✓ Διαχείριση των συστημάτων μέσω firewall ανά περίπτωση ✓ Κρυπτογράφηση δεδομένων για την διακίνηση των πληροφοριών όπου απαιτείται ✓ Κανονισμός διαχείρισης ασυρμάτων δικτύων ✓ Καταγραφή των συμβάντων μέσω log αρχείων

Communications Failure	✓ Κανονισμός διαχείρισης προβλημάτων στις επικοινωνίες για αποφυγή κενών ασφαλείας ✓ Καταγραφή των συμβάντων μέσω log αρχείων
Introduction of Damaging or Disruptive Software	✓ Προστασία από κακόβουλο λογισμικό ✓ Προστασία και διαχείριση των θυρών usb και των cd-dvd ✓ Κανονισμός ενημέρωσης των λογισμικών προστασίας από κακόβουλο λογισμικό ✓ Κανονισμός αντιμετώπισης μολυσμένων συστημάτων ✓ Καταγραφή των συμβάντων μέσω log αρχείων
Technical Failure of Host	✓ Κανονισμός διαχείρισης ελαττωματικών μέσων αποθήκευσης ✓ Καταγραφή των συμβάντων μέσω log αρχείων
System and Network Software Failure	✓ Κανονισμός ενημέρωσης των συστημάτων (updates/upgrades) για κάλυψη κενών ασφαλείας ✓ Κανονισμός διαχείρισης προβλημάτων αν αναφερθεί σφάλμα για την μη αποκάλυψη απόρρητων δεδομένων ✓ Καταγραφή των συμβάντων μέσω log αρχείων
Theft by Insiders	✓ Κανονισμός επιτήρησης για τους εξωτερικούς συνεργάτες που εργάζονται στον οργανισμό

	✓ Συμφωνητικό εχεμύθειας με ρήτρες διαρροής για τα απόρρητα και άλλα δεδομένα (απαιτητό στους οργανισμούς υγείας) ✓ Αυστηρός κανονισμός πρόσβασης στο δωμάτιο καταγραφής εικόνας και ήχου (απαιτητό στους οικονομικούς οργανισμούς)
Wilful Damage by Insiders	✓ Κανονισμός επιτήρησης για τους εξωτερικούς συνεργάτες που εργάζονται στον οργανισμό
Fire	✓ Αυστηρός κανονισμός πρόσβασης στο δωμάτιο του πληροφοριακού συστήματος ✓ Σχέδιο έκτακτης ανάγκης
Power Failure	✓ Λειτουργία ups ή γεννήτριας ρεύματος για την αποφυγή δυσλειτουργιών ✓ Αυστηρός κανονισμός πρόσβασης στο δωμάτιο του πληροφοριακού συστήματος
Air Conditioning Failure	✓ Λειτουργία δεύτερου κλιματιστικού συστήματος ✓ Συντήρηση των συστημάτων κλιματισμού ✓ Αυστηρός κανονισμός πρόσβασης στο δωμάτιο του πληροφοριακού συστήματος
Water Damage	✓ Σχέδιο έκτακτης ανάγκης ✓ Αυστηρός κανονισμός πρόσβασης στο δωμάτιο του πληροφοριακού συστήματος

Κεφάλαιο 5^{ο} – Νομικά Ζητήματα

5.1 Εισαγωγή

Η Ελλάδα υπήρξε από τις πρώτες χώρες που μετέφεραν την κοινοτική Οδηγία στο εσωτερικό δίκαιο για την προστασία των προσωπικών δεδομένων. Το ελληνικό νομοθετικό πλαίσιο συγκροτείται από το συνταγματικό δικαίωμα προστασίας προσωπικών δεδομένων όπως κατοχυρώνεται στο άρθρο 9 Α του Συντάγματος, τον νόμο 2472/97 (ΦΕΚ Α' 50/10.04.1997) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως ισχύει μετά τις τροποποιήσεις που κατά καιρούς εισήχθησαν καθώς και τον νόμο 3471/06 (ΦΕΚ Α' 133/28.06.2006).

Η προστασία των προσωπικών δεδομένων δεν περιλαμβάνει μόνο την παρεμπόδιση της μη εξουσιοδοτημένης χρήσης ή της αποκάλυψης σε άλλους. Αποτελείται και συνίσταται σε ένα πλέγμα αρχών, δικαιωμάτων και εγγυήσεων. Ως δίκαιο προστασίας προσωπικών δεδομένων αντιλαμβανόμαστε συνεπώς το σύνολο των κανόνων, προϋποθέσεων, όρων, εξουσιών και απαγορεύσεων σε σχέση με τη συλλογή και επεξεργασία προσωπικών δεδομένων, καθώς και τις ρυθμίσεις που αφορούν διαδικασίες, θεσμικούς ελέγχους, εγγυήσεις και αντίβαρα των περιορισμών των δικαιωμάτων προστασίας των προσωπικών δεδομένων των προσώπων. [14]

5.2 Περιπτώσεις μελέτης

Στους **υγειονομικούς οργανισμούς έ**χουν εφαρμογή το άρθρο 371ΠΚ (καθήκον εχεμύθειας), τα άρθρα 13 και 14 του Κώδικα Ιατρικής Δεοντολογίας (υποχρέωση τήρησης απορρήτου και υποχρέωση τήρησης ιατρικού αρχείου) και ο Ν. 2472/1997 (προστασία, εκτός των άλλων, των ευαίσθητων δεδομένων υγείας).

Στους **οικονομικούς οργανισμούς** έχουν εφαρμογή η αστική διάταξη του άρθρου 57ΑΚ, η ποινική διάταξη του άρθρου 371ΠΚ (καθήκον εχεμύθειας) και οι νόμοι 2472/1997 (προστασία από επεξεργασία των προσωπικών δεδομένων) και 1858/1989 άρθ. 10 - 1868/1989 άρθ. 27 (τραπεζικό απόρρητο).

Συμπεράσματα

Κατά τη διάρκεια της εκπόνησης αυτής της διπλωματικής εργασίας και κατόπιν διεξαγωγής πολλαπλών ερευνών σχετικά με τη διασφάλιση της ιδιωτικότητας προέκυψαν τα παρακάτω συμπεράσματα:

- Τα όρια της ιδιωτικότητας και της προστασίας καθορίζονται από τεχνολογικούς παράγοντες, την παγκοσμιοποίηση της επεξεργασίας και της επικοινωνίας, τις αλλαγές των αντιλήψεων τόσο των ατόμων όσο και των κρατικών και κοινωνικών οργανώσεων ως προς το περιεχόμενο της ιδιωτικότητας όσο και ως προς τη σχέση της με άλλα δημόσια και ιδιωτικά αγαθά και επιδιώξεις
- Σημαντικός παράγοντας είναι η εμπιστοσύνη του υπεργολάβου σε συνάρτηση με τον οργανισμό που εργάζεται
- Πρέπει τα μέτρα να συνοδεύονται με συμφωνητικά εχεμύθειας και αυστηρές ρήτρες για την μη τήρηση της ιδιωτικότητας των πληροφοριών που επεξεργάζονται ή έρχονται σε επαφή
- Η εκπαίδευση των εργαζομένων στους οργανισμούς για την τήρηση των κανονισμών και τη διαχείριση του προσωπικού του υπεργολάβου είναι πολύ θετικό στην προστασία της ιδιωτικότητας των δεδομένων του οργανισμού
- Θα πρέπει να καλύπτεται ο νόμος περί επεξεργασίας των προσωπικών δεδομένων σε όλες τις περιπτώσεις και όλες οι σχετικές διατάξεις ελληνικού και ευρωπαϊκού δικαίου

Βιβλιογραφία

[1] Bassham E., et. al., *"Threat Assessment of Malicious Code and Human Threats",* National Institute of Standards and Technology, March 1994, [Online Article], Available at:http://csrc.nist.gov/publications/nistir/threats/subsubsection3_3_1_1.html

[2] Krebs B., *"A Short History of Computer Viruses and Attacks Washington Post"*, February 2003, [Online Article], Available at: http://www.washingtonpost.com/ac2/wp-dyn/A50636-2002Jun26?start=15&per=18

[3] TrendLabs, *"2009s most persistent malware threats",* March 2010, [Online Report], Available at: http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/2009s_most_persistent_malware_threats__march_2010_.pdf

[4] DarkReading, "*Social Engineering, the USB Way",* Security Dark Reading, June 2006, [Online Article], Available at: http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634

[5] Jones M., et. al., *"Protecting the Intranet against JavaScript Malware and Related Attacks",* Proceeding of ACM Detection of Intrusions and Malware, and Vulnerability Assessment, Vol. 4579 (2007), pp. 40-59., 2007, [Online Article], Available at: http://www.informatik.uni-hamburg.de/SVS/archiv/papers/2007_DIMVA_Johns_Winter_Anti_JS_Malware_lncs.pdf

[6] Goodin D., *"Three hospital worm infection dubbed 'substantive failure",* February 2009, [Online Article], Available at: http://www.theregister.co.uk/2009/02/02/nhs_worm_infection_aftermath/

[7] Miller C., *"Mass attacks on government, financial sites continue"*, July 2009, [Online Article], Available at: http://www.scmagazineus.com/mass-attacks-on-government-financial-sites-continue/article/139752/

[8] National Cyber-Security Advisory Council of Spain (CSACS), [Web Site], Available at: http://www.cnccs.es/

[9] Κομνηνός Θ., Σπυράκης Π., *"Ασφάλεια Δικτύων και Υπολογιστικών Συστημάτων"*, Εκδόσεις: Ελληνικά Γράμματα, 2002

[10] Zhang Y. et. al., *"The Effects of Threading, Infection Time, and Multiple-Attacker Collaboration on Malware Propagation",* 2009, [Online Article], Available at: http://www.iam.unibe.ch/~rvs/research/pub_files/YBH09.pdf

[11] Holz T. et. al., *"New threats and attacks on the world wide web",* New Threats and Attacks on the World Wide Web, 4(2):72–75, March 2006

[12] Computer Based Social Engineering Tools: Social Engineer Toolkit (SET), [Website], Available at: http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_%28SET

[13] CRAMM Version 5.1 User Guide

[14] "Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα", (συντάκτες Λαμπρινουδάκης Κ., Μήτρου Λ., Γκρίτζαλης Σ. και Κάτσικας Σ.), Εκδόσεις Παπασωτηρίου, Αθήνα, 2009

[15] Security threats scenarios in trust and reputation models for distributed systems. Fe´lix Go´mez Ma´rmol, Gregorio Martı´nez Pe´rez. 2009

[16] Threats to Information Systems: Today's Reality, Yesterday's Understanding. Karen D. Loch, Houston H. Carr and Merrill E. Warkentin. 2012 Available at: http://www.jstor.org/stable/249574?origin=JSTOR-pdf

[17] A Management Perspective on Risk of Security Threats to Information Systems. Springer Science + Business Media. 2005

[18] Data privacy by design: digital infrastructures for clinical collaborations. Majkic, Z. and Banerjee, R. and Zegzhda, D.P. and Wang, G. 2009

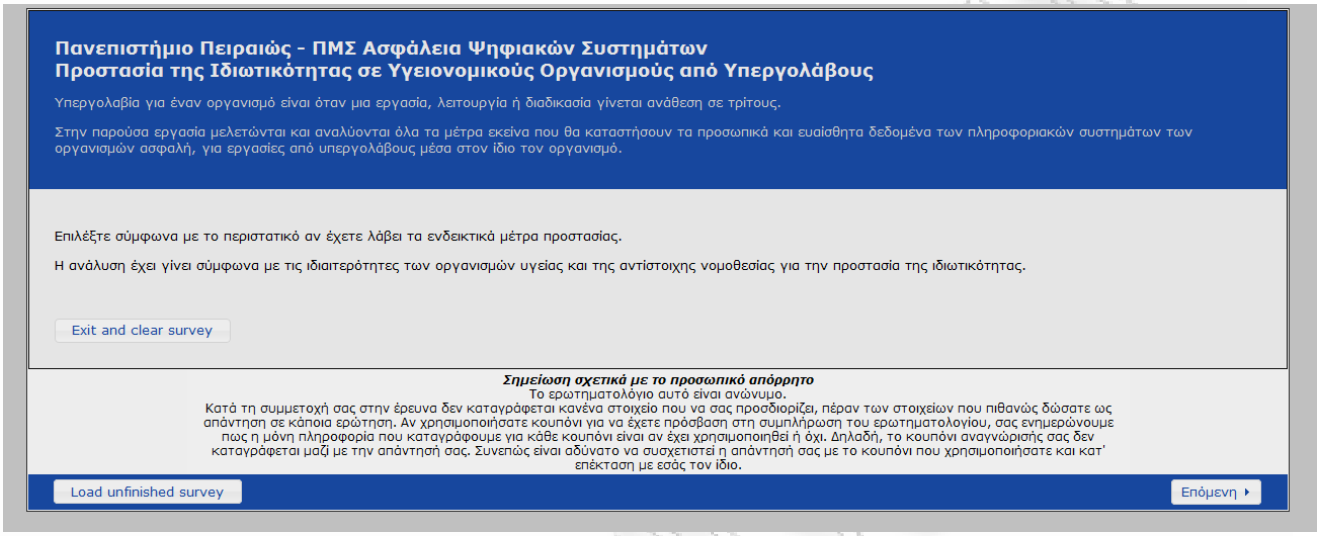
[19] ENEMY AT THE GATE: THREATS TO INFORMATION SECURITY. Michael E. Whitman. COMMUNICATIONS OF THE ACM. August 2003

[20] Security in Clinical Information Systems. Ross J Anderson. 2001

[21] k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY. LATANYA SWEENEY. 2002

Παράρτημα Α' – Ερωτηματολόγιο Υγειονομικών Οργανισμών

Ακολουθεί το ερωτηματολόγιο σε μορφή checklist για τον σχετικό οργανισμό:



Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Υγειονομικούς Οργανισμούς από Υπεργολάβους

Υπεργολαβία για έναν οργανισμό είναι όταν μια εργασία, λειτουργία ή διαδικασία γίνεται ανάθεση σε τρίτους.

