Πανεπιστήμιο Αιγαίου

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

321-3404 Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Διδάσκων: Καρύδα Μαρία , Καμπουράκης Γεώργιος

Αποτίμηση & Διαχείριση Επικινδυνότητας

Εργαστηριακοί Συνεργάτες : Νίκος Αλεξίου & Αλέξανδρος Φακής

Μέλη Ομάδας

Αντωνιάδης Χαράλαμπος icsd10011

Ευκαρπίδης Κωνσταντίνος icsd15051

Ζιώζας Γεώργιος icsd15058

Σάμος, 21/4, 2018

Περιεχόμενα

Αντωνιάδης Χαράλαμπος icsd10011 , Ευκαρπίδης Κωνσταντίνος icsd15051 , Ζιώζας Γεώργιος icsd15058

1 Εισαγωγή

Η παρακάτω αναφορά εγγράφου έχει ως στόχο να παρουσιάσει με πρακτικά παραδείγματα την μέθοδο Αποτίμησης και Διαχείρισης Επικινδυνότητας η οποία σκοπεύει στην

- Συστηματική αναγνώριση κινδύνων
- Αποτίμηση της πιθανότητας εμφάνισης τους
- Επιπτώσεις τους στην επιχείρηση
- Προτεραιοποίηση των κινδύνων και της υλοποίησης των αντιμέτρων για την αντιμετώπισή τους.
- Εμπλοκή των συμμετεχόντων στη λήψη αποφάσεων ασφάλειας και διαρκής ενημέρωσή τους
- Ενημέρωση στελεχών και προσωπικού για τους κινδύνους, τις επιπτώσεις τους και τις δράσεις αντιμετώπισης
- Ενίσχυση της αποτελεσματικότητας της παρακολούθησης αντιμετώπισης κινδύνων
- Παροχή διαρκούς ανάδρασης προς τη βελτίωση της διαχείρισης επικινδυνότητας

2 Θέμα εργασίας

Το μικροβιολογικό εργαστήριο Υ βρίσκεται στο ισόγειο τριώροφου κτηρίου επί της παραλιακής οδού στο Βαθύ της Σάμου. Το κτήριο κατασκευάστηκε πριν από 35 έτη και σε αυτό στεγάζονται άλλα 5 επαγγελματικά γραφεία και ιατρεία και μία δημόσια υπηρεσία. Η είσοδος του κτηρίου είναι κοινή και παραμένει ανοικτή όλο το 24ωρο. Οι ηλεκτρολογικές και υδραυλικές εγκαταστάσεις εμαφανίζουν συχνά προβλήματα. Σποραδικά σημειώνονται απροειδοποίητες διακοπές ηλεκτρικού ρεύματος, ειδικά σε συνθήκες κακοκαιρίας.

Το εργαστήριο έχει τρεις χώρους. Στον πρώτο, όπως μπαίνουν οι επισκέπτες, βρίσκεται ο χώρος αναμονής και το γραφείο της γραμματέως. Εσωτερική πόρτα οδηγεί στο χώρου του εργαστηρίου, το οποίο επικοινωνεί μεσω άλλης εσωτερικής πόρτας με το γραφείο των ιατρών-μικροβιολόγων. Το ιατρείο έχει μία μόνο είσοδο, από ένα παράθυρο στο χώρο αναμονής και το γραφείο των ιατρών και δεν διαθέτει συναγερμό. Λειτουργεί τα τελευταία 15 έτη, 09:00- 14:00 και 16:00– 21:00, Δευτέρα έως Παρασκευή και δέχεται περίπου 30 ασθενείς την ημέρα.

Το μικροβιολογικό εργαστήριο διαθέτει τρεις υπολογιστές. Ο ένας βρίσκεται στο γραφείο της γραμματέως, ο δεύτερος στο εργαστήριο και ο τρίτος στο γραφείο των ιατρών. Διαθέτουν λειτουργικό σύστημα Windows 10 και βασικό πακέτο εφαρμογών Office 2010.