Στην παρούσα εργασία μελετώνται και αναλύονται όλα τα μέτρα εκείνα που θα καταστήσουν τα προσωπικά και ευαίσθητα δεδομένα των πληροφοριακών συστημάτων των οργανισμών ασφαλή, για εργασίες από υπεργολάβους μέσα στον ίδιο τον οργανισμό.

Επιλέξτε σύμφωνα με το περιστατικό αν έχετε λάβει τα ενδεικτικά μέτρα προστασίας.

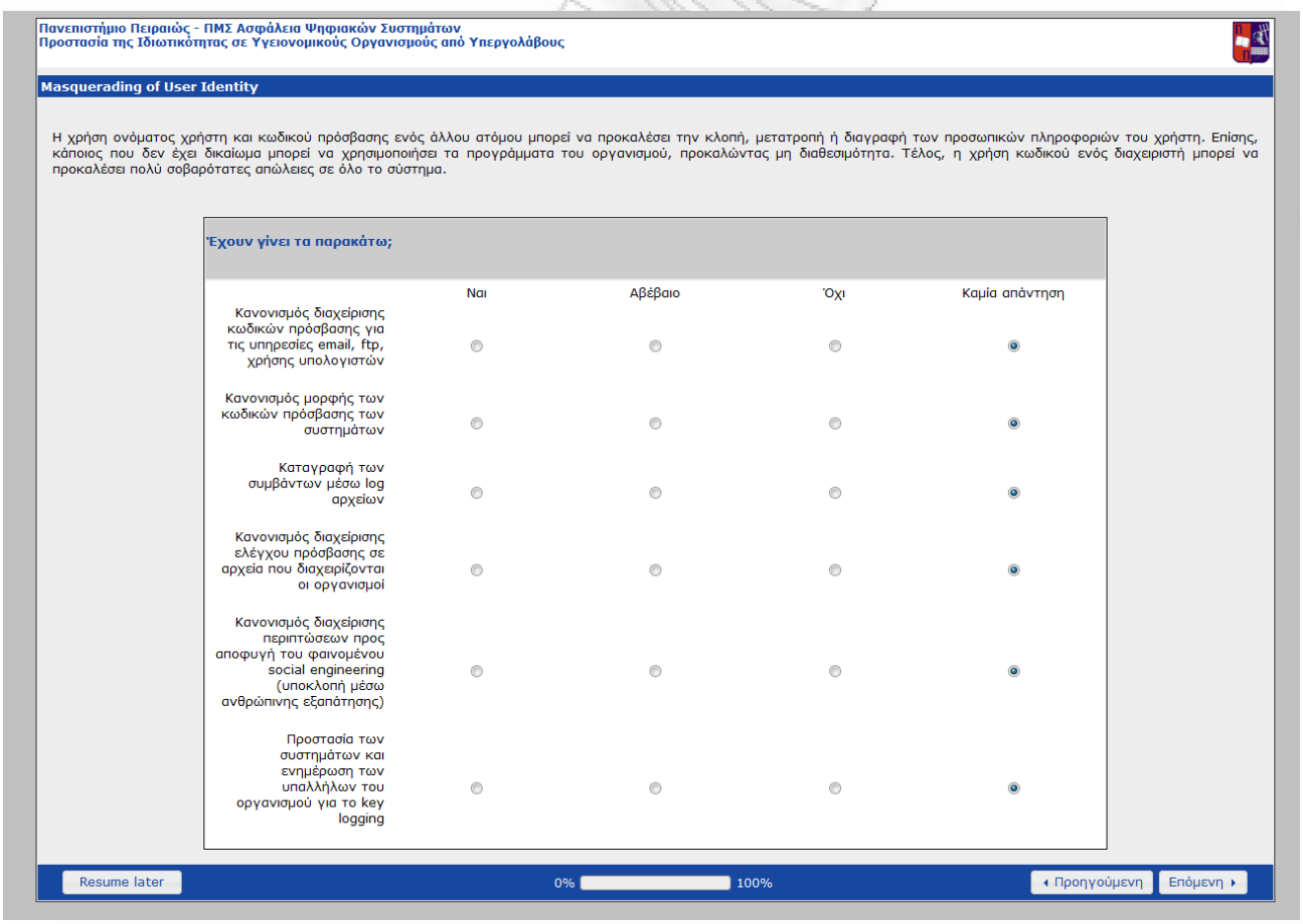
Η ανάλυση έχει γίνει σύμφωνα με τις ιδιαιτερότητες των οργανισμών υγείας και της αντίστοιχης νομοθεσίας για την προστασία της ιδιωτικότητας.

Exit and clear survey

Σημείωση σχετικά με το προσωπικό απόρρητο
Το ερωτηματολόγιο αυτό είναι ανώνυμο.
Κατά τη συμμετοχή σας στην έρευνα δεν καταγράφεται κανένα στοιχείο που να σας προσδιορίζει, πέραν των στοιχείων που πιθανώς δώσατε ως απάντηση σε κάποια ερώτηση. Αν χρησιμοποιήσατε κουπόνι για να έχετε πρόσβαση στη συμπλήρωση του ερωτηματολογίου, σας ενημερώνουμε πως η μόνη πληροφορία που καταγράφουμε για κάθε κουπόνι είναι αν έχει χρησιμοποιηθεί ή όχι. Δηλαδή, το κουπόνι αναγνώρισής σας δεν καταγράφεται μαζί με την απάντησή σας. Συνεπώς είναι αδύνατο να συσχετιστεί η απάντησή σας με το κουπόνι που χρησιμοποιήσατε και κατ' επέκταση με εσάς τον ίδιο.

Load unfinished survey

Επόμενη



Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Υγειονομικούς Οργανισμούς από Υπεργολάβους

Masquerading of User Identity

Η χρήση ονόματος χρήστη και κωδικού πρόσβασης ενός άλλου ατόμου μπορεί να προκαλέσει την κλοπή, μετατροπή ή διαγραφή των προσωπικών πληροφοριών του χρήστη. Επίσης, κάποιος που δεν έχει δικαίωμα μπορεί να χρησιμοποιήσει τα προγράμματα του οργανισμού, προκαλώντας μη διαθεσιμότητα. Τέλος, η χρήση κωδικού ενός διαχειριστή μπορεί να προκαλέσει πολύ σοβαρότατες απώλειες σε όλο το σύστημα.

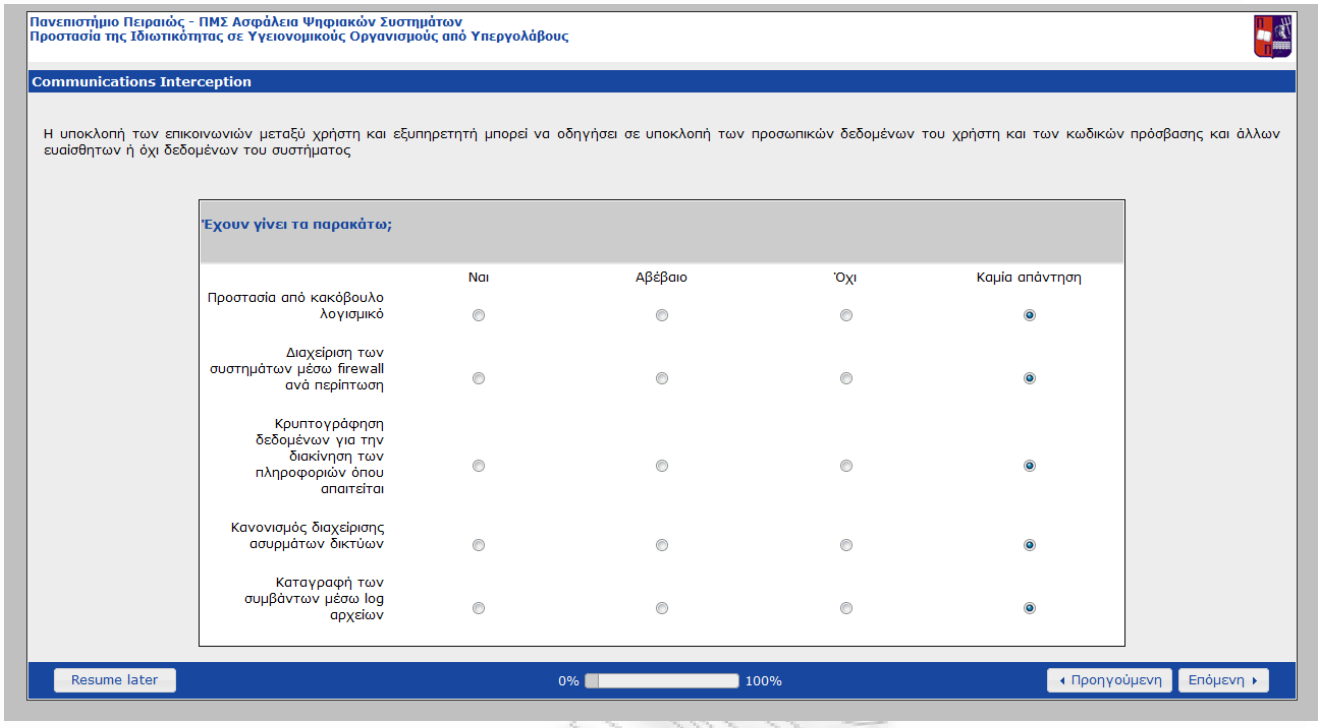
Έχουν γίνει τα παρακάτω;

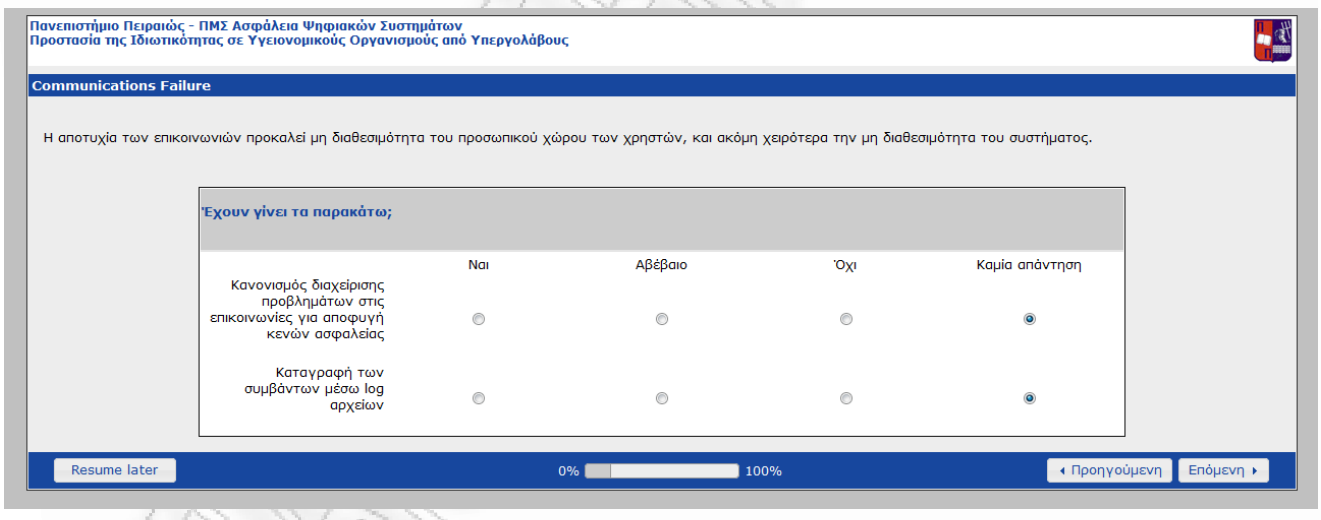
	Ναι	Αβέβαιο	Όχι	Καμία απάντηση
Κανονισμός διαχείρισης κωδικών πρόσβασης για τις υπηρεσίες email, ftp, χρήσης υπολογιστών	○	○	○	◉
Κανονισμός μορφής των κωδικών πρόσβασης των συστημάτων	○	○	○	◉
Καταγραφή των συμβάντων μέσω log αρχείων	○	○	○	◉
Κανονισμός διαχείρισης ελέγχου πρόσβασης σε αρχεία που διαχειρίζονται οι οργανισμοί	○	○	○	◉
Κανονισμός διαχείρισης περιπτώσεων προς αποφυγή του φαινομένου social engineering (υποκλοπή μέσω ανθρώπινης εξαπάτησης)	○	○	○	◉
Προστασία των συστημάτων και ενημέρωση των υπαλλήλων του οργανισμού για το key logging	○	○	○	◉

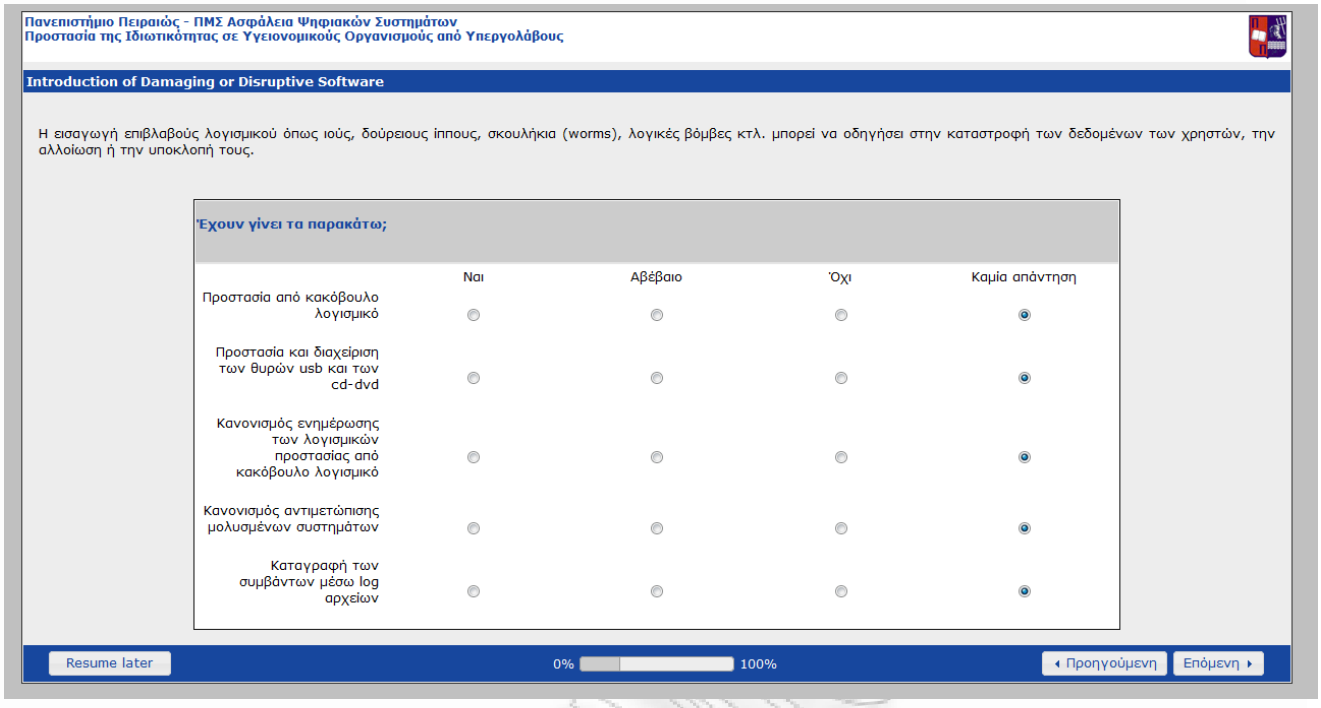
Resume later

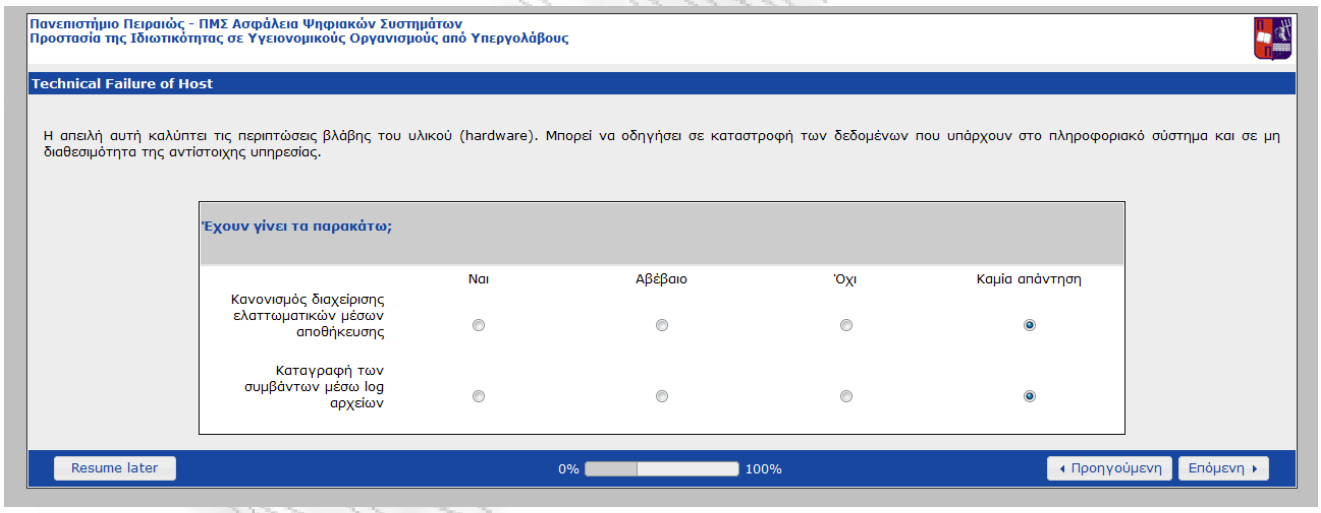
0% 100%

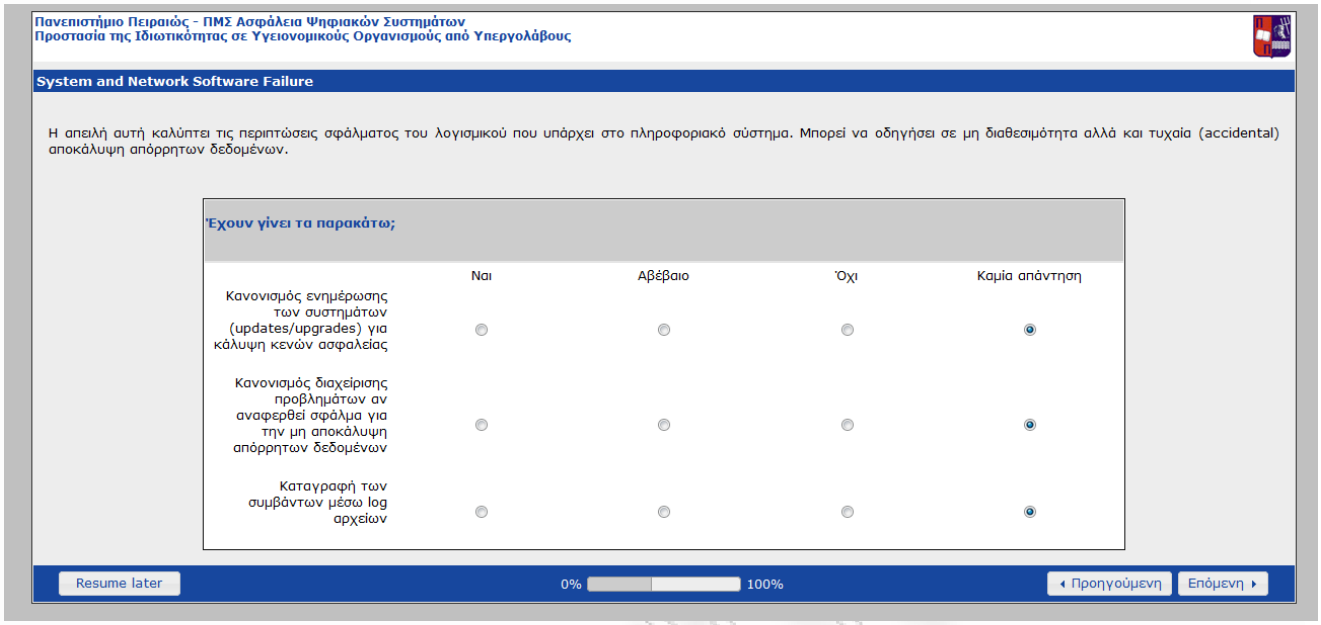
Προηγούμενη Επόμενη

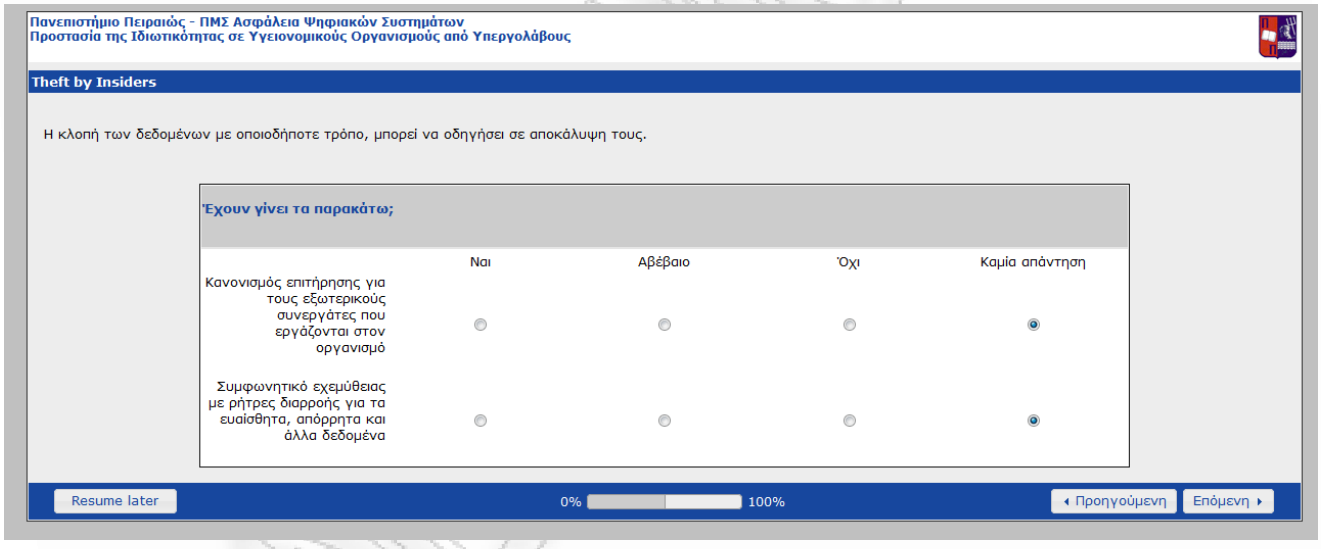

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Υγειονομικούς Οργανισμούς από Υπεργολάβους
Communications Interception
Η υποκλοπή των επικοινωνιών μεταξύ χρήστη και εξυπηρετητή μπορεί να οδηγήσει σε υποκλοπή των προσωπικών δεδομένων του χρήστη και των κωδικών πρόσβασης και άλλων ευαίσθητων ή όχι δεδομένων του συστήματος
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Προστασία από κακόβουλο λογισμικό
Διαχείριση των συστημάτων μέσω firewall ανά περίπτωση
Κρυπτογράφηση δεδομένων για την διακίνηση των πληροφοριών όπου απαιτείται
Κανονισμός διαχείρισης ασυρμάτων δικτύων
Καταγραφή των συμβάντων μέσω log αρχείων
Resume later
0%
100%
Προηγούμενη
Επόμενη