Το εργαστήριο χρησιμοποιεί ένα εμπορικό «πακέτο» (Laboratory IS) για τη διαχείριση των ραντεβού και των φακέλλων των ασθενών που αποτελείται από τρία υποσυστήματα: Το Υποσύστημα Διαχείρισης Ασθενών (εγκατεστημένο στο γραφείο των ιατρών και της γραμματέως), το Υποσύστημα Διαχείρισης Εργαστηρίου (εγκατεστημένο στον υπολογιστή του εργαστηρίου που συνδέεται και με τα μηχανήματα ανάλυσης) και το Υποσύστημα Διαχείρισης Διοικητικών και Οικονομικών Υπηρεσιών που είναι εγκατεστημένο στον υπολογιστή της γραμματέως. Οι υπολογιστές επικοινωνούν μεταξύ τους μέσω του τοπικού δικτύου.

Οι υπολογιστές έχουν πρόσβαση στο Διαδίκτυο, μέσω ενός οικιακού δρομολογητή (router/gateway) που έχει εγκαταστήσει ο πάροχος της σύνδεσης στο Διαδίκτυο (Internet Service Provider). Εκτός από ένα δωρεάν antivirus που είναι εγκατεστημένο στους υπολογιστές, δεν χρησιμοποιείται κάποιο άλλο σύστημα ή λογισμικό ασφάλειας.

3 Data & Physical assets

1. Data assets

- Υποσύστημα Διαχείρισης Ασθενών
- Υποσύστημα Διαχείρισης Εργαστηρίου
- Υποσύστημα Διαχείρισης Διοικητικών και Οικονομικών Υπηρεσιών
- Τοπικό Δίκτυο
- Δρομολογητής (router/gateway)
- Διαδίκτυο (ISP)
- 3 Υπολογιστές
- Πελάτες
- Λ.Σ Windows 10
- Office 2010
- Laboratory IS
- Antivirus

2. Physical assets

- Μικροβιολογικό Εργαστήριο
- Εξοπλισμός εργαστηρίου
- 3 εσωτερικοί Χώροι
- 3 υπολογιστές
- Εργαζόμενοι
- 1 δρομολογητής

4 Αποτίμηση επιπτώσεων

Αποτίμηση Επιπτώσεων Παραβίασης Δεδομένων	**Χαμηλή Επίπτωση (1)**	**Μέτρια Επίπτωση (2)**	**Υψηλή Επίπτωση (3)**	**Σχόλια**
Μη Διαθεσιμότητα (3ώρες)	✔			Χαμηλή επίπτωση καθώς το χρονικό όριο είναι αρκετά μικρό
Μη Διαθεσιμότητα (1 ημέρα)		✔		Μέτρια Επίπτωση καθώς 1 ημέρα Μη διαθεσιμότητας σημαίνει απώλεια εσόδων μίας ημέρας
Μη Διαθεσιμότητα (5 ημέρες)			✔	Υψηλή Επίπτωση καθώς το εργαστήριο αδυνατεί να ανταπεξέλθει και να αποθηκεύσει τα δεδομένα των ασθενών του, επίσης χάνεται η εμπιστοσύνη από τους πελάτες και τσαλακώνεται η εικόνα του ιατρείου
Καταστροφή (Μερική)		✔		Μερική επίπτωση αφού τουλάχιστον σώθηκαν τα μισά δεδομένα της βάσης
Καταστροφή (Ολική)			✔	Υψηλή Επίπτωση αφού το βασικό εργαλείο της επιχείρησης έχει αχρηστευθεί και η εμπιστοσύνη των πελατών έχει μειωθεί προς αυτήν
Αποκάλυψη σε τρίτους			✔	Μείωση Εμπιστοσύνης καθώς η επιχείρηση δεν τηρεί ένα από τα βασικά της προνόμια , την εχεμύθεια
Μη εξουσιοδοτημένη μεταβολή			✔	Υψηλή Επίπτωση καθώς κάτι τέτοιο μπορεί να οδηγήσει σε λανθασμένες αποφάσεις προς τους ασθενείς και να αποβεί μοιραίο

5 Αξιολόγηση κόστους αντικατάστασης υλικού / λογισμικού

Χρηματική αξία υλικού & λογισμικού	**[1-2500€] (1)**	**[2500-5000€] (2)**	**[5000- 10000€] (3)**	**[10000- 15000€] (4)**	**[15000€ +]**
Κτήριο					✔
Μικροβιολογικός Εξοπλισμός					✔
Εξοπλισμός γραφείου			✔		
PC's	✔				
Software		✔			
Δίκτυο	✔				

6 Καταγραφή απειλών

Η είσοδος του κτηρίου είναι κοινή και παραμένει ανοικτή όλο το 24ωρο.

Το μικροβιολογικό εργαστήριο περιέχει ακριβό εξοπλισμό και "ευαίσθητα" δεδομένα των πελατών . Συνεπώς η ύπαρξη κοινής εισόδου ,η οποία να είναι μονίμως ανοιχτή, θέτει σε κίνδυνο την ασφάλεια των δεδομένων.

Οι ηλεκτρολογικές και υδραυλικές εγκαταστάσεις εμφανίζουν συχνά προβλήματα.

Η εμφάνιση ηλεκτρολογικών και υδραυλικών προβλημάτων σε ένα μικροβιολογικό εργαστήριο βάζει σε ρίσκο κυρίως την ασφάλεια των ασθενών (ανεπιθύμητη λειτουργία των ηλεκτρικών συσκευών κ.ά.) και έπειτα την ασφάλεια των μηχανημάτων.

Το ιατρείο δεν διαθέτει συναγερμό.

Η έλλειψη συναγερμού στον χώρο του εργαστηρίου αποτελεί σημαντική αμέλεια καθώς σε περίπτωση διάρρηξης θέτει σε κίνδυνο και την ζωή των εργαζομένων/πελατών και της ασφάλειας των προσωπικών αρχείων των ασθενών και την ασφάλεια των μηχανημάτων.

Εκτός από ένα δωρεάν antivirus που είναι εγκατεστημένο στους υπολογιστές, δεν χρησιμοποιείται κάποιο άλλο σύστημα ή λογισμικό ασφάλειας.

Η σωστή πρόληψη ασφάλειας για την προστασία των αρχείων αποτελεί ανώτατο μέτρο ειδικά σε ένα εργαστήριο με τόσο ευαίσθητα δεδομένα που μπορεί να παραβιαστούν ηλεκτρονικά.

Εσωτερική πόρτα οδηγεί στο χώρο του εργαστήριου, το οποίο επικοινωνεί μέσω άλλης εσωτερικής πόρτας με το γραφείο των ιατρών-μικροβιολόγων.

Εδώ βλέπουμε ότι υπάρχει λανθασμένη εκμετάλλευση χώρου διότι ο μόνος τρόπος εισόδου στο γραφείο των ιατρών είναι μέσω του εργαστηρίου. Ο χώρος του εργαστηρίου περιέχει σημαντικά δεδομένα και ευαίσθητο εξοπλισμό , έτσι η έκθεση αυτών στους πελάτες καθημερινά αποτελεί ρίσκο ασφαλείας.

7 Πιθανότητας εκδήλωσης απειλών

Πιθανότητα Εκδήλωσης Απειλών	Αρκετά Μικρή (1)	Μικρή (2)	Μεσαία (3)	Υψηλή (4)	Πολύ Υψηλή (5)
Η είσοδος του κτηρίου είναι κοινή και παραμένει ανοικτή όλο το 24ωρο (Παραβίαση)		✔			
Ηλεκτρολογικές και Υδραυλικές βλάβες (Βλάβη Εξοπλισμού)				✔	
Απουσία Συναγερμού &καμερών (Παραβίαση)					✔
Ανεπαρκής Ασφάλεια των ηλεκτρονικών δεδομένων (Υποκλοπή)					✔
Αρχείο ασθενών στη γραμματεία				✔	
Σύνδεση στο διαδίκτυο					✔
Φυσικές καταστροφές				✔	
Λανθασμένη υποδομή γραφείων (Ρίσκο ασφαλείας)			✔		

8 Αξιολόγηση βαθμού ευπάθειας

Αξιολόγηση Βαθμού Ευπάθειας	**Λίγο Ευπαθές (1)**	**Μέτρια Ευπαθές (2)**	**Πολύ Ευπαθές (3)**
Η είσοδος του κτηρίου είναι κοινή και παραμένει ανοικτή όλο το 24ωρο (Παραβίαση)		✔	
Ηλεκτρολογικές και Υδραυλικές βλάβες (Βλάβη Εξοπλισμού)			✔
Απουσία Συναγερμού &καμερών (Παραβίαση)		✔	
Ανεπαρκής Ασφάλεια των ηλεκτρονικών δεδομένων (Υποκλοπή)			✔
Φυσικές καταστροφές			✔
Σύνδεση στο διαδίκτυο			✔
Αρχείο ασθενών στη γραμματεία		✔	
Λανθασμένη υποδομή γραφείων (Ρίσκο ασφαλείας)	✔		