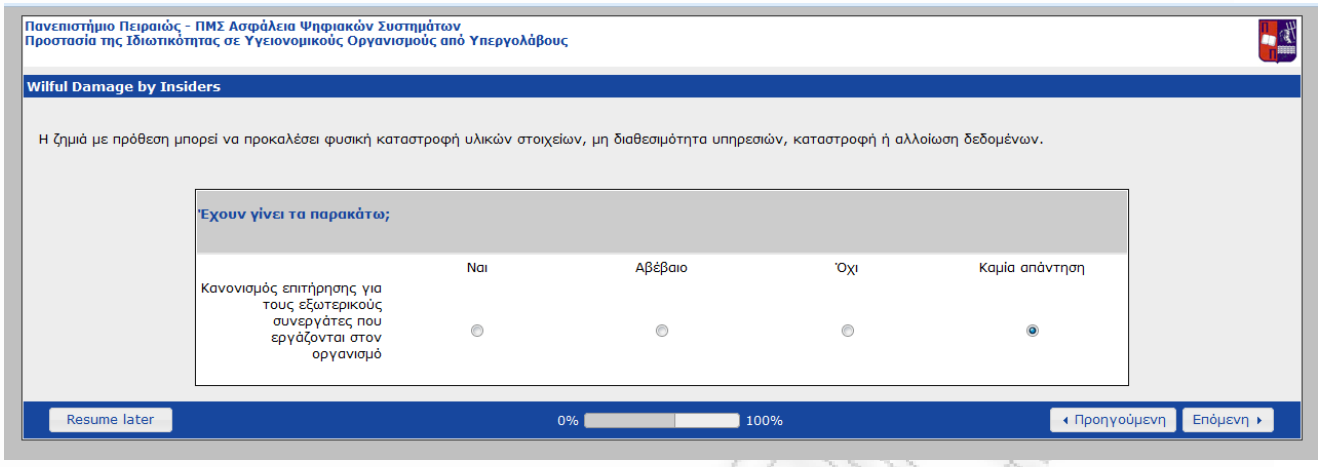

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Υγειονομικούς Οργανισμούς από Υπεργολάβους
Communications Failure
Η αποτυχία των επικοινωνιών προκαλεί μη διαθεσιμότητα του προσωπικού χώρου των χρηστών, και ακόμη χειρότερα την μη διαθεσιμότητα του συστήματος.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Κανονισμός διαχείρισης προβλημάτων στις επικοινωνίες για αποφυγή κενών ασφαλείας
Καταγραφή των συμβάντων μέσω log αρχείων
Resume later
0%
100%
Προηγούμενη
Επόμενη

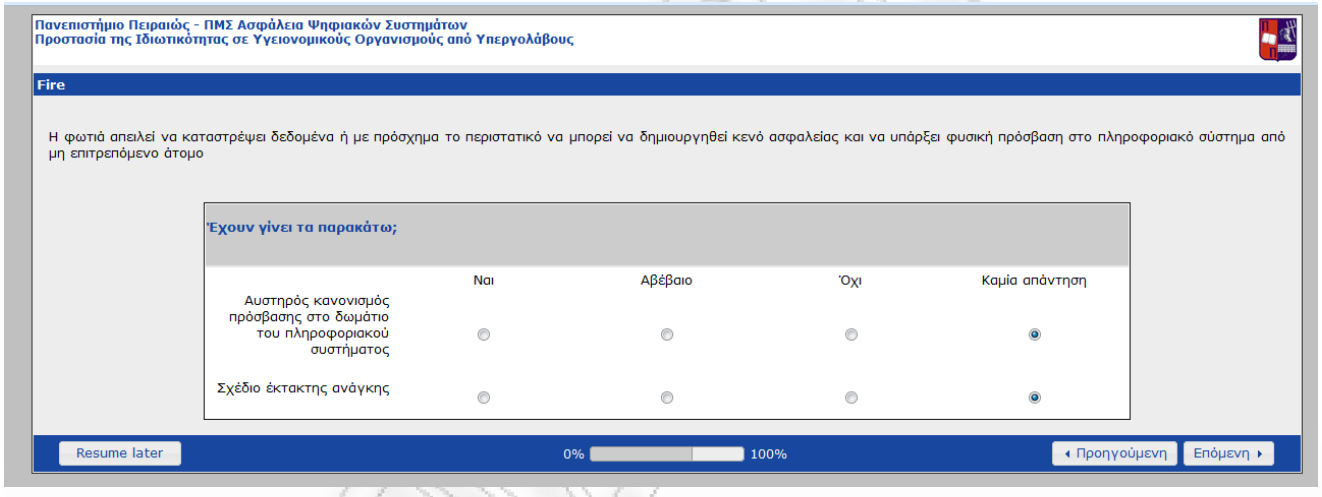

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Υγειονομικούς Οργανισμούς από Υπεργολάβους
Introduction of Damaging or Disruptive Software
Η εισαγωγή επιβλαβούς λογισμικού όπως ιούς, δούρειους ίππους, σκουλήκια (worms), λογικές βόμβες κτλ. μπορεί να οδηγήσει στην καταστροφή των δεδομένων των χρηστών, την αλλοίωση ή την υποκλοπή τους.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Προστασία από κακόβουλο λογισμικό
Προστασία και διαχείριση των θυρών usb και των cd-dvd
Κανονισμός ενημέρωσης των λογισμικών προστασίας από κακόβουλο λογισμικό
Κανονισμός αντιμετώπισης μολυσμένων συστημάτων
Καταγραφή των συμβάντων μέσω log αρχείων
Resume later
0%
100%
Προηγούμενη
Επόμενη

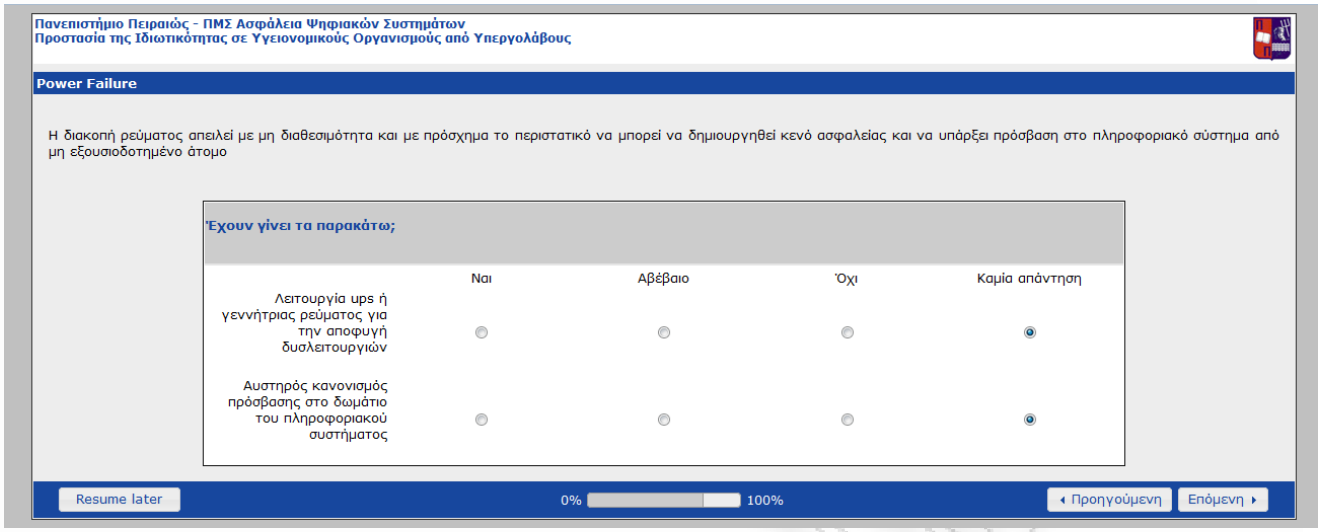

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Υγειονομικούς Οργανισμούς από Υπεργολάβους
Technical Failure of Host
Η απειλή αυτή καλύπτει τις περιπτώσεις βλάβης του υλικού (hardware). Μπορεί να οδηγήσει σε καταστροφή των δεδομένων που υπάρχουν στο πληροφοριακό σύστημα και σε μη διαθεσιμότητα της αντίστοιχης υπηρεσίας.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Κανονισμός διαχείρισης ελαττωματικών μέσων αποθήκευσης
Καταγραφή των συμβάντων μέσω log αρχείων
Resume later
0%
100%
Προηγούμενη
Επόμενη

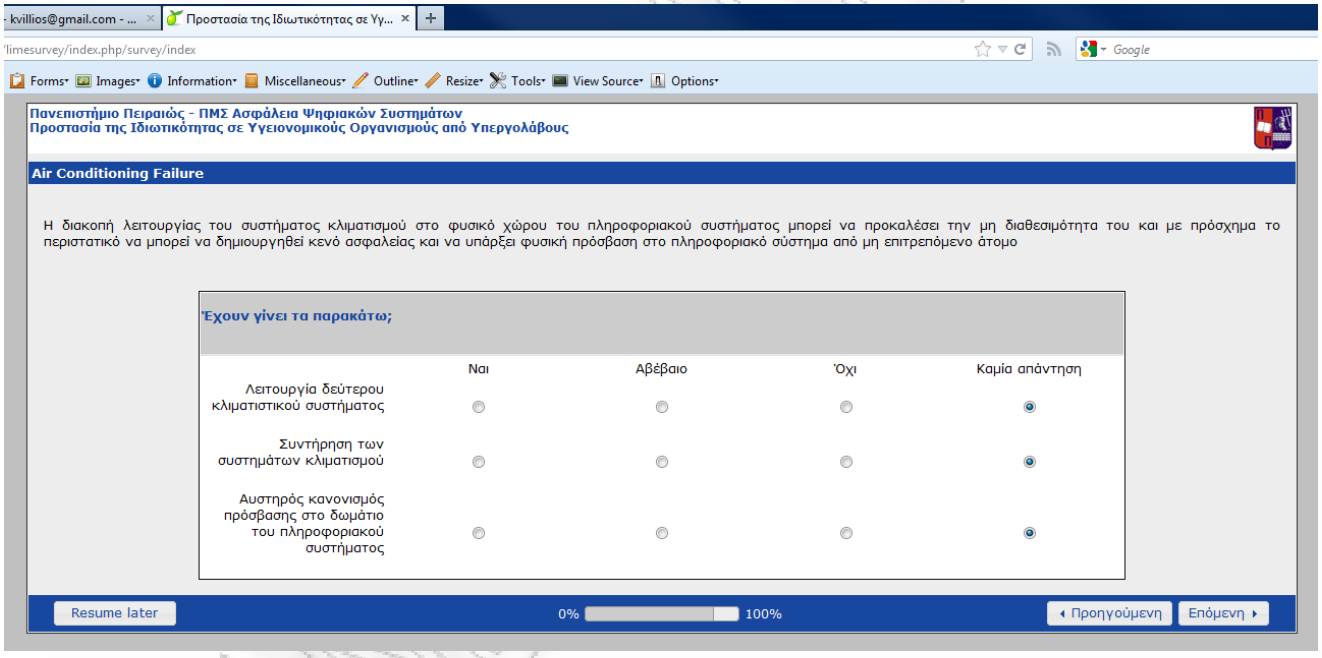

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Υγειονομικούς Οργανισμούς από Υπεργολάβους
System and Network Software Failure
Η απειλή αυτή καλύπτει τις περιπτώσεις σφάλματος του λογισμικού που υπάρχει στο πληροφοριακό σύστημα. Μπορεί να οδηγήσει σε μη διαθεσιμότητα αλλά και τυχαία (accidental) αποκάλυψη απόρρητων δεδομένων.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Κανονισμός ενημέρωσης των συστημάτων (updates/upgrades) για κάλυψη κενών ασφαλείας
Κανονισμός διαχείρισης προβλημάτων αν αναφερθεί σφάλμα για την μη αποκάλυψη απόρρητων δεδομένων
Καταγραφή των συμβάντων μέσω log αρχείων
Resume later
0%
100%
Προηγούμενη
Επόμενη