- Διάρρηξη για δεδομένα & εξοπλισμό με πιθανή μερική έως και ολική καταστροφή
- Μη λειτουργεία του εργαστήριου λόγω απώλειας ρεύματος. Κίνδυνος καταστροφής εξοπλισμού και πιθανή μόλυνση
- Έλλειψη άμεσης αντιμετώπισης και ενημέρωσης της κατάστασης σε περίπτωση κλοπής.
- Απομακρυσμένη υποκλοπή ευαίσθητων δεδομένων
- Σημαντική καταστροφή από πλημμύρα ή άλλα φυσικά αίτια. Φυσική μόλυνση του χώρου.
- Κίνδυνος καταστροφής δεδομένων ή υποκλοπή αυτών από απομακρυσμένο διαρρήκτη (hacker)
- Παραβίαση λογισμικού (λόγω έλλειψης παρουσίας γραμματέα), υποκλοπή κωδικών και ευαίσθητων δεδομένων των ασθενών
- Υψηλή επικινδυνότητα ζημίας εξοπλισμού και κακή ποιότητα υγιεινής ,σύμφωνα με τα κατάλληλα πρότυπα.

9 Σενάρια υψηλότερης επικινδυνότητας

Ηλεκτρολογικές και Υδραυλικές βλάβες (Βλάβη Εξοπλισμού

i) Ένα εργαστήριο που δουλεύει κατά κύριο λόγω με ηλεκτρονικό εξοπλισμό και απαιτεί απόλυτη φερεγγυότητα σε αυτόν , η έλλειψη "ασφαλούς" χρήσης του εξοπλισμού θέτει σε κίνδυνο και την ασφάλεια των πελατών άλλα και των μηχανημάτων.

ii) Εξαιτίας της συχνής κακοκαιρίας και κακής υδροηλεκτρικής υποδομής, η πιθανότητα καταστροφής του εξοπλισμοί ή πρόβλημα μόλυνσης από το αποχετευτικό σύστημα είναι πολύ υψηλή, ακόμα και καταστροφή κτιρίου λόγου πυρκαγιάς. Γενικότερα μπορεί να υποστούμε βλάβες υψηλού κόστους.

Απουσία Συναγερμού (Παραβίαση)

i) Η απουσία συναγερμού και κλειστού κυκλώματος παρακολούθησης αποτελεί σενάριο υψηλής επικινδυνότητας καθώς οι προσωπικές πληροφορίες πρέπει να μένουν εμπιστευτικές και η έλλειψη σωστών μέτρων ασφαλείας θέτει σε υψηλό κίνδυνο τη διάρρηξη του γραφείου.

ii) Διαρρήκτης έρχεται να παραβιάσει το χώρο μας. Λόγω έλλειψης συναγερμοί και κλειστού συστήματος παρακολούθησης (κάμερες) , έχει τη δυνατότητα να πράττει ανενόχλητος. Έπειτα από τη παραβίαση της βασικής πόρτας καταφέρνει να μπει στο χωρώ υποδοχής ασθενών, χωρίς να ενημερωθεί κανένας για το περιστατικό. Αρχικά ο διαρρήκτης έχει τη δυνατότητα να υποκλέψει τα αρχεία των ασθενών από τον υπολογιστή της γραμματέως. Η είσοδος στο υποσύστημα του υπολογιστή δεν είναι δύσκολη υπόθεση, από τη στιγμή που η γραμματέας κρατάει γραμμένους τους κωδικούς του υπολογισμοί και του προγράμματος Laboratory IS στο συρτάρι του γραφείου της, το οποίο παραμένει ξεκλείδωτο. Ακολούθως, έχει πρόσβαση στο επόμενο δωμάτιο που είναι το εργαστήριο, που μπορεί να υποκλέψει εξοπλισμό και ευαίσθητα δεδομένα ή ακόμα και παραποίηση δειγμάτων από ασθενής.

Ανεπαρκής Ασφάλεια των ηλεκτρονικών δεδομένων (Υποκλοπή)

iii) Από τη στιγμή που τα προσωπικά δεδομένα του ιατρείου αποθηκεύονται σε ηλεκτρονική μορφή απαιτείται αναγκαία η πλήρης ασφάλιση αυτών από ηλεκτρονικές υποκλοπές, έτσι η χρήση σωστών μέτρων ασφαλείας (ισχυρό antivirus, επίβλεψη).

iv) Κάποιος κακόβουλος, μας επιτίθεται απομακρυσμένα μέσω διαδικτύου και λόγω έλλειψης αντιικού και λόγω σύνδεσης με το διαδίκτυο, οι ευπάθειες είναι πολλές (Vulnerabilities) και είναι πιθανό να μας υποκλαπούν δεδομένα καθώς και να έχουμε ζημία στο ίδιο το σύστημα.

10 Αντίμετρα Προστασίας

ΚΛΟΠΗ

- ✓ Εγκατάσταση συναγερμού για την αποφυγή πιθανής διάρρηξης και κάμερες για παρακολούθηση 24/7 του χώρου.
- ✓ Επειδή το κτήριο αποτελείται από γραφεία και ιατρεία και δημόσια υπηρεσία μπορούμε να συνεννοηθούμε με τους υπόλοιπους ιδιοκτήτες και να κλειδώνουμε την εξώπορτα για λόγους ασφαλείας από τις 9 το βράδυ ως το πρώτο γραφείο που ανοίγει το πρωί.
- ✓ Προτείνεται ο γραμματέας από το τερματικό του να έχει περιορισμένη πρόσβαση ΜΟΝΟ στα ονόματα των ασθενών και στα στοιχεία επικοινωνίας χωρίς το ιστορικό και οποιαδήποτε άλλη ευαίσθητη πληροφορία.
- ✓ Προτείνεται αλλαγή διαρρύθμισης στο χώρο ώστε να υπάρχει πρόσβαση από το χώρο αναμονής των ασθενών άμεσα στο ιατρείο και στο εργαστήριο. Επίσης, πρέπει να εγκατασταθούν αντίμετρα ασφαλείας σε όλα τα σημεία πρόσβασης, όπως πχ παράθυρα ασφαλείας.

ΙΝΤΕΡΝΕΤ

- ✓ Εγκατάσταση ασφαλέστερων παραμέτρων ασφαλείας στο υπολογιστικό δίκτυο για αποφυγή υποκλοπής "ευαίσθητων δεδομένων". (ισχυρό συνδρομητικό antivirus , καλύτερο firewall).
- ✓ Ένα αντίμετρο στη σύνδεση με το διαδίκτυο, είναι η δημιουργία private Network (ιδιωτικού δικτύου) όπου θα είναι τα υποσυστήματα λειτουργίας του Laboratory IS. Παράλληλα μπορεί να υπάρχει router και σύνδεση στο διαδίκτυο με ***wi-fi*** χωρίς να επιτρέπεται η επικοινωνία μεταξύ τους. Δηλαδή να διατηρούνται τα δεδομένα και όλο το σύστημα offline.

ΥΔΡΟΗΛΕΚΤΡΙΚΑ ΠΡΟΒΛΗΜΑΤΑ

- ✓ Επισκευή των ηλεκτρολογικών και υδραυλικών συστημάτων καθώς υπάρχει κίνδυνος καταστροφής του ιατρικού εξοπλισμού, προσθήκη UPS για την σταθεροποίηση της τάσης και την ασφαλή διεκπεραίωση των ενεργών διαδικασιών.
- ✓ Σε συνεννόηση με του υπόλοιπους ένοικους, να γίνουν επισκευές στις σωληνώσεις και στο αποχετευτικό καθώς και στις ηλεκτρικές εγκαταστάσεις.

ΦΥΣΙΚΗ ΤΟΠΟΘΕΣΙΑ ΚΤΗΡΙΟΥ

- ✓ Λόγω της τοποθεσίας ο χώρος μας είναι ευάλωτος σε φυσικές καταστροφές από τη θάλασσα, προτείνεται αλλαγή κτιρίου κατά προτίμηση μακριά από τη θάλασσα.