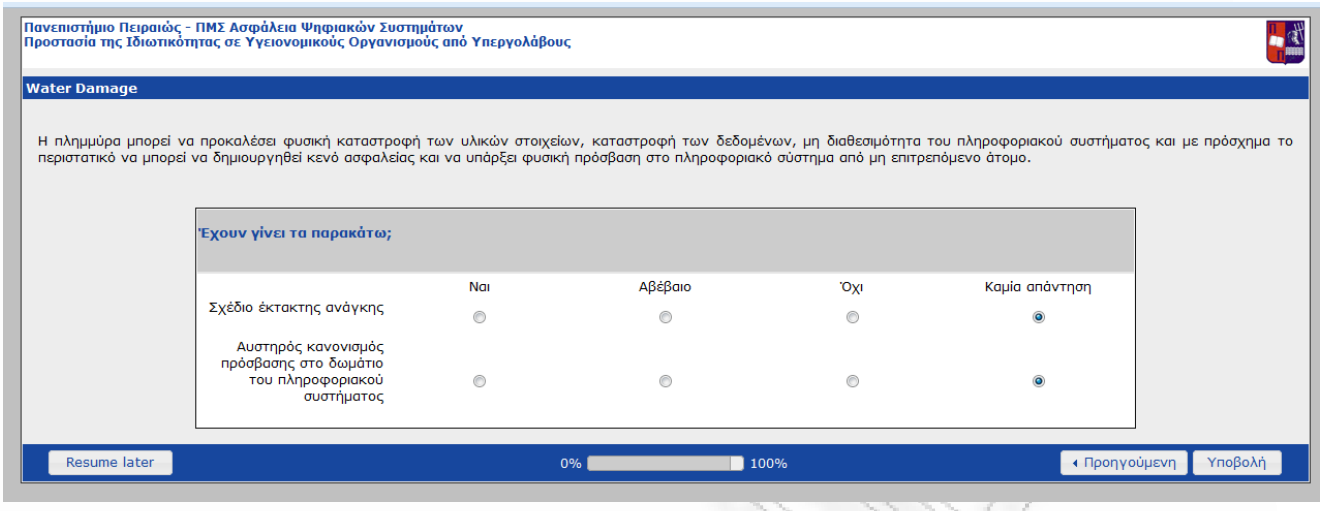

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Υγειονομικούς Οργανισμούς από Υπεργολάβους
Theft by Insiders
Η κλοπή των δεδομένων με οποιοδήποτε τρόπο, μπορεί να οδηγήσει σε αποκάλυψη τους.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Κανονισμός επιτήρησης για τους εξωτερικούς συνεργάτες που εργάζονται στον οργανισμό
Συμφωνητικό εχεμύθειας με ρήτρες διαρροής για τα ευαίσθητα, απόρρητα και άλλα δεδομένα
Resume later
0%
100%
Προηγούμενη
Επόμενη

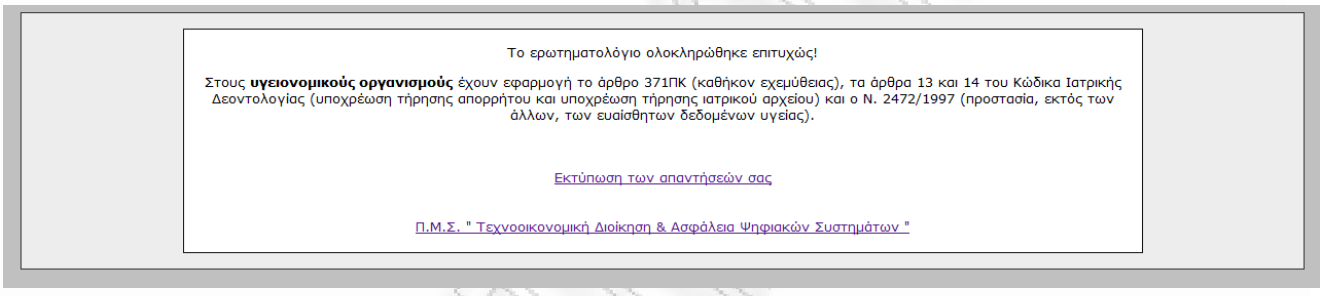

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Υγειονομικούς Οργανισμούς από Υπεργολάβους
Wilful Damage by Insiders
Η ζημιά με πρόθεση μπορεί να προκαλέσει φυσική καταστροφή υλικών στοιχείων, μη διαθεσιμότητα υπηρεσιών, καταστροφή ή αλλοίωση δεδομένων.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Κανονισμός επιτήρησης για τους εξωτερικούς συνεργάτες που εργάζονται στον οργανισμό
Resume later
0%
100%
Προηγούμενη
Επόμενη


Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Υγειονομικούς Οργανισμούς από Υπεργολάβους
Fire
Η φωτιά απειλεί να καταστρέψει δεδομένα ή με πρόσχημα το περιστατικό να μπορεί να δημιουργηθεί κενό ασφαλείας και να υπάρξει φυσική πρόσβαση στο πληροφοριακό σύστημα από μη επιτρεπόμενο άτομο
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Αυστηρός κανονισμός πρόσβασης στο δωμάτιο του πληροφοριακού συστήματος
Σχέδιο έκτακτης ανάγκης
Resume later
0%
100%
Προηγούμενη
Επόμενη


Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Υγειονομικούς Οργανισμούς από Υπεργολάβους
Power Failure
Η διακοπή ρεύματος απειλεί με μη διαθεσιμότητα και με πρόσχημα το περιστατικό να μπορεί να δημιουργηθεί κενό ασφαλείας και να υπάρξει πρόσβαση στο πληροφοριακό σύστημα από μη εξουσιοδοτημένο άτομο
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Λειτουργία ups ή γεννήτριας ρεύματος για την αποφυγή δυσλειτουργιών
Αυστηρός κανονισμός πρόσβασης στο δωμάτιο του πληροφοριακού συστήματος
Resume later
0%
100%
Προηγούμενη
Επόμενη

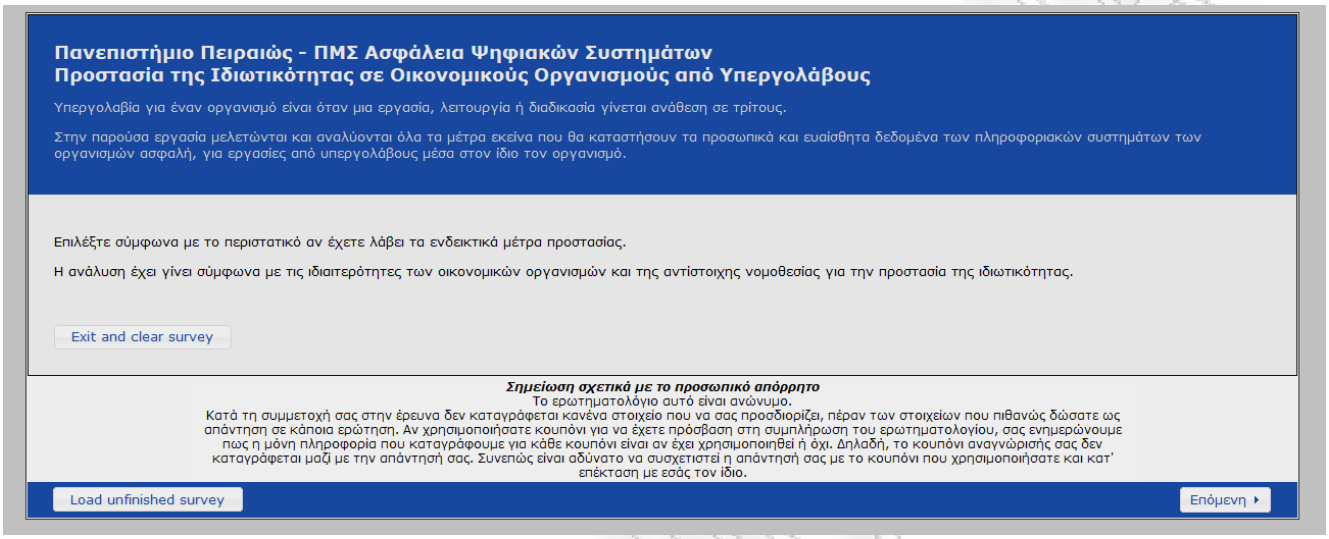

kvillios@gmail.com - ...
Προστασία της Ιδιωτικότητας σε Υγ...
limesurvey/index.php/survey/index
Forms
Images
Information
Miscellaneous
Outline
Resize
Tools
View Source
Options
Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Υγειονομικούς Οργανισμούς από Υπεργολάβους
Air Conditioning Failure
Η διακοπή λειτουργίας του συστήματος κλιματισμού στο φυσικό χώρου του πληροφοριακού συστήματος μπορεί να προκαλέσει την μη διαθεσιμότητα του και με πρόσχημα το περιστατικό να μπορεί να δημιουργηθεί κενό ασφαλείας και να υπάρξει φυσική πρόσβαση στο πληροφοριακό σύστημα από μη επιτρεπόμενο άτομο
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Λειτουργία δεύτερου κλιματιστικού συστήματος
Συντήρηση των συστημάτων κλιματισμού
Αυστηρός κανονισμός πρόσβασης στο δωμάτιο του πληροφοριακού συστήματος
Resume later
0%
100%
Προηγούμενη
Επόμενη

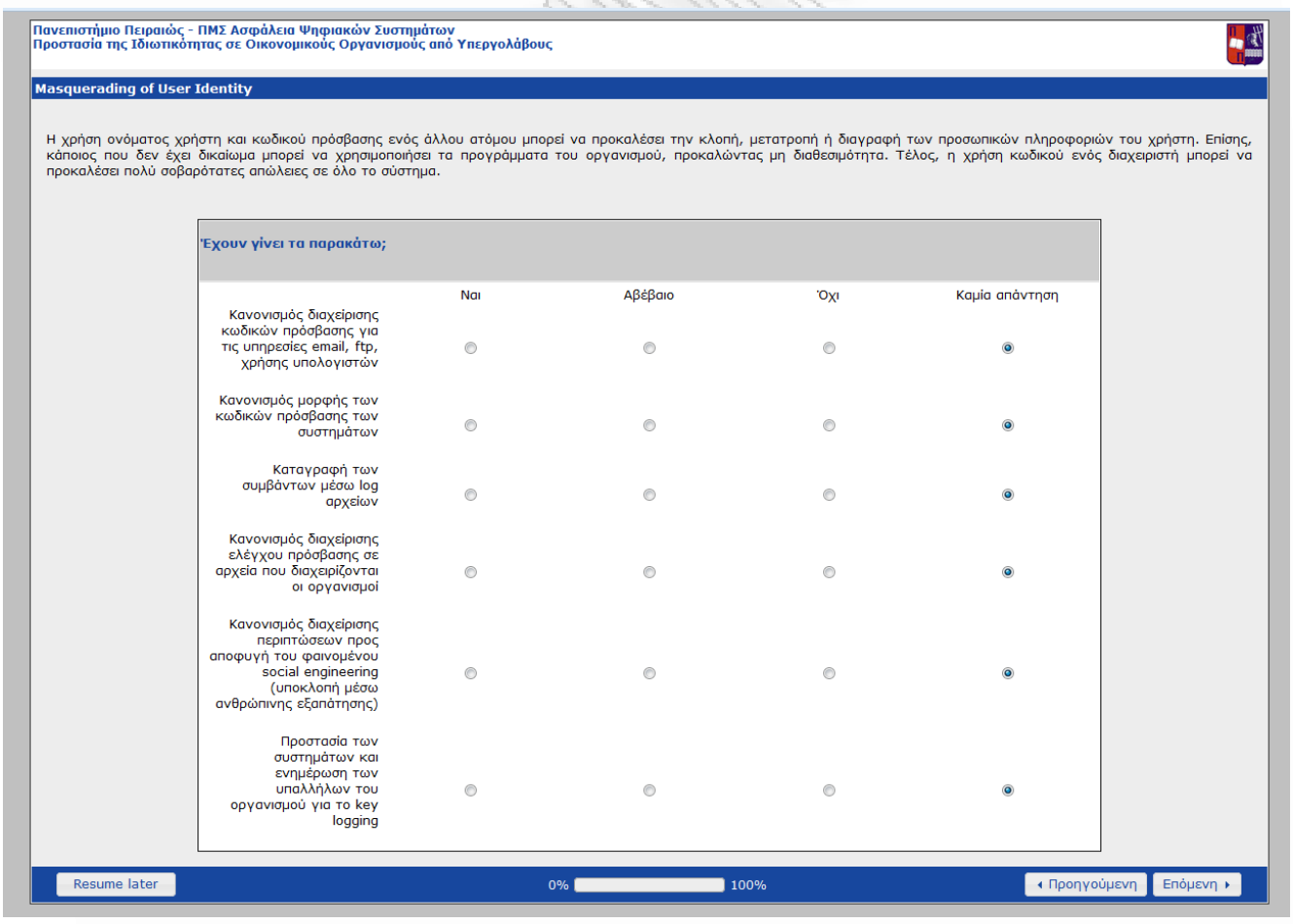

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Υγειονομικούς Οργανισμούς από Υπεργολάβους
Water Damage
Η πλημμύρα μπορεί να προκαλέσει φυσική καταστροφή των υλικών στοιχείων, καταστροφή των δεδομένων, μη διαθεσιμότητα του πληροφοριακού συστήματος και με πρόσχημα το περιστατικό να μπορεί να δημιουργηθεί κενό ασφαλείας και να υπάρξει φυσική πρόσβαση στο πληροφοριακό σύστημα από μη επιτρεπόμενο άτομο.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Σχέδιο έκτακτης ανάγκης
Αυστηρός κανονισμός πρόσβασης στο δωμάτιο του πληροφοριακού συστήματος
Resume later
0%
100%
Προηγούμενη
Υποβολή

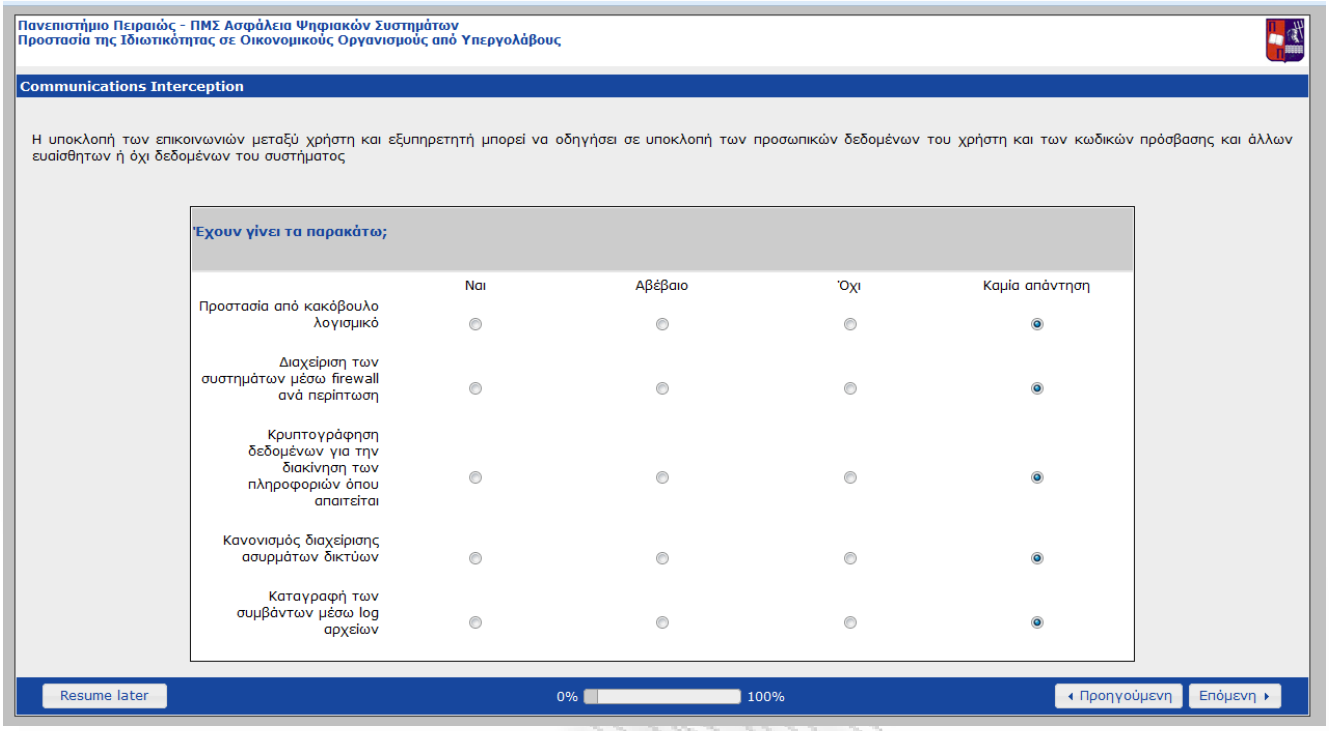

Το ερωτηματολόγιο ολοκληρώθηκε επιτυχώς!
Στους **υγειονομικούς οργανισμούς** έχουν εφαρμογή το άρθρο 371ΠΚ (καθήκον εχεμύθειας), τα άρθρα 13 και 14 του Κώδικα Ιατρικής Δεοντολογίας (υποχρέωση τήρησης απορρήτου και υποχρέωση τήρησης ιατρικού αρχείου) και ο Ν. 2472/1997 (προστασία, εκτός των άλλων, των ευαίσθητων δεδομένων υγείας).
Εκτύπωση των απαντήσεών σας
Π.Μ.Σ. " Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων "

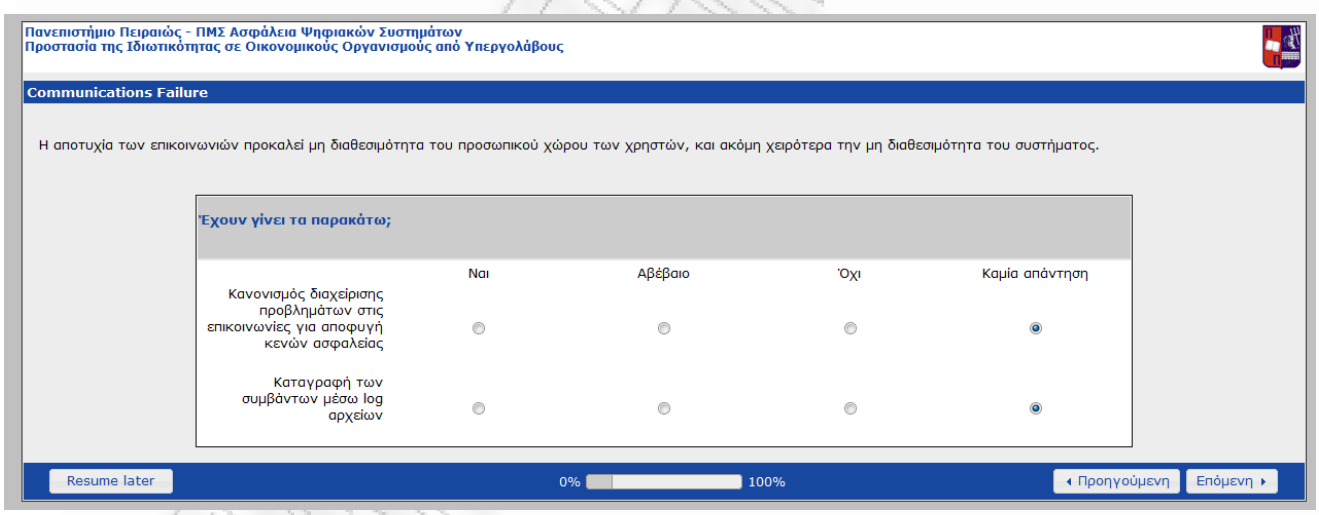
Παράρτημα Β' – Ερωτηματολόγιο Οικονομικών Οργανισμών

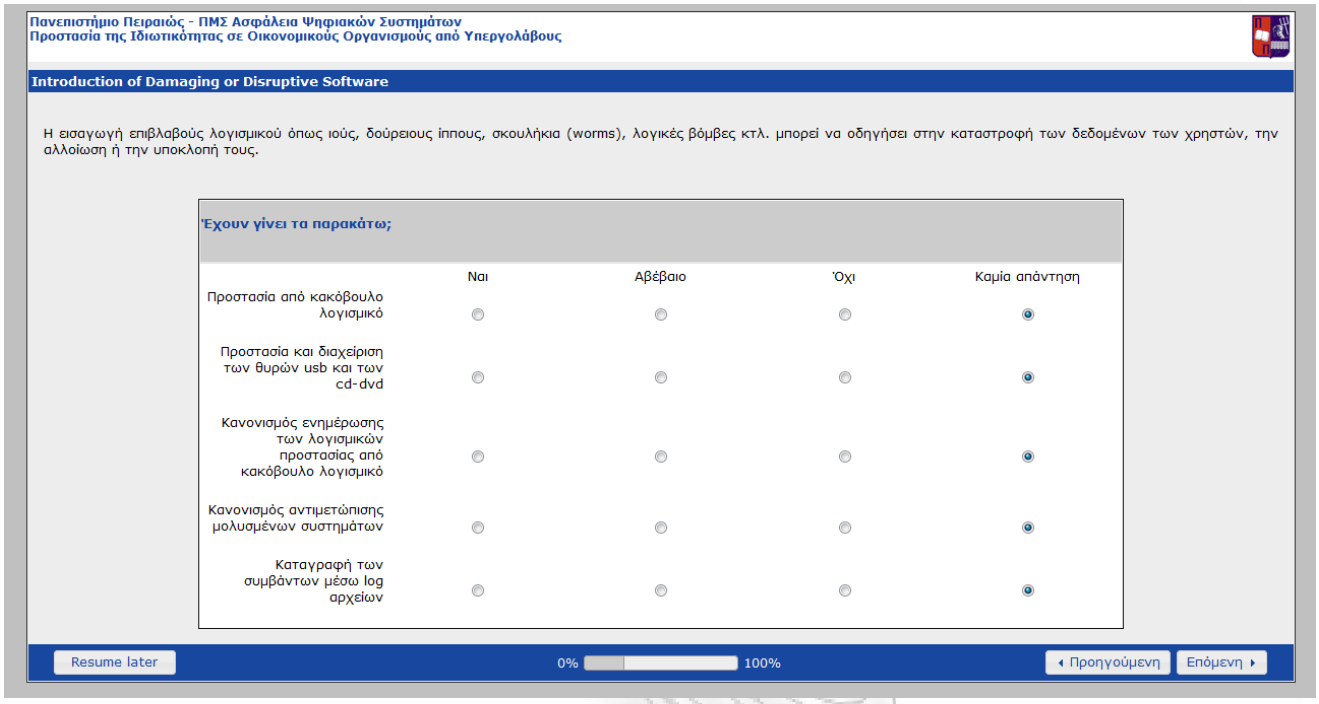
Ακολουθεί το ερωτηματολόγιο σε μορφή checklist για τον σχετικό οργανισμό:

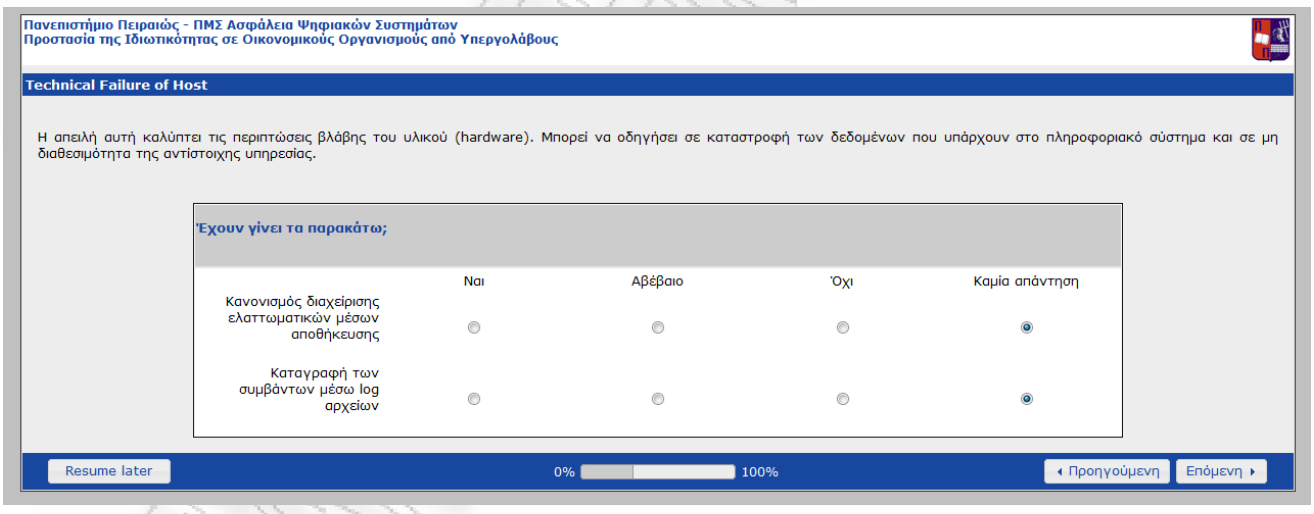


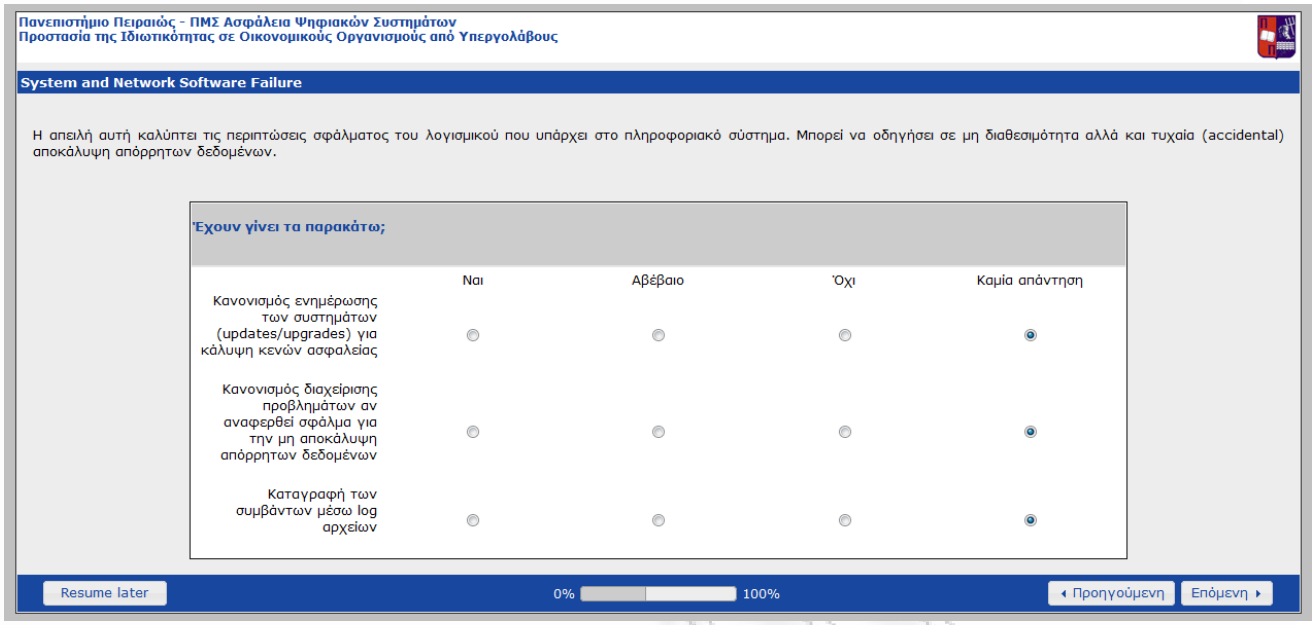


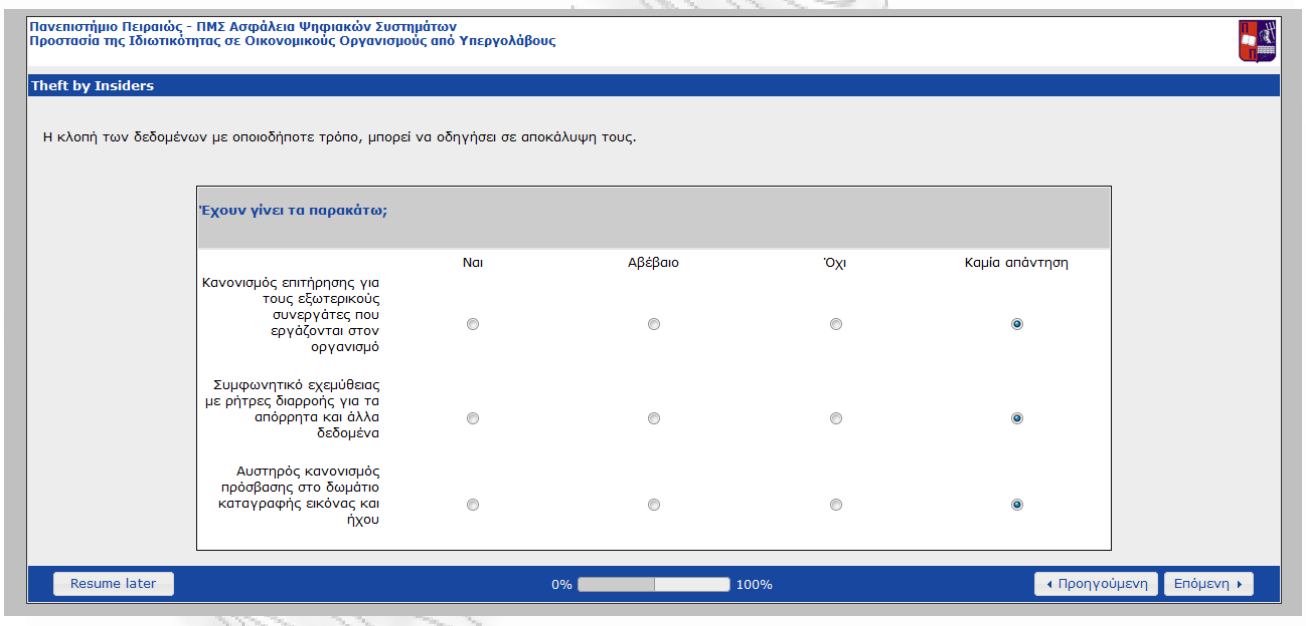

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Οικονομικούς Οργανισμούς από Υπεργολάβους
Communications Interception
Η υποκλοπή των επικοινωνιών μεταξύ χρήστη και εξυπηρετητή μπορεί να οδηγήσει σε υποκλοπή των προσωπικών δεδομένων του χρήστη και των κωδικών πρόσβασης και άλλων ευαίσθητων ή όχι δεδομένων του συστήματος
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Προστασία από κακόβουλο λογισμικό
Διαχείριση των συστημάτων μέσω firewall ανά περίπτωση
Κρυπτογράφηση δεδομένων για την διακίνηση των πληροφοριών όπου απαιτείται
Κανονισμός διαχείρισης ασυρμάτων δικτύων
Καταγραφή των συμβάντων μέσω log αρχείων
Resume later
0%
100%
Προηγούμενη
Επόμενη

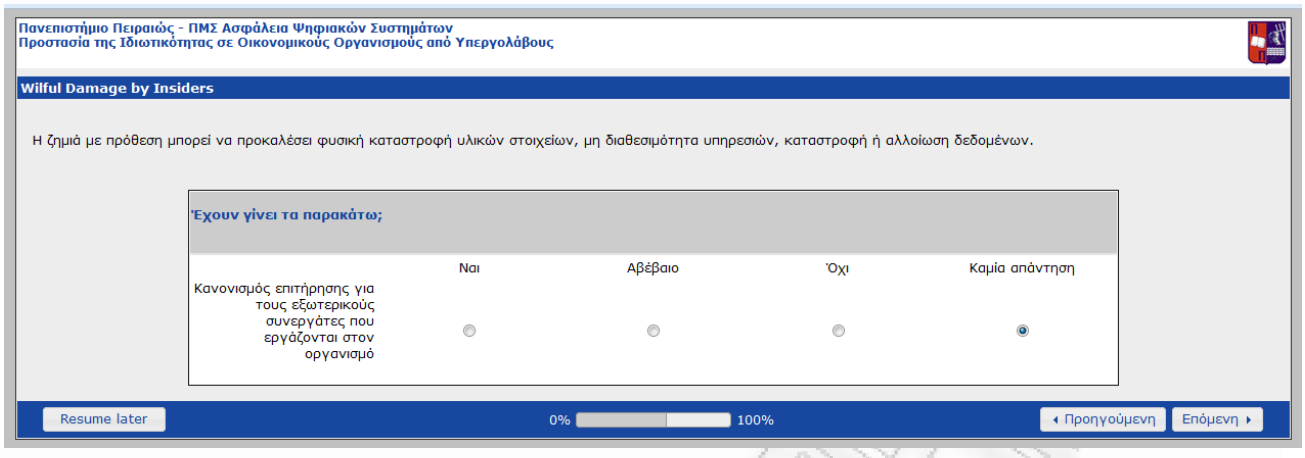

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Οικονομικούς Οργανισμούς από Υπεργολάβους
Communications Failure
Η αποτυχία των επικοινωνιών προκαλεί μη διαθεσιμότητα του προσωπικού χώρου των χρηστών, και ακόμη χειρότερα την μη διαθεσιμότητα του συστήματος.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Κανονισμός διαχείρισης προβλημάτων στις επικοινωνίες για αποφυγή κενών ασφαλείας
Καταγραφή των συμβάντων μέσω log αρχείων
Resume later
0%
100%
Προηγούμενη
Επόμενη

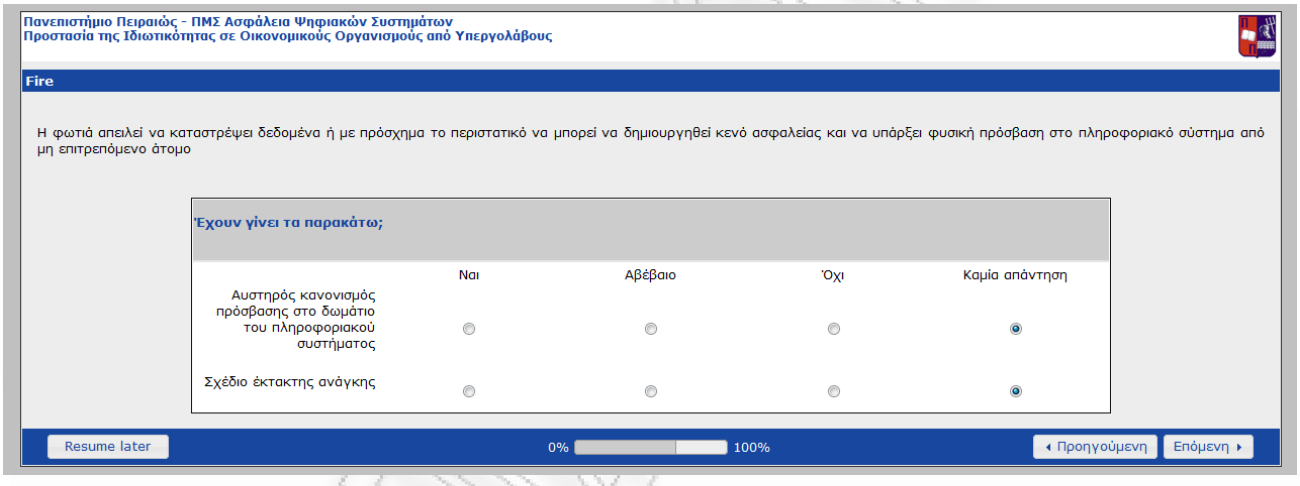

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Οικονομικούς Οργανισμούς από Υπεργολάβους
Introduction of Damaging or Disruptive Software
Η εισαγωγή επιβλαβούς λογισμικού όπως ιούς, δούρειους ίππους, σκουλήκια (worms), λογικές βόμβες κτλ. μπορεί να οδηγήσει στην καταστροφή των δεδομένων των χρηστών, την αλλοίωση ή την υποκλοπή τους.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Προστασία από κακόβουλο λογισμικό
Προστασία και διαχείριση των θυρών usb και των cd-dvd
Κανονισμός ενημέρωσης των λογισμικών προστασίας από κακόβουλο λογισμικό
Κανονισμός αντιμετώπισης μολυσμένων συστημάτων
Καταγραφή των συμβάντων μέσω log αρχείων
Resume later
0%
100%
Προηγούμενη
Επόμενη

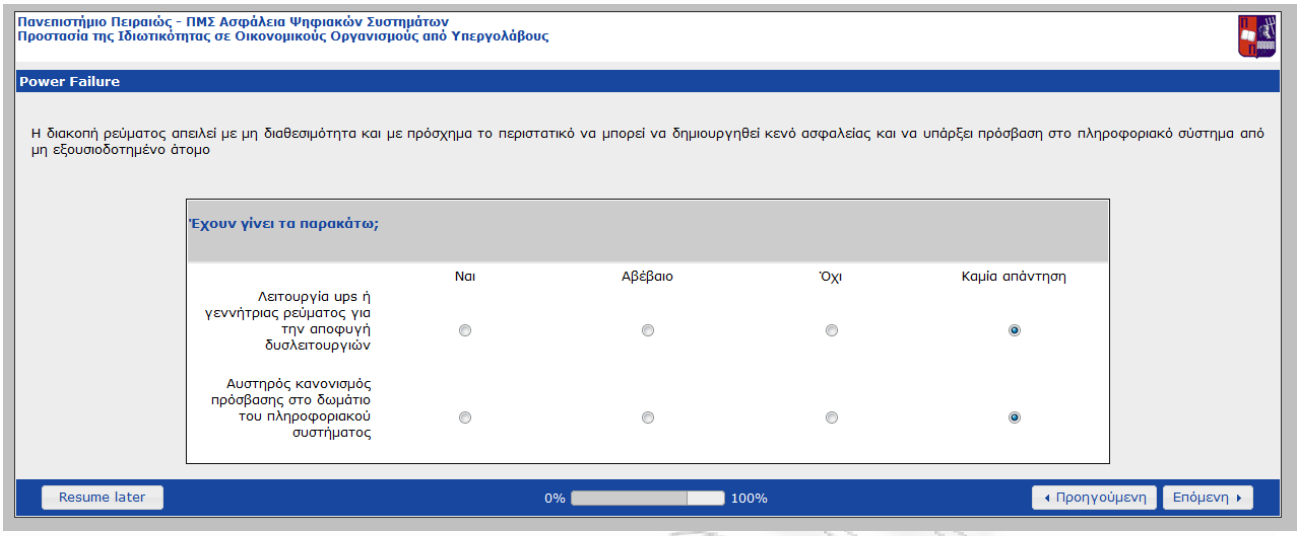

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Οικονομικούς Οργανισμούς από Υπεργολάβους
Technical Failure of Host
Η απειλή αυτή καλύπτει τις περιπτώσεις βλάβης του υλικού (hardware). Μπορεί να οδηγήσει σε καταστροφή των δεδομένων που υπάρχουν στο πληροφοριακό σύστημα και σε μη διαθεσιμότητα της αντίστοιχης υπηρεσίας.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Κανονισμός διαχείρισης ελαττωματικών μέσων αποθήκευσης
Καταγραφή των συμβάντων μέσω log αρχείων
Resume later
0%
100%
Προηγούμενη
Επόμενη

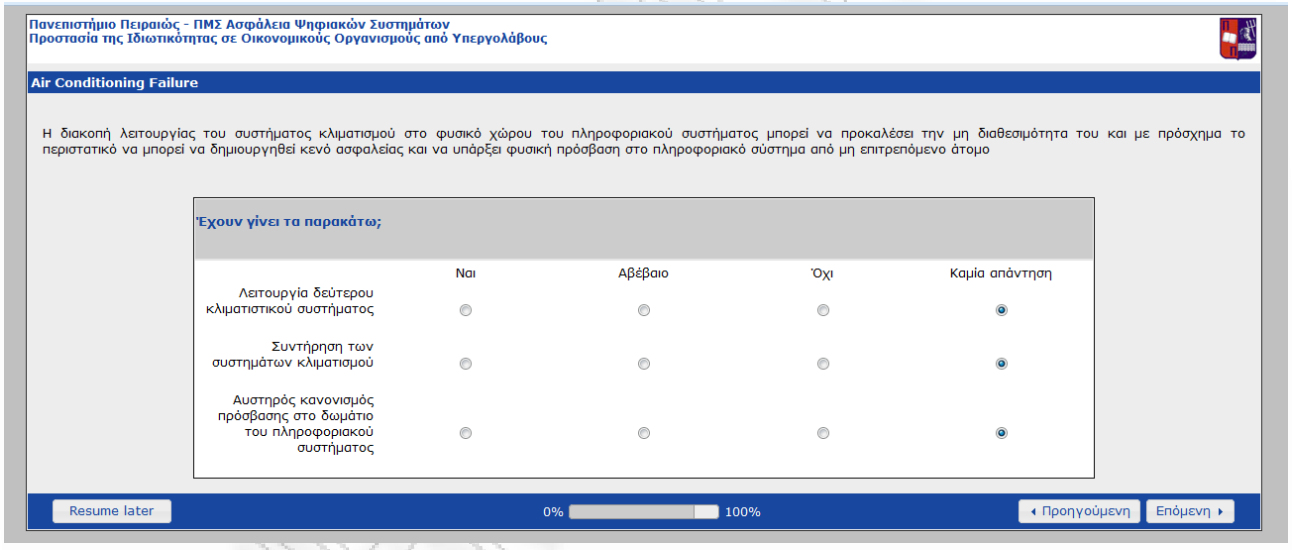

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Οικονομικούς Οργανισμούς από Υπεργολάβους
System and Network Software Failure
Η απειλή αυτή καλύπτει τις περιπτώσεις σφάλματος του λογισμικού που υπάρχει στο πληροφοριακό σύστημα. Μπορεί να οδηγήσει σε μη διαθεσιμότητα αλλά και τυχαία (accidental) αποκάλυψη απόρρητων δεδομένων.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Κανονισμός ενημέρωσης των συστημάτων (updates/upgrades) για κάλυψη κενών ασφαλείας
Κανονισμός διαχείρισης προβλημάτων αν αναφερθεί σφάλμα για την μη αποκάλυψη απόρρητων δεδομένων
Καταγραφή των συμβάντων μέσω log αρχείων
Resume later
0%
100%
Προηγούμενη
Επόμενη

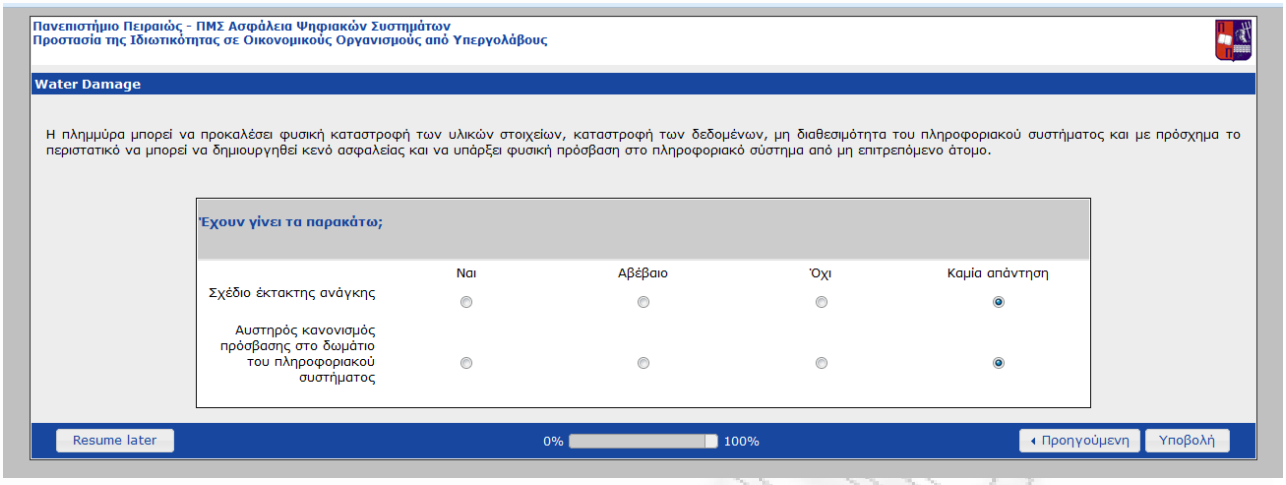

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Οικονομικούς Οργανισμούς από Υπεργολάβους
Theft by Insiders
Η κλοπή των δεδομένων με οποιοδήποτε τρόπο, μπορεί να οδηγήσει σε αποκάλυψη τους.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Κανονισμός επιτήρησης για τους εξωτερικούς συνεργάτες που εργάζονται στον οργανισμό
Συμφωνητικό εχεμύθειας με ρήτρες διαρροής για τα απόρρητα και άλλα δεδομένα
Αυστηρός κανονισμός πρόσβασης στο δωμάτιο καταγραφής εικόνας και ήχου
Resume later
0%
100%
Προηγούμενη
Επόμενη

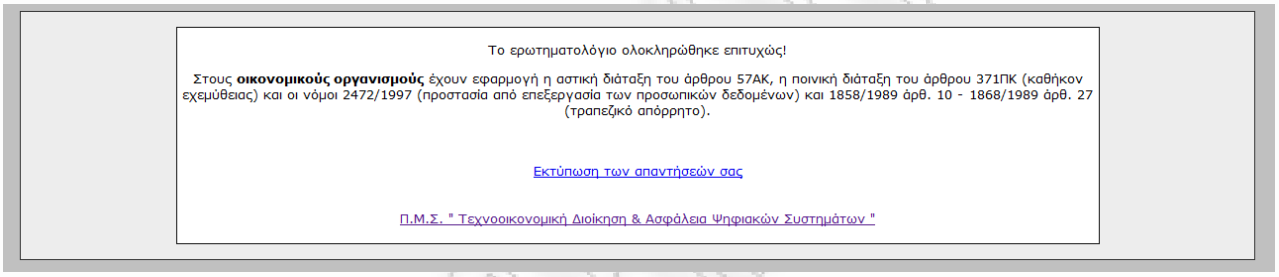

Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Οικονομικούς Οργανισμούς από Υπεργολάβους
Wilful Damage by Insiders
Η ζημιά με πρόθεση μπορεί να προκαλέσει φυσική καταστροφή υλικών στοιχείων, μη διαθεσιμότητα υπηρεσιών, καταστροφή ή αλλοίωση δεδομένων.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Κανονισμός επιτήρησης για τους εξωτερικούς συνεργάτες που εργάζονται στον οργανισμό
Resume later
0%
100%
Προηγούμενη
Επόμενη


Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Οικονομικούς Οργανισμούς από Υπεργολάβους
Fire
Η φωτιά απειλεί να καταστρέψει δεδομένα ή με πρόσχημα το περιστατικό να μπορεί να δημιουργηθεί κενό ασφαλείας και να υπάρξει φυσική πρόσβαση στο πληροφοριακό σύστημα από μη επιτρεπόμενο άτομο
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Αυστηρός κανονισμός πρόσβασης στο δωμάτιο του πληροφοριακού συστήματος
Σχέδιο έκτακτης ανάγκης
Resume later
0%
100%
Προηγούμενη
Επόμενη


Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Οικονομικούς Οργανισμούς από Υπεργολάβους
Power Failure
Η διακοπή ρεύματος απειλεί με μη διαθεσιμότητα και με πρόσχημα το περιστατικό να μπορεί να δημιουργηθεί κενό ασφαλείας και να υπάρξει πρόσβαση στο πληροφοριακό σύστημα από μη εξουσιοδοτημένο άτομο
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Λειτουργία ups ή γεννήτριας ρεύματος για την αποφυγή δυσλειτουργιών
Αυστηρός κανονισμός πρόσβασης στο δωμάτιο του πληροφοριακού συστήματος
Resume later
0%
100%
Προηγούμενη
Επόμενη


Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Οικονομικούς Οργανισμούς από Υπεργολάβους
Air Conditioning Failure
Η διακοπή λειτουργίας του συστήματος κλιματισμού στο φυσικό χώρου του πληροφοριακού συστήματος μπορεί να προκαλέσει την μη διαθεσιμότητα του και με πρόσχημα το περιστατικό να μπορεί να δημιουργηθεί κενό ασφαλείας και να υπάρξει φυσική πρόσβαση στο πληροφοριακό σύστημα από μη επιτρεπόμενο άτομο
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Λειτουργία δεύτερου κλιματιστικού συστήματος
Συντήρηση των συστημάτων κλιματισμού
Αυστηρός κανονισμός πρόσβασης στο δωμάτιο του πληροφοριακού συστήματος
Resume later
0%
100%
Προηγούμενη
Επόμενη


Πανεπιστήμιο Πειραιώς - ΠΜΣ Ασφάλεια Ψηφιακών Συστημάτων
Προστασία της Ιδιωτικότητας σε Οικονομικούς Οργανισμούς από Υπεργολάβους
Water Damage
Η πλημμύρα μπορεί να προκαλέσει φυσική καταστροφή των υλικών στοιχείων, καταστροφή των δεδομένων, μη διαθεσιμότητα του πληροφοριακού συστήματος και με πρόσχημα το περιστατικό να μπορεί να δημιουργηθεί κενό ασφαλείας και να υπάρξει φυσική πρόσβαση στο πληροφοριακό σύστημα από μη επιτρεπόμενο άτομο.
Έχουν γίνει τα παρακάτω;
Ναι
Αβέβαιο
Όχι
Καμία απάντηση
Σχέδιο έκτακτης ανάγκης
Αυστηρός κανονισμός πρόσβασης στο δωμάτιο του πληροφοριακού συστήματος
Resume later
0%
100%
Προηγούμενη
Υποβολή


Το ερωτηματολόγιο ολοκληρώθηκε επιτυχώς!
Στους **οικονομικούς οργανισμούς** έχουν εφαρμογή η αστική διάταξη του άρθρου 57ΑΚ, η ποινική διάταξη του άρθρου 371ΠΚ (καθήκον εχεμύθειας) και οι νόμοι 2472/1997 (προστασία από επεξεργασία των προσωπικών δεδομένων) και 1858/1989 άρθ. 10 - 1868/1989 άρθ. 27 (τραπεζικό απόρρητο).
Εκτύπωση των απαντήσεών σας
Π.Μ.Σ. " Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων "