ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΝΑΠΤΥΞΗ ΠΑΙΧΝΙΔΙΟΥ ΣΟΒΑΡΟΥ ΣΚΟΠΟΥ ΡΟΛΩΝ ΜΕ ΚΑΡΤΕΣ

Διπλωματική Εργασία

της

Ευφροσύνη Γαροφαλάκη

Θεσσαλονίκη, 02/2019

.

ΑΝΑΠΤΥΞΗ ΠΑΙΧΝΙΔΙΟΥ ΣΟΒΑΡΟΥ ΣΚΟΠΟΥ ΡΟΛΩΝ ΜΕ ΚΑΡΤΕΣ

Ευφροσύνη Γαροφαλάκη

Πτυχίο Πληροφορικής, Ιόνιο Πανεπιστήμιο, 2016

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Ιωάννης Μαυρίδης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 27/02/2019

ΜΑΥΡΙΔΗΣ ΙΩΑΝΝΗΣ	ΠΑΠΑΔΗΜΗΤΡΙΟΥ ΠΑΝΑΓΙΩΤΗΣ	ΞΥΝΟΓΑΛΟΣ ΣΤΥΛΙΑΝΟΣ
.....	.....	.....

Ευφροσύνη Γαροφαλάκη

.....

Περίληψη

Ο σκοπός της διπλωματικής εργασίας ήταν η ανάπτυξη ενός παιχνιδιού σοβαρού σκοπού, με στόχο οι παίκτες να αναγνωρίζουν πιθανά σενάρια κυβερνο-επιθέσεων. Τα εκπαιδευτικά σενάρια είναι βασισμένα στην μεθοδολογία Cyber Kill Chain, που αποτελεί την βασική ιδέα για τα βήματα που ακολουθούν οι χάκερς προκειμένου να εκτελέσουν μια επίθεση. Για την δημιουργία του παιχνιδιού με κάρτες χρησιμοποιήθηκαν διάφορες γλώσσες προγραμματισμού και τεχνολογίες διαδικτύου. Τα εκπαιδευτικά σενάρια στο παιχνίδι έχουν εντάξει διάφορες κυβερνο-επιθέσεις που έχουν συμβεί και συμβαίνουν καθημερινά. Στόχος είναι ο παίκτης κατανοώντας την επίθεση σε κάθε στάδιο να μπορεί να δώσει έστω και μια λύση για να περάσει στο επόμενο στάδιο που αποτελεί την συνέχεια για το προηγούμενο. Συγκεκριμένα, το κάθε εκπαιδευτικό σενάριο έχει τα δικά του στάδια με τις δικές του λύσεις. Για το εκπαιδευτικό κομμάτι χρησιμοποιήθηκε η μεθοδολογία επτά βημάτων για την δημιουργία εκπαιδευτικών παιχνιδιών με κάρτες που αναλύει τους στόχους που πρέπει να επιτύχει ο δημιουργός ώστε να δώσει την κατάλληλη εκπαιδευτική βοήθεια στους παίκτες. Για τον λόγο αυτό, στο παιχνίδι υπάρχει η εκπαιδευτική βοήθεια που αναλύει κάθε στάδιο. Η εκπαιδευτική βοήθεια που αναλύει κάθε λύση και η εκπαιδευτική βοήθεια με τα εικονίδια σε κάθε ίδια κάρτα στάδιο και κάρτα λύση. Οι εκπαιδευτικές έννοιες που αναλύονται στο παιχνίδι είναι το Cyber Kill Chain, DDoS,
Phishing attacks, malware, trojan. Κάθε στάδιο στο παιχνίδι έχει προσχεδιαστεί ώστε να υπάρχει συγκεκριμένος στόχος. Μόλις βρουν την κατάλληλη άμυνα τότε περνούν στο επόμενο στάδιο. Ο παίκτης που θα φτάσει πρώτος και θα ολοκληρώσει το τελικό στάδιο τότε είναι νικητής και ταυτόχρονα έχει προστατέψει το σύστημα του από την επίθεση.

Λέξεις Κλειδιά:

κεβερνοασφάλεια, cyber security, παιχνίδι, ασφάλεια, cyber kill chain, capec, μεθοδολογία επτά βημάτων

Abstract

The purpose of the master thesis is the development of a serious game, aiming in the players' ability to recognize possible cyber-attack scenarios. The scenarios are based on the Cyber Kill Chain methodology, which is the basic steps a hacker would follow in order to perform an attack.

Various programming languages and web technologies was used for the development of the card game.

The scenarios use various cyber-attacks the have happened in the past and keep happening on a daily basis. The player must understand the attack and provide at least one solution, in order to proceed to the next stage of the scenario. Specifically, every scenario has its own stages with their own solutions.

For the educational part, the seven step methodology for creating educational card games was used, which analyzes the goals the creator should have in order to provide the players with proper educational help. So, to provide the necessary help, there were added an explanation of each stage, an explanation for every solution and an icon, linking each card with the stage. The educational concepts, explained in the game are Cyber Kill Chain, DDoS, Phishing attacks, malware, and trojan. Each stage in the game has a predefined goal. When a player finds a proper defense, then the player proceeds to the next stage. The player who reaches and answers successfully the last stage wins the game and has successfully protected his system from the attack.

Keywords:

cyber security, serious games, security, cyber kill chain, capec, 7 steps methodology

Περιεχόμενα

Κατάλογος Εικόνων

Κεφάλαιο Α

Εισαγωγή

Α.1 Εισαγωγή στην κεβερνοασφάλεια

Το Διαδίκτυο αποτελεί σημαντικό κλειδί στην καθημερινότητα των ανθρώπων. Σχεδόν όλοι οι άνθρωποι είναι συνδεδεμένοι στο Διαδίκτυο καθημερινά. Χρησιμοποιούν το Διαδίκτυο για να ενημερώνονται για τις επιχειρήσεις τους, για τις ειδήσεις σε ολόκληρο τον κόσμο, να επικοινωνούν με την οικογένεια και τους φίλους τους. Όμως, το πρόσωπο του Διαδικτύου έχει δύο πλευρές (Lance Spitzner, 2018). Επιθέσεις σε επιχειρήσεις πραγματοποιούνται καθημερινά για να κλέψουν ευαίσθητα δεδομένα των επιχειρήσεων και των κυβερνήσεων. Βέβαια, υπάρχουν πιο απλές επιθέσεις που πραγματοποιούνται για να κλέψουν ευαίσθητα προσωπικά δεδομένα όπως είναι οι τραπεζικοί λογαριασμοί για οικονομικές απάτες αλλά και προσωπικά δεδομένων ανθρώπων (Lance Spitzner, 2018). Καθημερινά η κατάσταση των επιθέσεων στο Διαδίκτυο γίνεται ολοένα και χειρότερη λόγω της ανακάλυψης νέων τεχνικών για επιθέσεις και καινούργιων τύπων ιών που προσβάλλουν συσκευές και ηλεκτρονικά συστήματα.

Για τον λόγο αυτό, υπάρχουν ερευνητές που αναζητούν και ανακαλύπτουν διάφορες τεχνικές άμυνας στην κεβερνοασφάλεια (Lance Spitzner, 2018). Ανακαλύπτουν τους λόγους που οι χάκερς επιτίθενται, αδυναμίες στο δίκτυο επιχειρήσεων και κυβερνήσεων, καθώς και τον τρόπο σκέψης των επιτιθέμενων ώστε να αναγνωρίζουν αν η επιχείρηση βρίσκεται υπό την επήρεια μιας ενδεχόμενης επίθεσης (Lance Spitzner, 2018). Οι μηχανισμοί άμυνας που ανακαλύπτονται συνήθως αφορούν την κατανόηση του δικτύου, τον τρόπο σκέψης των επιτιθέμενων, τα κίνητρα τους, τους μεθόδους επίθεσης που χρησιμοποιούν και τις αδυναμίες που έχουν τα συστήματα και μπορούν να εκμεταλλευτούν οι επιτιθέμενοι για να επιτεθούν (Lance Spitzner, 2018). Στόχος τους είναι να μετριάσουν τις αδυναμίες στα συστήματα των κυβερνήσεων και των οργανισμών ώστε να αποτρέψουν μια μελλοντική επίθεση.

Οι επιχειρήσεις για να προστατευτούν από μια μελλοντική επίθεση είναι σημαντικό να ανιχνεύσουν για αδυναμίες στο σύστημα τους, να κατανοήσουν τα κίνητρα των επιτιθέμενων, καθώς και τα δεδομένα που διαθέτουν και είναι πολύτιμα (Lance Spitzner, 2018).

Οπότε είναι σημαντικό όλες οι επιχειρήσεις και οι κυβερνήσεις να διαθέτουν μηχανισμούς άμυνας στο σύστημα τους ώστε να αποτρέπουν μελλοντικές επιθέσεις. Οι κυβερνοεπιθέσεις αποτελούν ένα ευαίσθητο θέμα στον κόσμο της ασφάλειας υπολογιστών. Σε όλο τον κόσμο, οι κυβερνήσεις και οι επιχειρήσεις παρέχουν τεραστία προσπάθεια για να ασφαλίσουν τα δεδομένα τους από επιθέσεις χρησιμοποιώντας διάφορες τεχνικές και εργαλεία για να αμύνονται σε επιθέσεις τύπου ιών, δούρειων ίππων και botnets (Lance Spitzner, 2018). Καθημερινά η κατάσταση στις κυβερνοεπιθέσεις γίνονται όλο και χειρότερη διότι νέοι τύποι κακόβουλων λογισμικών ανακαλύπτονται.

Οι κυβερνήσεις και οι επιχειρήσεις αφιερώνουν μεγάλο ποσοστό χρημάτων στην ασφάλεια του δικτύου τους και των συστημάτων τους από κακόβουλες επιθέσεις (Lance Spitzner, 2018). Σκοπός των κυβερνήσεων και των επιχειρήσεων είναι η κατανόηση του τρόπου σκέψης των επιτιθέμενων και η ανακάλυψη των αδυναμιών στο σύστημα τους, ώστε να αναλάβουν δραστικά μέτρα για να προφυλαχτούν από τέτοιου είδους επιθέσεις. Όμως, στον κόσμο της ασφάλειας είναι δύσκολο οι επιχειρήσεις να προφητεύουν μια ενδεχόμενη επίθεση στο σύστημα τους, από τις αδυναμίες που υπάρχουν στο δίκτυο τους (Lance Spitzner, 2018).

Επομένως, η ανάλυση του συστήματος και του δικτύου των επιχειρήσεων και κυβερνήσεων αποτελεί σημαντικό βήμα για να προσδιοριστούν οι πιθανές ευπάθειες στο σύστημα τους, που πρόκειται να χρησιμοποιηθούν για μια ενδεχόμενη επίθεση. Επίσης, ο σωστός χειρισμός κατά την διάρκεια μιας επίθεσης είναι σημαντικό βήμα από την εταιρεία για να διαφυλάξουν το σύστημα τους και τα πολύτιμα δεδομένα που διαθέτουν, η άμεση δράση και ανακάλυψη ότι το σύστημα έχει δεχθεί επίθεση αποτελεί σημαντικό κομμάτι για τις επιχειρήσεις (Lance Spitzner, 2018).

Η ευαισθητοποίηση σε θέματα ασφάλειας δεν είναι τίποτα περισσότερο από εντολές όπως η κρυπτογράφηση, οι κωδικοί πρόσβασης, τα τείχη προστασίας, η προστασία από ιούς και η πρόβλεψη χαμένων δεδομένων από διάφορα λογισμικά (DLP) (Lance Spitzner, 2018).

Οι κυβερνοεπιθέσεις έχουν μεγάλο αντίκτυπο και τεράστιες αρνητικές επιπτώσεις σε οργανισμούς, κυβερνήσεις και επιχειρήσεις (Tarun Yadav, 2015). Το Cyber Kill Chain είναι μια αλυσίδα επιθέσεων και αποτελεί το μονοπάτι που ακολουθεί ένας εισβολέας για να επιτεθεί σε πληροφοριακά συστήματα με την πάροδο του χρόνου (Tarun Yadav, 2015).

Α.2 Διάρθρωση της μελέτης

Στα επόμενα κεφάλαια θα παρουσιαστεί το θέμα της κεβερνοασφάλειας με σκοπό την δημιουργία του παιχνιδιού για σοβαρό εκπαιδευτικό σκοπό, παρουσιάζονται οι κανόνες του παιχνιδιού η σχεδίαση του και τα συμπεράσματα της διπλωματικής εργασίας.

Συγκεκριμένα, στο κεφάλαιο 2, πραγματοποιείται μια ανάλυση των παιχνιδιών σοβαρού σκοπού στην κεβερνοασφάλεια με κάρτες, η μεθοδολογία τους, οι κανόνες και ο τρόπος που παίζονται τα παιχνίδια.

Στο κεφάλαιο 3, πραγματοποιείται ανάλυση του κάθε παιχνιδιού, με τους κανόνες, τις οδηγίες και τα εκπαιδευτικά σενάρια, ακόμη αναλύεται βήμα-βήμα πως παίζεται το παιχνίδι.

Στο κεφάλαιο 4, αναλύεται η μεθοδολογία επτά βημάτων για την σχεδίαση των καρτών, τις αρχές, τον σχεδιασμό και την εφαρμογή στην σχεδίαση του παιχνιδιού.

Στο κεφάλαιο 5, πραγματοποιείται ανάλυση για την ανάπτυξη του παιχνιδιού, τις τεχνολογίες που χρησιμοποιήθηκαν, τις εκπαιδευτικές κάρτες για τα στάδια και τις λύσεις καθώς και την ανάλυση των κλάσεων για την ανάπτυξη του εκπαιδευτικού παιχνιδιού.

Α.3 Τα παιχνίδια σοβαρού σκοπού στην κεβερνοασφάλεια

Τα παιχνίδια σοβαρού σκοπού συνήθως αναφέρονται σε παιχνίδια που χρησιμοποιούνται στην εκπαίδευση, την διαφήμιση και την ψυχαγωγία. Έχουν σχεδιαστεί για να λειτουργούν σε προσωπικούς υπολογιστές ή κονσόλες βιντεοπαιχνιδιών (Susi, Johannesson, Backlund, 2007). Ο γενικός σκοπός των παιχνιδιών σοβαρού σκοπού είναι ότι χρησιμεύουν για την εκπαίδευση των μαθητών μέσω των εκπαιδευτικών παιχνιδιών. Τα παιχνίδια αυτά χρησιμεύουν στην εκπαίδευση των μαθητών, όμως έχουν και ψυχαγωγικό χαρακτήρα. Ο όρος των “Παιχνιδιών Σοβαρού Σκοπού” εισήχθηκε από τον Clark Abt στο βιβλίο με τίτλο “Serious Games” το 1970 (Vik, 2009).

Πιο συγκεκριμένα, τα παιχνίδια σοβαρού σκοπού έχουν ψυχαγωγικό χαρακτήρα με δύο σκοπούς. Με το παιχνίδι οι μαθητές ψυχαγωγούνται ενώ παράλληλα διαθέτει και εκπαιδευτικό χαρακτήρα όπου διδάσκονται καινούργιοι όροι, με αποτέλεσμα να αναπτύσσονται νέες δεξιότητες και να αποκτούν μια σοβαρή διαπαιδαγώγηση. Τα

εκπαιδευτικά παιχνίδια σοβαρού σκοπού εστιάζουν στην ενίσχυση των κινήτρων των μαθητών μέσα από την πρόκληση, την περιέργεια, το αίσθημα ελέγχου και την φαντασία.

Παρακάτω, αναφέρονται οι προδιαγραφές για την ανάπτυξη εκπαιδευτικού παιχνιδιού.

Οι στόχοι των εκπαιδευτικών παιχνιδιών εξετάζονται σε δύο άξονες:

1. Γνωστικός άξονας: Οι στόχοι του παιχνιδιού οφείλουν να κατηγοριοποιούνται στις πληροφορίες που λαμβάνουν οι μαθητές από το παιχνίδι.
2. Συναισθηματικός άξονας: Οι στόχοι του παιχνιδιού πρέπει να καθοριστούν ώστε οι παίκτες να διαχειρίζονται μέσα από ανάλογες καταστάσεις τα συναισθήματα τους.
3. Η επιλογή πλαισίου εργασίας λειτουργεί ως καταλυτικός παράγοντας και είναι ο οδηγός της σωστής εκπαίδευσης των μαθητών μέσω των παιχνιδιών. Ο εκπαιδευτικός οφείλει να λάβει υπόψη του τι συμβαίνει στον πραγματικό κόσμο.
4. Η επιλογή μιας αυθεντικής ιστορίας ή σεναρίου ώστε το παιχνίδι να είναι ελκυστικό στους μαθητές. Επομένως, το ενδιαφέρον αποτελεί τον βασικό άξονα σε ένα παιχνίδι για να εκπαιδεύει και ταυτόχρονα να ψυχαγωγεί.
5. Σημαντικά είναι τα επεξηγηματικά μηνύματα κατά την διάρκεια του παιχνιδιού, ώστε σε περίπτωση δυσκολίας οι μαθητές να βοηθηθούν.
6. Χρήση τεχνικών στην επεξήγηση της ιστορίας του παιχνιδιού καθώς και ο τρόπος που παίζεται το παιχνίδι, συνήθως αποτελεί μια σύντομη λεκτική περιγραφή ή βίντεο επεξήγησης.
7. Βοήθεια στους μαθητές με υποσημειώσεις από παρόμοιες λύσεις σε προβλήματα.
8. Εργαλεία για την κατασκευή της γνώσης και της επικοινωνίας.

Τα παιχνίδια εκπαιδευτικού σκοπού πρέπει να καλύπτουν τους εκπαιδευτικούς στόχους ανάλογα με την ενότητα εκμάθησης. Ουσιαστικά αν πρόκειται για την εκπαίδευση μιας γλώσσας προγραμματισμού οι εκπαιδευτικοί στόχοι πρέπει να περιλαμβάνουν έννοιες και ορολογίες που αφορούν την εκμάθηση τέτοιου τομέα. Ο στόχος των εκπαιδευτικών παιχνιδιών είναι η κάλυψη διδακτικών ενοτήτων που περιλαμβάνονται στο παιχνίδι είτε σε συγκεκριμένα επίπεδα, είτε αποτελούν εξολοκλήρου το παιχνίδι (Βαγγέλης Τσαλιγωνέας, 2015). Γενικά, τα προβλήματα που καλούνται να λύσουν οι μαθητές είναι συνεπή με τους εκπαιδευτικούς στόχους και τους γνωστικούς περιορισμούς της διδακτικής ενότητας. Η εφαρμογή των παιχνιδιών σοβαρού σκοπού βρίσκεται σε διάφορους κλάδους όπως ο στρατός, η υγεία, η εκπαίδευση, η διαφήμιση, η πολιτική, η τέχνη, η οργάνωση, τα χρηματοοικονομικά, η κυβέρνηση και η διοίκηση τεχνολογίας (Βαγγέλης Τσαλιγωνέας, 2015).

Τα εκπαιδευτικά παιχνίδια χρησιμοποιούνται από διάφορους κλάδους με διαφορετικό τρόπο αλλά ως κοινό παρανομαστή έχουν την εκπαίδευση. Σύμφωνα με το Prensky το 2001 αναφέρει ότι τα εκπαιδευτικά παιχνίδια έχουν ως σκοπό την εκπαίδευση (Βαγγέλης Τσαλιγωνέας, 2015).

Τα ηλεκτρονικά παιχνίδια αποτελούνται από τα εξής δομικά στοιχεία:

1. Κανόνες: Θέτουν τους στόχους για το παιχνίδι για να προκαλέσει τον ενθουσιασμό των παικτών
2. Σκοπός - Στόχοι
3. Διαδραστικότητα: Επιτυγχάνεται σε δύο επίπεδα που αφορούν την σχέση του παίκτη με τους συμπαίκτες του και την σχέση του παίκτη με τον ηλεκτρονικό υπολογιστή
4. Έκβαση: Τρόπος για βοήθεια των παικτών ώστε να παρακολουθούν την πρόοδο τους για να επιτύχουν τους στόχους τους
5. Σύγκρουση - Ανταγωνισμός - Αντιπαράθεση - Πρόκληση: Αφορούν τις καταστάσεις που αντιμετωπίζουν οι παίκτες προσπαθώντας να επιλύσουν τα προβλήματα του παιχνιδιού με σκοπό την αύξηση της αδρεναλίνης στο παιχνίδι.
6. Αναπαράσταση: Εμπεριέχεται σε κάθε παιχνίδι και αναφέρεται σε κάποιο θέμα το οποίο περιλαμβάνει όλα τα αφηγηματικά στοιχεία του παιχνιδιού.

Α.4 Ασφάλεια υπολογιστών

Η ασφάλεια υπολογιστών αποτελεί ένα σημαντικό κομμάτι στις επιχειρήσεις σήμερα. Ανεξαρτήτως της επιχείρησης η ασφάλεια υπολογιστών και των συστημάτων ασφαλείας οφείλει να ενσωματώνεται σε κάθε επιχείρηση καθώς οι κυβερνοεπιθέσεις έχουν αυξηθεί σε σημαντικό ποσοστό καθημερινά. Με την εξέλιξη της τεχνολογίας οι χάκερς έχουν εξελιχθεί με αποτέλεσμα οι επιθέσεις να γίνονται ολοένα και πιο δύσκολες (Oracle Corporetion, 2018). Όμως, οι επιχειρήσεις και οι οργανισμοί δημιουργούν ομάδες με άτομα για την ασφάλεια των συστημάτων τους ώστε να αμύνονται σε πιθανές επιθέσεις και να ανακαλύπτουν αδυναμίες στα συστήματα τους, με αποτέλεσμα να αποτρέπουν μελλοντικές επιθέσεις (Oracle Corporetion, 2018). Οι επιχειρήσεις και οργανισμοί πρέπει να είναι προετοιμασμένοι για κυβερνοεπιθέσεις καθώς όλοι αποτελούν πιθανά θύματα για επίθεση από τους χάκερς (Oracle Corporetion, 2018).

Είναι γεγονός ότι οι χάκερς αποτελούν τους καινούργιες επικίνδυνους εγκληματίες, με αποτέλεσμα να γίνονται ολοένα και περισσότερο οργανωτικοί στις επιθέσεις τους. Οι χάκερς έχουν δημιουργήσει μια μεγάλη βιομηχανία (Oracle Corporetion, 2018).

Μερικά παραδείγματα για το πως οι χάκερς έχουν δημιουργήσει βιομηχανία επιθέσεων είναι:

- Μπορούν να πάρουν τα δεδομένα πλήρης ασφάλισης υγείας πληρώνοντας 1000 δολάρια
- Με 7 δολάρια την ώρα μπορούν να δημιουργήσουν οι πιθανοί πελάτες να δημιουργήσουν μια επίθεση τύπου Distributed Denial Of Service στον ανταγωνιστή τους.
- Μπορούν να αγοράσουν την ταυτότητα και τον φορολογικό αριθμό πολιτών με 40 δολάρια.
- Μπορούν να αγοράσουν 10.000 ακόλουθους στο twitter με 15 δολάρια.
- Μπορούν να έχουν πρόσβαση σε κυβερνητικούς servers με 6 δολάρια.

Επομένως, οι κυβερνοεπιθέσεις είναι μια μεγάλη βιομηχανία εγκλήματος που ολοένα και μεγαλώνει καθώς παρέχουν εικοσιτετράωρη εξυπηρέτηση, πληρωμή μετά την επιτυχία της επίθεσης και προσφορά δοκιμαστικών επιθέσεων (Oracle Corporetion, 2018).

Κεφάλαιο Β

Ανάλυση παιχνιδιών με κάρτες στην κεβερνοασφάλεια

Β.1 Elevation of Privilege, μεθοδολογία και οδηγίες παιχνιδιού

Το παιχνίδι Elevation of Privilege είναι ο πιο εύκολος τρόπος να ξεκινήσουν να μαθαίνουν οι μαθητές το μοντέλο απειλών που αποτελεί το πιο βασικό δομικό στοιχείο για τον κύκλο ανάπτυξης της ασφάλειας στην Microsoft (SDL). Το παιχνίδι έχει ως αντικείμενο τις κάρτες, που βοηθούν να αποσαφηνιστούν και να εξεταστούν πιθανές απειλές στο λογισμικό και στο πληροφοριακό σύστημα. Το EoP εστιάζει στις ακόλουθες επιθέσεις:

- Spoofing: Είναι η απειλή στην οποία ο επιτιθέμενος παριστάνει κάτι άλλο ή κάποιον άλλο άνθρωπο ώστε να υποκλέψει ευαίσθητα προσωπικά δεδομένα.
- Tampering: Σε αυτή την απειλή ο επιτιθέμενος τροποποιεί κάτι το οποίο δεν πρέπει, τέτοια παραδείγματα αποτελούν ασύρματα πακέτα, bits στον σκληρό δίσκο ή bits στην μνήμη.
- Repudiation: Είναι η απειλή στην οποία ο επιτιθέμενος υποστηρίζει ότι δεν έχει πραγματοποιήσει κάποιο αδίκημα και ας το έχει κάνει.
- Information Disclosure: Η συγκεκριμένη απειλή είναι για να εκθέτει ο επιτιθέμενος πληροφορίες σε άλλους ανθρώπους που δεν έχουν την εξουσιοδότηση να λάβουν αυτές τις πληροφορίες.
- Denial of Service: Οι συγκεκριμένες επιθέσεις είναι σχεδιασμένες για να προλαμβάνουν ή να εμποδίζουν ένα σύστημα ώστε να παρέχει μια υπηρεσία, οι επιτιθέμενοι ρίχνουν το σύστημα στέλνοντας συνέχεια αιτήματα στον server προκειμένου να γεμίσουν όλη την μνήμη του.
- Elevation of Privilege: Η συγκεκριμένη απειλή αποτελεί ένα πρόγραμμα ή
- έναν χρήστη ο οποίος μπορεί τεχνικά να αλλάξει ή να τροποποίηση δεδομένα τα οποία δεν πρέπει.

Το παιχνίδι χρησιμοποιεί την τεχνική STRIDE. Παρακάτω υπάρχουν μερικές απειλές που οφείλονται σε αυτή την τεχνική.

Με το Spoofing ο επιτιθέμενος μπορεί να παριστάνει ότι είναι κάποιος άλλος για να υποκλέψει πληροφορίες, για τον λόγο αυτό χρειάζεται το σύστημα να παρέχει ένα είδος αυθεντικοποίησης και να ελέγχει τους χρήστες στο σύστημα. Επίσης, κάποιος άλλος μπορεί να παριστάνει ότι η ιστοσελίδα ανήκει σε άλλον, έτσι οι διαχειριστές πρέπει να βεβαιώσουν και να χρησιμοποιήσουν τα απαραίτητα πιστοποιητικά αυθεντικοποίησης SSL και ένα μοναδικό domain. Κάποιος άλλος επιτιθέμενος

μπορεί στην ιστοσελίδα να τοποθετήσει ένα link το οποίο να παραπέμπει σε μια φόρμα για την αποστολή παραγγελίας με αποτέλεσμα οι χρήστες να συμπληρώνουν τα στοιχεία τους, τα οποία στέλνονται στον εχθρό. Για τον λόγο αυτό, πρέπει οι διαχειριστές και οι χρήστες να ελέγχουν τα πεδία που σκοπεύουν να στείλουν στο σύστημα καθώς μπορεί η συγκεκριμένη φόρμα να αποτελεί κακόβουλη επίθεση για την υποκλοπή προσωπικών στοιχείων ή στοιχεία από πιστωτικές κάρτες.

Στην απειλή Tampering ο επιτιθέμενος μπορεί να αλλοιώσει δεδομένα στο back end, δηλαδή τα δεδομένα μπορούν να αλλάξουν καθώς έρχονται ή φεύγουν από το σύστημα.

Στην απειλή Repudiation κάποια από τις προηγούμενες ενέργειες ίσως χρειαστεί οι διαχειριστές να ερευνήσουν τι συνέβη, έτσι ελέγχουν αν οι πληροφορίες είναι σωστές και προστατεύουν τις καταγραφές από προηγούμενες παραβιάσεις.

Στο Information Disclosure κάποιος συνδέεται στην βάση δεδομένων και διαβάζει ή γράφει πληροφορίες.

Στο Denial of Service , ξαφνικά εμφανίζονται χιλιάδες χρήστες σε μια ιστοσελίδα με αποτέλεσμα ο server να πέσει λόγω της υψηλής χρήσης των πόρων και της μικρής μνήμης.

Η τελευταία απειλή του μοντέλου STRIDE είναι το Elevation of Privilege στην οποία υπάρχουν ερωτήσεις όπως, αν στο μπροστά κομμάτι της εφαρμογής έχουν πρόσβαση οι πελάτες ή αν οι διαχειριστές έχουν χρησιμοποιήσει προληπτικά μέτρα για να μην ανεβάζουν μη εξουσιοδοτημένα άτομα κακόβουλο κώδικα.

Πως παίζεται το παιχνίδι:

1. Αρχικά, ανακατεύονται καλά οι κάρτες
2. Ο παίκτης με τα τρία tempering είναι ο αρχηγός του γύρου
3. Κάθε παίκτης παίζει μια κάρτα, ξεκινώντας με τον παίκτη που είναι ο αρχηγός του συγκεκριμένου γύρου, έπειτα η ροή γυρίζει με την φορά του ρολογιού.
4. Για να παιχτεί μια κάρτα ο παίκτης την διαβάζει δυνατά και στην συνέχεια ελέγχει αν επηρεάζει το σύστημα το οποίο έχει δημιουργηθεί στο διάγραμμα των παικτών. Αν η κάρτα συνδέεται τότε ο παίκτης την γράφει και δίνει τους ανάλογους πόντους στον εαυτό του. Το παιχνίδι συνεχίζεται στον επόμενο παίκτη.
5. Όταν όλοι οι παίκτες έχουν παίξει τις κάρτες τους, τότε ο παίκτης με την κάρτα που έχει τους περισσότερους πόντους κερδίζει τον γύρο και γίνεται ο αρχηγός, στον επόμενο γύρο του παιχνιδιού.
6. Όταν όλες οι κάρτες έχουν παιχτεί το παιχνίδι τελειώνει και ο παίκτης που έχει τους περισσότερους πόντους κερδίζει.

7. Αν το σύστημα με το μοτίβο απειλών έχει ολοκληρωθεί τότε οι υπόλοιποι παίκτες ψάχνουν για σφάλματα στο σύστημα (bugs).

Β.2 Control-alt-hack, μεθοδολογία και οδηγίες παιχνιδιού

Το παιχνίδι Control-alt-hack είναι ένα επιτραπέζιο παιχνίδι για τους νόμιμους χάκερς. Είναι βασισμένο στους μηχανισμούς του παιχνιδιού από τον Steve Jackson τον δημιουργό του Munchkin και GURPS. Το Control-alt-hack δημιουργήθηκε στο Πανεπιστήμιο της Washington και περιέχει διάφορα σενάρια από επιθέσεις στην ασφάλεια υπολογιστών, διάφορους χαρακτήρες ως χάκερς με ιδιαίτερα χαρακτηριστικά και μερικά αστεία από διάφορα περιστατικά στην ασφάλεια υπολογιστών. Η επιτρεπόμενη ηλικία που μπορούν οι παίκτες να παίξουν είναι 14+, ενώ οι παίκτες είναι τρεις έως έξι. Η διάρκεια του παιχνιδιού είναι περίπου μία ώρα (Denning, Kohno, Shostack, 2012).

Οι παίκτες δουλεύουν σε μια μικρή εταιρεία ασφάλειας για ηθικούς σκοπούς (οι χάκερς ονομάζονται white hackers), ενώ η εταιρεία του παιχνιδιού Hackers inc. Οι χακερς στην εταιρεία παρέχουν υπηρεσίες ασφάλειας και το μότο τους είναι “Μας πληρώνουν για να τους χακάρουμε” (Denning, Kohno, Shostack, 2012).
Η δουλεία του κάθε παίκτη είναι να ολοκληρώσει αποστολές με την χρήση των ικανοτήτων του ώστε να επιτύχουν την κάθε αποστολή. Στο παιχνίδι οι μαθητές πρέπει να χρησιμοποιήσουν τις ικανότητες και τις γνώσεις τους στο social engineering και τις άριστες γνώσεις τους στα δίκτυα ώστε να προσπελάσουν το βορειοδυτικό τμήμα του δίκτυο. Το παιχνίδι περιλαμβάνει το βιβλίο μαζί με τους κανόνες, τρία ζάρια, 156 κάρτες, 58 hacker cred tokens και 42 money tokens.
Το control-alt-hack έχει σχεδιαστεί για να ψυχαγωγεί τους παίκτες και να τους εκπαιδεύει στην ορολογία της ασφάλειας υπολογιστών. Το παιχνίδι έχει σχεδιαστεί με τέτοιο τρόπο ώστε οι παίκτες να επιθυμούν να παίξουν ξανά και ξανά, βέβαια σκοπός του είναι να μαθαίνουν ορολογίες στην ασφάλεια υπολογιστών (Denning, Kohno, Shostack, 2012). Το παιχνίδι από εκπαιδευτική άποψη έχει σχεδιαστεί για να βοηθήσει τους μαθητές να κατανοήσουν τις δυσκολίες στην ασφάλεια υπολογιστών. Αυτό έχει ως αποτέλεσμα οι παίκτες να μαθαίνουν πότε μπορεί να επιτεθεί ο δράστης. Επίσης, οι μαθητές μπορούν να μάθουν τι ικανότητες χρειάζονται ώστε να γίνουν επαγγελματίες στην ασφάλεια υπολογιστών.
Αν οι παίκτες γνωρίζουν από ασφάλεια υπολογιστών μπορούν να κατανοήσουν μερικά αστεία που αναφέρονται στο παιχνίδι και αποτελούν πραγματικά γεγονότα

που έχουν προηγηθεί από κάποια ατυχήματα στην ασφάλεια (Denning, Kohno, Shostack, 2012).

Το κύριο ακροατήριο του συγκεκριμένου παιχνιδιού είναι επιστήμονες στην αρχή της καριέρας τους στην επιστήμη των υπολογιστών, προπτυχιακοί, μεταπτυχιακοί φοιτητές και τελειόφοιτοι μαθητές (Hannah Hickey, 2012).

Ο πρωτεύον στόχος του παιχνιδιού είναι η αύξηση της γνώσης των ανθρώπων σε θέματα ασφάλειας υπολογιστών ώστε να είναι ενημερωμένοι σε τεχνολογικά θέματα (Denning, Kohno, Shostack, 2012). Ακόμη ένας στόχος του παιχνιδιού είναι να αποδώσουν μια σφαιρική κατανόηση της σημασίας που έχει η ασφάλεια υπολογιστών καθώς και τους πιθανούς κινδύνους που υπάρχουν στην ασφάλεια υπολογιστών ώστε σε μια επίθεση να κατανοήσουν τους κινδύνους και να αντιμετωπίσουν το πρόβλημα (Hannah Hickey, 2012). Επόμενος, στόχος είναι η εξέλιξη της γνώσης των παικτών σε θέματα τεχνολογίας και ασφάλειας υπολογιστών όχι μόνο στις συμβατικές υπολογιστικές πλατφόρμες ή τους web servers αλλά και στις αναδυόμενες πλατφόρμες και τα cyber physical συστήματα[1].

Ο δευτερεύον στόχος του παιχνιδιού είναι η γενική αντίληψη που υπάρχουν σε θέματα ασφάλειας υπολογιστών στα δύο φύλλα (Denning, Kohno, Shostack, 2012). Επομένως, το παιχνίδι αυτό μπορεί να θεωρηθεί ως μια ευκαιρία για να βοηθήσει τα δύο φύλλα σε αρνητικά στερεότυπα που υπάρχουν στην επιστήμη των υπολογιστών αλλά και στην ασφάλεια. Με αυτό τον τρόπο σημειώνεται η ποικιλία των επαγγελματικών και προσωπικών ευκαιριών που είναι διαθέσιμες για αυτούς τους επαγγελματίες (Hannah Hickey, 2012)..

Σε θέματα εκπαίδευσης οι στόχοι που εποικοδομούν οι μαθητές είναι η αναγνώριση πιθανόν απειλών, η εφαρμογή, η ασφάλεια διαχείρισης κινδύνου και οι άμυνες που υπάρχουν σε διάφορες επιθέσεις, με σκοπό να εξάψουν την περιέργεια των μαθητών για να αναζητήσουν στο Διαδίκτυο διάφορες επιθέσεις στην κυβερνοασφάλεια (Denning, Kohno, Shostack, 2012).

Για την δημιουργία του περιεχομένου των καρτών υπάρχουν κάρτες οι οποίες έχουν τεχνικό περιεχόμενο και περιέχουν mapping μηχανισμούς παιχνιδιών (Denning, Kohno, Shostack, 2012).

1 Control-alt-hack http://www.controlalthack.com/ (last visit: 20/2/2018)

Β.3 d0x3d!, μεθοδολογία και οδηγίες παιχνιδιού

Το d0x3d! είναι επιτραπέζιο παιχνίδι το οποίο σχεδιάστηκε για να εκπαιδεύσει τους μαθητές στην ορολογία της ασφάλειας δικτύου, στις επιθέσεις, στους μηχανισμούς άμυνας αλλά και σε βασικά θέματα υπολογιστών. Το παιχνίδι είναι ανοικτού κώδικα, επομένως μπορούν οι παίκτες να εκτυπώσουν τις οδηγίες και τις κάρτες για να διαμορφώσουν το παιχνίδι όπως επιθυμούν (Fredrik Svantes, 2013). Στην επίσημη ιστοσελίδα του αναφέρεται ως επιτραπέζιο παιχνίδι που έχει σχεδιαστεί για να εισάγει τους παίκτες στην ορολογία της ασφάλεια δικτύων για επιθέσεις αλλά και μηχανισμούς άμυνας για ενδεχόμενες επιθέσεις που υπάρχουν στην πραγματική ζωή (Fredrik Svantes, 2013).

Είναι διασκεδαστικό παιχνίδι και εκπαιδευτικό εργαλείο το οποίο διδάσκει την ασφάλεια δικτύων και πληροφοριών. Το συγκεκριμένο παιχνίδι έχει δυνατό εκπαιδευτικό χαρακτήρα στη διδασκαλία. Η φιλοσοφία του παιχνιδιού είναι ότι οι άνθρωποι τείνουν να μαθαίνουν καλύτερα ένα συγκεκριμένο τομέα μέσω των παιχνιδιών και έχει αποδειχθεί ότι είναι η καλύτερη πρακτική για την εκπαίδευση ενός αντικειμένου.

Ο τρόπος που παίζεται το παιχνίδι είναι ο εξής:

Το επιτραπέζιο παιχνίδι χρειάζεται τέσσερις παίκτες που αναλαμβάνουν τον ρόλο των χάκερς, διεισδύουν σε ένα δίκτυο για να διεκδικήσουν ότι προηγουμένως έχει κλαπεί. Τα δεδομένα που έχουν κλαπεί συνήθως είναι πολύτιμα ψηφιακά στοιχεία, όπως οικονομικά δεδομένα, προσωπικές πληροφορίες, διαπιστευτήρια ελέγχου ταυτότητας και δικαιώματα πνευματικής ιδιοκτησίας. Ενώ οι παίκτες ψάχνουν πολύτιμα ψηφιακά στοιχεία, οι διαχειριστές δικτύων αναλαμβάνουν να φτιάξουν μηχανισμούς και να τους ενεργοποιήσουν ή συναγερμούς ώστε να γνωρίζουν αν κάποιος έχει εισέλθει στο σύστημα ή έχει αλλάξει κάποιο κομμάτι στον κώδικα του δίκτυο, ώστε να αναγνωρίσουν τις κινήσεις των παικτών - χάκερ.

Ο Fredrik Svantes σε μια κριτική για το παιχνίδι αναφέρει ότι έχει δυναμισμό στην κανονική ροή του, αλλά και όταν οι παίκτες συζητούν μεταξύ τους για αληθινές επιθέσεις στην ασφάλεια υπολογιστών που προκύπτουν καθώς παίζουν. Επίσης, το παιχνίδι δίνει την δυνατότητα να πραγματοποιηθούν συζητήσεις για τις καλύτερες τεχνικές στην τοπολογία των δικτύων (ή σε άλλα θέματα δικτύων) και για την προστασία των εφαρμογών τους από επιθέσεις με τον καλύτερο τρόπο που υπάρχει (Fredrik Svantes, 2013).

Το παιχνίδι παίζεται από έναν έως τέσσερις παίκτες ενώ η ηλικία των παικτών κυμαίνεται από δώδεκα και πάνω. Η διάρκεια του παιχνιδιού είναι από τριάντα έως εξήντα λεπτά.

Υπάρχει το παιχνίδι d0x3d! το οποίο αποτελεί την κλασσική του έκδοση, αλλά υπάρχει και η πιο εξελιγμένη έκδοση η οποία ονομάζεται “d0x3d! v2 a network security game” που εκδόθηκε το 2013. Η καινούργια έκδοση του παιχνιδιού παίζεται από έναν έως τέσσερα άτομα (Mark Gondree & Zachary Peterson, 2013). Σε αυτή την έκδοση οι παίκτες συνεργάζονται μαζί με μία ομάδα εξειδικευμένων χάκερς οι οποίοι ψάχνουν, σε κομμάτια, ένα ασφαλές δίκτυο και αν βρεθεί κάποιο πρόβλημα το φτιάχνουν πριν οι διαχειριστές του δικτύου το ανακαλύψουν (Mark Gondree & Zachary Peterson, 2013). Οι παίκτες σε αυτό το παιχνίδι παίζουν εναντίον του χρόνου, έτσι ώστε όταν εισέλθουν στο ασφαλές δίκτυο, να ψάξουν σε κομμάτια όλο το δίκτυο, να ανακαλύψουν προβλήματα και να τα λύσουν πριν τους καταλάβουν οι διαχειριστές των δικτύων (Mark Gondree & Zachary Peterson, 2013). Η συγκεκριμένη έκδοση του παιχνιδιού αλλάζει το επιτραπέζιο παιχνίδι διότι υπάρχουν συγκεκριμένα κουτιά τα οποία έχουν απεριόριστες κινήσεις (Mark Gondree & Zachary Peterson, 2013). Επομένως, το δίκτυο αποτελείται από εικοσιτέσσερα κουτιά με ασύμμετρο μονοπάτι με σκοπό να παρακινήσει τους παίκτες και να τους υποχρεώσει να ανακαλύψουν μια διαδρομή μέσω του συστήματος της νέας έκδοσης (Mark Gondree & Zachary Peterson, 2013). Επίσης, στην νέα έκδοση του παιχνιδιού έχουν προστεθεί δύο νέοι ρόλοι για χάκερς ώστε να υπάρξει περισσότερη ποικιλία στους παίκτες (Mark Gondree & Zachary Peterson, 2013).

Γενικά, ο σκοπός του παιχνιδιού είναι να προστατέψουν τα προσωπικά τους αρχεία, αλλιώς οι διαχειριστές, αν καταλαβαίνουν ότι απειλούνται, δημοσιεύουν στο Διαδίκτυο τα στοιχεία τους και η ομάδα των χάκερς χάνει. Το παιχνίδι είναι διασκεδαστικό και εισάγει τους παίκτες στην ορολογία της ασφάλειας δικτύων. (Mark Gondree & Zachary Peterson, 2013).

Επίσης, οι παίκτες όσο παίζουν το εκπαιδευτικό παιχνίδι μαθαίνουν καινούργιες ορολογίες στην ασφάλεια δικτύων και αντιμετωπίζουν καθημερινά προβλήματα στην ασφάλεια υπολογιστών. Φυσικά το παιχνίδι προσπαθεί να περάσει το μήνυμα ότι η ασφάλεια δικτύων διαρκώς αλλάζει και αποτελεί ένα ανταγωνιστικό πεδίο.

B.4 Protection Poker, μεθοδολογία και οδηγίες παιχνιδιού

Το εκπαιδευτικό παιχνίδι Protection Poker είναι ένα απλό αλλά αποτελεσματικό παιχνίδι για την ασφάλεια δικτύων και είναι διαδικτυακό (Laurie Williams & Andrew Maneely, 2010). Συγκεκριμένα το αποτέλεσμα του παιχνιδιού είναι μια λίστα από κάθε απαίτηση για την ασφάλεια κινδύνου (Laurie Williams & Andrew Maneely, 2010).

Η ομάδα χρησιμοποιεί το σχετικό κίνδυνο για να καθορίσει τον τύπο και τον σχεδιασμό στο verification and validation (V&V) ώστε αυτό να περιλαμβάνεται σε κάθε απαίτηση. Έπειτα, η ομάδα μπορεί να χρησιμοποιήσει την συγκεκριμένη λίστα για να βοηθήσει στο security engineering που έχει τον υψηλότερο ρίσκο στην επίθεση, αυτό βασίζεται σε δυο παράγοντες, όπως πόσο εύκολη είναι η νέα λειτουργία για την επίθεση που γίνεται μέσω της λειτουργικότητας (Laurie Williams & Andrew Maneely, 2010). Οι προτεραιότητες και οι αυξημένες γνώσεις μπορούν να οδηγήσουν την ομάδα στην ανάπτυξη ασφαλών λογισμικών. Το Protection Poker λειτουργεί για τις ομάδες οι οποίες χρησιμοποιούν επαναληπτικές διαδικασίες ανάπτυξης (Laurie Williams & Andrew Maneely, 2010).

Πως παίζεται το παιχνίδι:

Οι ομάδες πραγματοποιούν συνάντηση για να συντονίσουν και να σχεδιάσουν την στρατηγική που θα ακολουθήσουν στο παιχνίδι (Laurie Williams & Andrew Maneely, 2010). Ο σκοπός της συνάντησης είναι να εστιάσουν σε συγκεκριμένες απαιτήσεις οι οποίες είναι πιθανόν να εφαρμοστούν κατά την διάρκεια του παιχνιδιού. Το παιχνίδι περιλαμβάνει τις επαναληπτικές διαδικασίες που υπάρχουν για κάθε απαίτηση και δίνονται στους παίκτες (Laurie Williams & Andrew Maneely, 2010). Η ομάδα πραγματοποιεί μια εκτίμηση για τις απαραίτητες ενέργειες που πρέπει να πραγματοποιηθούν ώστε να εφαρμοστεί η κάθε απαίτηση που δίνεται με τον σωστό τρόπο. Επομένως, η ομάδα χρειάζεται ένα σχέδιο στο οποίο απαιτούνται οι πόροι του συστήματος για την ασφαλή εφαρμογή τους (Laurie Williams & Andrew Maneely, 2010).

Στην αρχή, ο product manager ή ο ιδιοκτήτης της εταιρείας εξηγεί τις απαιτήσεις στην κάθε ομάδα που πρέπει να εφαρμόσουν ώστε να νικήσουν. Στην συνέχεια, πραγματοποιούνται συναντήσεις οι οποίες περιλαμβάνουν περαιτέρω συζητήσεις με τις απαιτήσεις που ζητήθηκαν μέχρι να λυθούν όλες οι απορίες στην ομάδα και οι διαδικασίες να είναι πλήρως εμπεριστατωμένες και κατανοητές (Laurie Williams & Andrew Maneely, 2010). Έπειτα, η ομάδα συζητά τις νέες απαιτήσεις και τις επιπτώσεις που θα υπάρξουν στο σύστημα για την ασφάλεια του. Επομένως, οι νέες ερωτήσεις τις ομάδας για τις επιπτώσεις της ασφάλειας του συστήματος κρίνουν αν το σύστημα γίνεται ευάλωτο σε επιθέσεις και αν σε μια υποτιθέμενη επίθεση, ο χάκερ θα ανακαλύψει τα κομμάτια του συστήματος τα οποία είναι ευάλωτα για να του επιτεθεί (Laurie Williams & Andrew Maneely, 2010). Επίσης, στο παιχνίδι υπάρχει ο επόμενος παίκτης με τον τίτλο Moderator ο οποίος πραγματοποιεί ερωτήσεις του τύπου, ποίος θα ήθελε να επιτεθεί στο σύστημα, ή τι θα κάνει ένας επιτιθέμενος αν λάβει δεδομένα και τα κλέψει, τα διαγράψει ή τα αλλοιώσει (Laurie Williams & Andrew Maneely, 2010). Η χρήση αυτής της λίστας για το σύστημα και η αυξημένη γνώση

των παικτών οδηγεί την ομάδα στην ανάπτυξη ασφαλών συστημάτων. Το παιχνίδι Protection Poker είναι επιτυχημένο στην ανάπτυξη των επαναληπτικών δομών, με μικρές σχετικές επαναλήψεις (Laurie Williams & Andrew Maneely, 2010).

Η γνώμη της ομάδας στο Protection Poker είναι σημαντική, συνήθως η ψήφος βασίζεται στις διαφωνίες, στην αναλογικότητα της άποψης και στην γνώμη του ειδικού (Laurie Williams & Andrew Maneely, 2010).

Ο κίνδυνος για την ασφάλεια των υπολογιστών βγαίνει από την εξίσωση:

Στην συνέχεια, για την νίκη του παιχνιδιού Protection Poker υπάρχουν κάποιες ερωτήσεις που πρέπει να απαντηθούν όπως:

1. Ποίος πίνακας από την βάση δεδομένων είναι πιθανόν να δεκτή επίθεση.
2. Ποίος πίνακας από την βάση δεδομένων θα δεχτεί επίθεση επειδή είναι πιο ευάλωτος.
3. Στην συνέχεια οι παίκτες του παιχνιδιού χρησιμοποιούν τις κάρτες, ώστε να σχεδιάσουν τις βάσεις δεδομένων, όποια είναι περισσότερο ευάλωτη για την πρώτη επίθεση τις δίνουν την κάρτα με την αξία “1”.
4. Κυκλώνουν την βάση δεδομένων με τις τιμές που έχουν δοθεί και τις βάζουν με την σωστή σειρά σύμφωνα με την αξία τους.

Στο επόμενο βήμα οι παίκτες βρίσκουν από τις απαιτήσεις που τους δόθηκαν τις ευάλωτες βάσεις δεδομένων οι οποίες προσθέτουν μεγαλύτερη ευελιξία και αποτελούν εύκολο στόχο για τους χακερς. Ακόμη, οι παίκτες οφείλουν να λαμβάνουν υπόψη τους, τις κάρτες του παιχνιδιού, οι οποίες έχουν αξία και δυσκολεύουν την επίθεση, καθώς υπάρχουν πόντοι με αξία και χρησιμοποιούνται για να νικήσει η ομάδα το παιχνίδι.

Έπειτα, οι παίκτες υπολογίζουν τους κινδύνους που έχει η κάθε απαίτηση για την ασφάλεια του συστήματος. Η αναγνώριση του κάθε πίνακα δίνεται μέσω των αξιών που δόθηκαν στους παίκτες, γι’ αυτό οι παίκτες χρησιμοποιούν τους πίνακες που έχουν μεγάλη αξία. Για τους πίνακες με την μικρή αξία τους δίνεται ο τίτλος “Poker a value”.

Στην συνέχεια, οι παίκτες πραγματοποιούν τον υπολογισμό του αθροίσματος των τιμών για την κάθε βάση δεδομένων. Τοποθετούν την τιμή poker για κάθε τιμή με εύκολους πόντους και πραγματοποιούν συζήτηση των αλλαγών που μπορούν να πραγματοποιήσουν ώστε να μειώσουν την επιτυχία της επίθεσης (Laurie Williams & Andrew Maneely, 2010).

Τέλος, υπολογίζουν τους κινδύνους ασφάλειας με τον πολλαπλασιασμό της εύκολης αξίας. Οι παίκτες στην συνέχεια κατατάσσουν τους κινδύνους συζητώντας στην ομάδα που συμμετέχουν. Τα βήματα που ακολουθούν στην κατάταξη του κάθε

κινδύνου αφορούν τις τιμές που δόθηκαν στους πίνακες με την αξία τους και τα σχέδια ανάλογα με την ασφάλεια του κάθε κινδύνου που έχουν δοθεί.

Β.5 Maelstrom, μεθοδολογία και οδηγίες παιχνιδιού

Το Maelstrom είναι ένα μοντέλο παιχνιδιού για να αφυπνίσει τους παίκτες και να τους δώσει πτυχές της εκπαίδευσης στην ασφάλεια υπολογιστών και την επαγγελματική πορεία που μπορούν να ακολουθήσουν στον τομέα της κεβερνοασφάλειας.
Το παιχνίδι επεκτείνει τις γνώσεις των παικτών από τις βασικές γνώσεις τους, στο επίπεδο που το παιχνίδι αποκαλεί “Ninja” για την ασφάλεια των δικτύων. Το μοντέλο του παιχνιδιού είναι βασισμένο στην μεθοδολογία του “Lockhead Martin kill chain attack lifecycle”. Το παιχνίδι επίσης έχει δανειστεί στοιχεία από το Framework MITRE και τα μοτίβα επιθέσεων από παλαιότερες επιθέσεις (Shane Stelgar, 2016).
Ο στόχος του εισβολέα στο συγκεκριμένο παιχνίδι είναι να επιτύχει σε όλα τα στάδια που για να νικήσει αλλά και να εκπαιδευτεί. Οι παίκτες που βρίσκονται στην άμυνα παίζουν κάρτες με τακτικές και στρατηγικές ώστε να αποτρέψουν αυτή την εξέλιξη της επίθεσης. Επίσης, οι παίκτες επιλέγουν πλευρές, ηθοποιό και αγοράζουν ή δημιουργούν τις δικές τους κάρτες για να έχουν στο παιχνίδι.
Το παιχνίδι αυτό περιλαμβάνει διάφορα στάδια του κύκλου των επιθέσεων, όπως το μοντέλο Lockhead Martin το οποίο βασίζεται σε αυτή την υπόθεση. Οι φάσεις είναι Reconnaissance, Weaponization, Delivery, Exploit, Install, Command, Control και Act on objects (Shane Stelgar, 2016).
Ο σκοπός του παιχνιδιού είναι εκπαιδεύσει τους παίκτες με σκοπό να χτίσουν τις δικές τους στρατηγικές για να αμυνθούν ή να επιτεθούν. Έτσι, παίζοντας το παιχνίδι οι παίκτες κατανοούν και δημιουργούν τις δικές τους στρατηγικές οι οποίες μπορούν να χρησιμοποιηθούν και στην πραγματική ζωή. Το παιχνίδι αυτό βοηθάει ώστε οι παίκτες να συλλαμβάνουν νέες ιδέες.
Ο τρόπος που παίζεται το παιχνίδι:
Αρχικά οι παίκτες διαλέγουν πόσα άτομα θα υπάρξουν στο παιχνίδι. Οι επιτιθέμενοι παίκτες επιλέγουν ή ζωγραφίζουν το μοντέλο απειλών και το δημιουργούν για τον ηθοποιό που διάλεξαν.
Παρακάτω δίνεται η λίστα που οι παίκτες μπορούν να επιλέξουν τον ηθοποιό τους.

- State Actor
- Ware Fighter
- Freelance Spy
- Script Kiddles
- Physical/Social

- Insider Threat
- Hacktivist
- Disgruntled Employee
- Corporate Spy
- Criminal Organization
- Criminal Freelance
- Joker

Στην συνέχεια, αφού οι παίκτες επιλέξουν τον κατάλληλο ρόλο-ηθοποιό, ο καθένας κρύβει την κάρτα του ώστε οι υπόλοιποι παίκτες να μην γνωρίζουν την επιλογή του. Ο λόγος που οι παίκτες κρύβουν τις κάρτες τους, είναι έτσι ώστε το παιχνίδι να μοιάζει με την πραγματική ζωή, που οι διαχειριστές δεν γνωρίζουν από ποιον απειλείται το σύστημα τους (Shane Stelgar, 2016). Έπειτα, οι παίκτες διαλέγουν την κάρτα η οποία γράφει τον τρόπο που θα επιτεθούν στο παιχνίδι.

Παρακάτω δίνεται η λίστα που περιλαμβάνει όλους αυτούς τους ρόλους, οι παίκτες ακόμη μια φόρα δεν ανακαλύπτουν τον ρόλο που επέλεξαν, οι ρόλο είναι:

- Humiliate
- Pivot From Shared Space
- Blackmail
- Denial Of Service / Crypto wall
- Destroy
- Data Disclosure
- Exfiltration
- Plant False Data Information
- Persistent Foothold for Future
- Defacement / Vandalism
- Any Act on Objectives Joke

Υπάρχουν δύο τρόποι που παίζεται το παιχνίδι, ο πρώτος είναι ο εύκολος και καλύτερος τρόπος για να ξεκινήσει το παιχνίδι με αρχάριους παίκτες σε θέματα ασφάλειας υπολογιστών και δικτύων. Η εύκολη έκδοση δεν συμβαδίζει με την αληθινή ζωή στα θέματα της ασφάλειας. Αρχικά, σε αυτή την έκδοση παίζουν δύο παίκτες με ένα ζάρι, ο παίκτης που φέρνει την μεγαλύτερη ζαριά επιλέγει αν είναι ο επιτιθέμενος ή ο αμυνόμενος (Shane Stelgar, 2016). Ο άλλος παίκτης παίρνει τον ρόλο που έχει απομείνει.

Στην συνέχεια, ο επιτιθέμενος σημειώνει τις δράσεις του και χτίζει τις κάρτες του σύμφωνα με τις δράσεις που έχει επιλέξει. Την ίδια διαδικασία ακολουθεί και ο αμυνόμενος για να δημιουργήσει τις κάρτες του, με σκοπό να αμυνθεί στις επιθέσεις

του αντιπάλου του. Επομένως, ο επιτιθέμενος χρησιμοποιεί κάρτες επίθεσης και ο αμυνόμενος παίκτης τις αντίστοιχες κάρτες άμυνας. Ο κύριος στόχος του επιτιθέμενου παίκτη είναι να φτάσει και να τερματίσει το επιτραπέζιο παιχνίδι με την χρήση των καρτών σύμφωνα με το σχέδιο που ανέπτυξε (Shane Stelgar, 2016).

Στο παιχνίδι υπάρχουν επτά κάρτες οι οποίες έχουν σχεδιαστεί από κάθε παίκτη με τον επιτιθέμενο παίκτη να παίζει πρώτος στον αρχικό γύρο του παιχνιδιού. Στην κάθε κάρτα του επιτιθέμενου ή αμυνόμενου υπάρχει η περιγραφή της δράσης της κάρτας καθώς και τα βήματα που ο παίκτης οφείλει να χρησιμοποιεί μέσα στο μοντέλου του Attack Life Cycle αλλά και την στρατηγική που σχεδίασε (Shane Stelgar, 2016).

Όταν ο παίκτης παίξει μια κάρτα τότε ο επόμενος παίκτης μπορεί να συνεχίσει το παιχνίδι και να παίξει μια κάρτα που αποτελεί την συνέχεια της κάρτας αυτής. Οι παίκτες μπορούν να καταστρέψουν οποία/ες κάρτες δεν τους χρειάζονται στο παιχνίδι ή να ζητήσουν την καταστροφή μια κάρτα και στην θέση της να επιλέξουν μια καινούργια. Επομένως, το παιχνίδι συνεχίζεται έως ότου οι παίκτες παίξουν όλες τις κάρτες.

Με κάθε κάρτα που οι παίκτες παίζουν, οφείλουν να γράφουν περιγραφές για τις κάρτες που παίζονται, και κάποια “Fact Fiction” όπως αναφέρονται στο παιχνίδι για να δημιουργήσουν την ιστορία του παιχνιδιού.

Το επόμενο επίπεδο είναι το “College Level”. Στο συγκεκριμένο επίπεδο παίζουν πολλοί παίκτες οι οποίοι διαλέγουν ποίος από αυτούς θα ρίξει το πρώτο ζάρι για να ξεκινήσει το παιχνίδι. Έπειτα επιλέγουν τον αμυνόμενο και επιτιθέμενο ρόλο (Shane Stelgar, 2016).

Τέλος, το δυσκολότερο επίπεδο για τους παίκτες που μπορούν να παίξουν ονομάζεται “Ninja Level”. Αυτή η έκδοση περιέχει αληθινά περιστατικά ασφάλειας, και παίζεται στρατηγικά με συγκεκριμένο χρηματικό ποσό, έτσι οι παίκτες αισθάνονται σαν να δουλεύουν. Σε αυτή την έκδοση του παιχνιδιού οι παίκτες κατανοούν πως είναι η αληθινή ζωή σε θέματα ασφάλειας (Shane Stelgar, 2016).

Το συγκεκριμένο επίπεδο αποτελείται από στρατηγικές επιλογές με ρεαλιστικές προκλήσεις. Σε αυτό το επίπεδο υπάρχουν πολλοί παίκτες που μπορούν να παίξουν μαζί. Οι παίκτες αποφασίζουν τους ρόλους των επιτιθέμενων και των αμυνόμενων. Στην συνέχεια, τους δίνετε ένα χρηματικό ποσό το οποίο συνήθως αποφασίζεται με τα ζάρια ή σύμφωνα με τις ανάγκες των παικτών, το οποίο συζητούν κατά την διάρκεια του παιχνιδιού. Το ποσό που έχουν επιλέξει οι παίκτες πολλαπλασιάζεται με την ζαριά που φέρει ο παίκτης, έτσι το ποσό που έχει επιλεγεί από τους παίκτες πολλαπλασιάζεται με εκατό χιλιάδες. Επομένως, αν ο παίκτης φέρει τρία στο ζάρι τότε αυτό πολλαπλασιάζεται με το πόσο του και ισούται με τριακόσιες χιλιάδες δολάρια. (Shane Stelgar, 2016).

Ο γενικός σκοπός του παιχνιδιού είναι να εκπαιδεύσει τους νέους παίκτες σε μια επίθεση μέσα σε ένα ασφαλές σύστημα δικτύου και τους τρόπους άμυνας ανάλογα με την επίθεση (Shane Stelgar, 2016). Επίσης, οι παίκτες μαθαίνουν τον τρόπο σκέψης των χάκερς και τις λύσεις σε διάφορες επιθέσεις που συμβαίνουν σε αληθινά περιστατικά. Οι παίκτες μέσω του παιχνιδιού μαθαίνουν να πραγματοποιούν πιο αποτελεσματικές και επιθετικές στρατηγικές, ώστε να εκπαιδευτούν σε επιθέσεις και άμυνες.

Β.6 Cyber Threat Defender, μεθοδολογία και οδηγίες παιχνιδιού

Το παιχνίδι καρτών Cyber Threat Defender αποτελείται από πολλούς παίκτες που μπορούν να παίξουν μαζί και έχει σχεδιαστεί για να τους διδάξει διάφορες πληροφορίες, ορολογίες και στρατηγικές στο Cyber Security.

Το συγκεκριμένο παιχνίδι είναι εύκολο και δεν υπάρχει όριο ηλικίας ή επίπεδο των γνώσεων που μπορεί να έχει ο παίκτης. Ο στόχος του παιχνιδιού είναι οι παίκτες να προστατευτούν από επιθέσεις, καθώς σχεδιάζουν και φτιάχνουν, το δίκτυο τους, με σκοπό να γίνουν αληθινοί Cyber Threat Defenders. Το παιχνίδι συνιστάται να παίζεται από προπτυχιακούς ή μεταπτυχιακούς φοιτητές στην επιστήμη της Πληροφορικής (CIAS, UTSA)[2].

Κυρίως το παιχνίδι χρησιμοποιείται από τους καθηγητές, σε μαθητές γυμνασίου ώστε να διδαχτούν την βασική ορολογία του cyber security αλλά και σε μαθητές λυκείου για να διδαχτούν τρόπους άμυνας σε αληθινές επιθέσεις. Το συγκεκριμένο παιχνίδι έχει πάρει την ιδέα από το παιχνίδι με κάρτες Magic: The Gathering. Κανόνες του Cyber Threat Defender:

Οι παίκτες πρέπει να χρησιμοποιούν στην διάρκεια του παιχνιδιού κάποιο αντικείμενο για να ελέγχουν και να κρατούν την βαθμολογία τους. Κάθε παίκτης έχει τις δικές του κάρτες στο χέρι του, οι οποίες πρέπει να είναι τουλάχιστον πενήντα. Κάθε παίκτης ξεκινάει το παιχνίδι χτίζοντας το σύστημα του, επομένως πρέπει να υπάρχουν στο τραπέζι κάρτες όπως Desktop Computer και ISP συνδέσεις. Στην συνέχεια ανακατεύουν το deck με τις κάρτες τους και διαλέγουν επτά κάρτες που έχει ο παίκτης στο παιχνίδι.

Πως παίζεται το παιχνίδι:

Σε κάθε φάση οι παίκτες παίζουν παραπάνω από τρεις κάρτες με οποιονδήποτε συνδυασμό για επίθεση, άμυνα ή για άλλο σκοπό. Μπορούν να παίξουν δύο κάρτες

2 CIAS, UTSA http://cias.utsa.edu/ctd.php

από οποιονδήποτε τύπο καρτών σε κάθε φάση. Οι κάρτες event χρησιμοποιούνται οποιαδήποτε στιγμή. Όταν οι παίκτες έχουν τελειώσει με τις κάρτες που παίζουν, τότε πετάνε τις κάρτες που έχουν στα χέρια τους και μένουν μόνο με πέντε (CIAS, UTSA)[3].

Στην συνέχεια, σχεδιάζουν δύο ακόμη κάρτες, αν η στήλη που σχεδιάζονται οι κάρτες είναι άδειες τότε οι παίκτες ανακατεύουν τις κάρτες που πέταξαν και παίρνουν δύο κάρτες ακόμη στα χέρια τους για να γεμίσει η στήλη. Σε κάθε γύρο σημειώνεται η βαθμολογία των παικτών. Για να βγάλουν οι παίκτες την βαθμολογία τους πρέπει να προσθέσουν τους πόντους τους από τις κάρτες που έχουν κατεβάσει.

Το παιχνίδι τελειώνει μόλις ένας παίκτης φτάσει τριάντα πόντους. Αν οι δύο παίκτες φτάσουν ταυτόχρονα τους τριάντα πόντους στον ίδιο γύρο, τότε ο παίκτης με το μεγαλύτερο σύνολο νικάει. Όμως αν και οι δύο παίκτες έχουν το ίδιο σύνολο τότε το παιχνίδι συνεχίζεται μέχρι να φτάσει κάποιος από τους δύο, τους σαράντα πόντους. Αν πάλι υπάρχει ισοβαθμία στο παιχνίδι τότε αυτό συνεχίζεται μέχρι να βρεθεί νικητής.

Επίσης, αν ο παίκτης χάσει την σειρά του τότε δεν λαμβάνει πόντους. Στο αρχή του κάθε γύρου ο παίκτης μπορεί να δηλώσει το Critical Failure System. Με αυτό ο παίκτης που το δηλώνει παίρνει ξανά όλες τις κάρτες και ξεκινάει το παιχνίδι από την αρχή μαζί με την κάρτα ISP Connection και την Desktop Computer. Το παιχνίδι περιλαμβάνει τις κάρτες με τις κατηγορίες:

- Asset
- Defense
- Event
- Attack
- Sponsor Cards

Το Cyber Threat Defender πρέπει να διδάσκεται σε όλους τους ανθρώπους ανεξαρτήτως ηλικία. Γενικά, το cyber security πρέπει να διδάσκεται σε όλους τους κλάδους διότι ότι αρχείο ανεβαίνει, ότι λογαριασμός υπάρχει στο σύννεφο, κάθε διαδικτυακή κάμερα, παρουσιάζει μια ευκαιρία στους χάκερς ώστε να εισβάλουν στο σύστημα και να εισέλθουν στο λειτουργικό σύστημα για να υποκλέψουν ευαίσθητα προσωπικά στοιχεία. Επομένως, όταν οι άνθρωποι εκπαιδεύονται στο cyber security μαθαίνουν και να χτίζουν μια ασφαλή κοινωνία (CIAS, UTSA).

3 CIAS, UTSA http://cias.utsa.edu/ctd.php

Κεφάλαιο Γ’

Το παιχνίδι

Γ.1 Το παιχνίδι καρτών Defender

Το παιχνίδι Defender είναι ένα εκπαιδευτικής φύσης παιχνίδι σοβαρού σκοπού, με σκοπό οι παίκτες να διακρίνουν τα στάδια του cyber kill chain μιας Advanced Persistent Threat επίθεσης.

Η βασική ιστορία του παιχνιδιού βρίσκεται στα πλαίσια του κυβερνοπόλεμου που γίνεται μεταξύ δύο κρατών. Οι cyberwars προσπαθούν να καταφέρουν καίρια χτυπήματα προς μεγάλους οργανισμούς των κρατών. Σε ένα τελευταίο περιστατικό οι cyber-warriors φαίνεται ότι χτυπούν πολλούς οργανισμούς με σκοπό την δημιουργία δυσλειτουργίας (όπως η διαγραφή αρχείων, η παύση λειτουργίας, η δημοσιοποίηση απόρρητων στοιχείων) των υπηρεσιών των οργανισμών. Το προφίλ του επιτιθέμενου είναι cyber-warrior.

Γ.2 Cyber Kill Chain

Το μοντέλο Cyber Kill Chain δημιουργήθηκε από τον Lockheed Martin, είναι γνωστό ως ο κύκλος ζωής των κυβερνητικών επιθέσεων. Στην στρατιωτική ορολογία ο όρος Kill Chain είναι ένα μοντέλο φάσεων και περιγράφει τα στάδια μιας επίθεσης αλλά και ενημερώνει τους αμυνόμενους για τους τρόπους που μπορεί να αποφευχθεί μια τέτοια επίθεση. Τα στάδια στο στρατιωτικό μοντέλο Kill Chain είναι η αναζήτηση, διόρθωση, ανίχνευση, συμπλοκή και εκτίμηση.

Αποτελεί το μοντέλο για την αναγνώριση και την πρόληψη από cyber επιθέσεις. Το μοντέλο προσδιορίζει τα στάδια που κάνουν οι επιτιθέμενοι προκειμένου να ολοκληρώσουν μια κυβερνητική επίθεση και να πετύχουν τον στόχο τους. Το cyber Kill Chain μοντέλο έχει εστιάσει στις επιθέσεις που οφείλονται σε διάφορους τύπους ιών (malware). Επίσης, ο σκοπός του μοντέλου είναι οι οργανισμοί να προστατεύσουν το δίκτυο τους από τέτοιες επιθέσεις .

Το μοντέλο αποτελείται από επτά βήματα που βελτιώνουν την ορατότητα σε μια επίθεση, ώστε ο αναλυτής να κατανοήσει τον αντίπαλο του, τις τακτικές, τεχνικές και διαδικασίες που χρησιμοποιεί προκειμένου να επιτεθεί σε έναν οργανισμό. Κάθε στάδιο του μοντέλου δείχνει το μονοπάτι με τους στόχους του επιτιθέμενου .

Η επίθεση APT είναι από τα αρχικά Advanced Persistent Threat.

Τα βήματα της επίθεσης του μοντέλου Cyber Kill Chain είναι:

1. Reconnaissance (Ανίχνευση): Ο επιτιθέμενος αναζητεί απόρρητες πληροφορίες για τον οργανισμό όπως είναι τηλεφωνικοί αριθμοί, διευθύνσεις e-mails, την λίστα υπαλλήλων στον οργανισμό ή την τοποθεσία που βρίσκονται οι servers του οργανισμού. Αυτές τις πληροφορίες μπορεί εύκολα να το ανακαλύψει μέσω μιας απλής αναζήτησης σε ιστοσελίδες κοινωνικής δικτύωσης ή από αναζητήσεις για σχετικές πληροφορίες του οργανισμού. Στο Διαδίκτυο υπάρχουν πολλές πληροφορίες των οργανισμών που ο σκοπός τους είναι η ενημέρωση. Όμως ο επιτιθέμενος μπορεί να χρησιμοποιήσει αυτές τις πληροφορίες για να βλάψει τον οργανισμό. Στην συνέχεια χρησιμοποιεί τα δεδομένα που ανακάλυψε για να δημιουργήσει ένα δίαυλο επικοινωνίας με τον οργανισμό. Ο επιτιθέμενος μπορεί να εκτελέσει την επίθεση του με πληροφορίες που ανακάλυψε στο Διαδίκτυο. Ο επιτιθέμενος προσπαθεί να ψυχολογήσει το θύμα του, και να συλλέξει πολλές πληροφορίες, όπως το ιστορικό του περιηγητή ή τις διευθύνσεις e-mail που χρησιμοποιεί το θύμα.
2. Weaponization (Εξοπλισμός): Στο δεύτερο βήμα, ο επιτιθέμενος ενημερώνει τους υπαλλήλους του οργανισμού ότι θα λάβουν ένα e-mail από την τεχνική υποστήριξη του οργανισμού. Στην συνέχεια, δημιουργεί το όπλο με το οποίο θα επιτεθεί στον οργανισμό. Το όπλο αυτό μπορεί να είναι ένα αρχείο word, pdf στο οποίο θα εισάγει τον μολυσμένο κώδικα.
3. Delivery (Παράδοση): Στο επόμενο βήμα, ο επιτιθέμενος στέλνει το μολυσμένο αρχείο με διάφορους τρόπους, όπως με e-mail ή με την μεταφορά αρχείου μέσω φορητής συσκευής σκληρού δίσκου.
4. Exploitation (Εκμετάλλευση): Ο επιτιθέμενος εκμεταλλεύεται τις αδυναμίες των υπαλλήλων προκειμένου να εκτελέσουν το αρχείο που στάλθηκε ώστε ο υπολογιστής του θύματος να μολυνθεί χωρίς να γνωρίζει ότι πρόκειται για ιό. Ο επιτιθέμενος το καταφέρνει στέλνοντας, για παράδειγμα, ένα μήνυμα που το θύμα θα εμπιστευθεί τον αποστολέα, αν δεν υπάρχουν επιπλέον μέτρα ασφάλειας στο ηλεκτρονικό ταχυδρομείο του οργανισμού, όπως ένα λογισμικό προστασίας από ιούς.
5. Installation (Εγκατάσταση): Όπως προαναφέρθηκε το θύμα λαμβάνει με κάποιο τρόπο το μολυσμένο αρχείο. Όταν το αρχείο εκτελεστεί πραγματοποιείται εγκατάσταση του μολυσμένου κώδικα.

6. Command & Control (Υποδομή εντολών ελέγχου): Δημιουργείται ένα κανάλι επικοινωνίας με τον επιτιθέμενο, ανάλογα με τους στόχους της επίθεσης.
7. Actions on Objectives (Ενέργειες στο στόχο): Με την πρόσβαση στον υπολογιστή του θύματος, ο επιτιθέμενος πετυχαίνει τους αρχικούς στόχους του.

Οι οργανισμοί χρησιμοποιούν το μοντέλο ώστε την κατάλληλη στιγμή να αναγνωρίσουν την επίθεση και να την αποτρέψουν. Βέβαια, χρησιμοποιώντας το μοντέλο αυτό χρειάζεται ιδιαίτερη ευφυΐα για να ανιχνεύσουν οι οργανισμοί το πρόβλημα στο δίκτυο τους. Ο διαχειριστής του δικτύου οφείλει να γνωρίζει το σύστημα. Επίσης, οι οργανισμοί είναι καλό να χρησιμοποιούν συναγερμούς για παραβιάσεις στο σύστημα τους. Όσο πιο γρήγορα οι οργανισμοί αντιληφθούν ότι δέχονται επίθεση, με την χρήση του μοντέλου Cyber Kill Chain, τόσο το καλύτερο για να αποτρέψουν την επίθεση.

Από την άλλη πλευρά, αν η επίθεση δεν γίνει ορατή γρήγορα, τότε χρειάζεται προσπάθεια για να σώσουν τα μηχανήματα που μολύνθηκαν, αλλά και να κατανοήσουν τις αλλαγές που έγιναν στο δίκτυο τους καθώς και τις απόρρητες πληροφορίες που έκλεψαν οι επιτιθέμενοι[4] .

Σχεδιάζοντας το σύστημα παρακολούθησης με το μοντέλο Cyber Kill Chain αποτελεί μια αποτελεσματική μέθοδο, καθώς επικεντρώνεται σε πραγματικές κυβερνοεπιθέσεις.

Οι πιο κοινοί τύποι εξοπλισμού που χρησιμοποιούν οι cyber criminals είναι:

- Botnet: Αποτελεί όπλο στο οποίο ο επιτιθέμενος χρησιμοποιεί ένα δίκτυο από ηλεκτρονικούς υπολογιστές και με μη εξουσιοδοτημένη άδεια τους αναγκάζει να εργάζονται ταυτόχρονα.
- DDoS: Οι επιθέσεις Distributed Denial of Service εκτελούνται όταν το σύστημα υπολογιστών ή το δίκτυο πλημμυρίζει από δεδομένα κίνησης. Αυτό έχει ως αποτέλεσμα το σύστημα να μην μπορεί να διαχειριστή την κίνηση από τις αιτήσεις, με αποτέλεσμα το σύστημα να τίθεται εκτός λειτουργίας και να μην ανταποκρίνεται καθόλου.
- Malware: Σε αυτή την περίπτωση, στο σύστημα εισέρχεται το μολυσμένο λογισμικό, χωρίς το θύμα να το καταλάβει ότι το σύστημα του μολύνθηκε.

4 Deloitte, 2017 https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf (last visit: 26/1/2019)

Τέτοια παραδείγματα από ιούς είναι τα worms, trojan horse, logic bombs, viruses, packet sniffers[5].

Δύο βασικοί μέθοδοι παράδοσης είναι:

- Ελεγχόμενη παράδοση, η οποία περιλαμβάνει άμεσο hacking μέσω ανοικτής θύρας (port).
- Παράδοση μέσω κυκλοφορίας, στην οποία προωθεί το malware στον στόχο μέσω Phishing.

Γ.3 Ανάλυση Defender

Στο παιχνίδι Defender υπάρχουν συνολικά πέντε σενάρια, που οι λύσεις τους προέρχονται από την μεθοδολογία CAPEC. Συνολικά υπάρχουν επτά στάδια στα οποία οι παίκτες, σύμφωνα με το σενάριο που τους δόθηκε πρέπει να συνδυάσουν σωστά τις κάρτες που έχουν στο χέρι τους και να απαντήσουν σωστά στο κάθε στάδιο της επίθεσης που τους δίνεται. Η κάθε φάση του παιχνιδιού αποτελεί ένα στάδιο από την επίθεση που πραγματοποιείται εναντίον του οργανισμού που ο επιτιθέμενος εκτελεί την επίθεση του. Στόχος του κάθε παίκτη είναι να ανακύψει τα μοτίβα επιθέσεων και να αμυνθεί σε κάθε στάδιο.

Ο πρώτος παίκτης που θα αμυνθεί σωστά και θα ολοκληρώσει τα επτά στάδια του σεναρίου του, είναι ο νικητής του παιχνιδιού. Στόχος του παιχνιδιού είναι οι παίκτες να συνδυάσουν σωστά τις κάρτες για να λύσουν το στάδιο που βρίσκονται. Ο παίκτης που κατεβάζει τις κάρτες με την λύση του προβλήματος περνάει στο επόμενο στάδιο. Σε κάθε γύρο οι παίκτες επιλέγουν την κάρτα-λύση που δεν τους χρησιμεύει για την λύση του σταδίου τους και σηκώνουν μια καινούργια κάρτα από το deck.

Οι παίκτες που δεν κατάφεραν να λύσουν το πρόβλημα παραμένουν στο ίδιο στάδιο, ενώ οι παίκτες που κατάφεραν να λύσουν το πρόβλημα, πηγαίνουν στο επόμενο στάδιο της επίθεσης.

Συνολικά στο παιχνίδι υπάρχουν επτά στάδια, τα οποία αποτελούν τα στάδια επίθεσης από το μοντέλο Cyber Kill Chain. Ο παίκτης σκέφτεται ως χάκερ και προσπαθεί να δημιουργήσει άμυνες και τρόπους αντιμετώπισης στις επιθέσεις που

5Deloitte, 2017 https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf (last visit: 26/1/2019)

είναι βασισμένες στο μοντέλο Cyber Kill Chain. Ο στόχος του είναι να αναγνωρίσει πιθανές αδυναμίες στην ασφάλεια του συστήματος του, πριν οι χάκερς επιτεθούν στα δεδομένα της εταιρείας του.

Γ.4 Σενάρια παιχνιδιού

Γ.4.1 Πρώτο σενάριο

- **Στάδιο 1ο - Reconnaissance (Ανίχνευση):**

  Οι χάκερς έχουν στόχο την εταιρεία που δουλεύεις και ασχολείται με την εξόρυξη δεδομένων. Ξεκινούν να ανιχνεύουν και να μαθαίνουν πληροφορίες από τις ιστοσελίδες, social media, linkedin ώστε να συλλέξουν διευθύνσεις e-mails, τηλεφωνικούς αριθμούς και την ιεραρχική κλίμακα των υπαλλήλων της εταιρείας (CTO, managers,leaders, developers κτλ). Επικοινωνούν μαζί σου και προσποιούνται ότι είναι εταιρεία που συνεργάζεσαι, με αποτέλεσμα να σου προσφέρουν αναβάθμιση των servers σας. Ο υπάλληλος αποκαλύπτει πληροφορίες για τα μηχανήματα της εταιρείας.

  Λύση - Άμυνα του παίκτη

  1. Διεξαγωγή αξιολόγησης του προσωπικού για να εξακριβωθεί ο βαθμός που ακολουθούνται οι πολιτικές ασφαλείας.
  2. Εκπαίδευση υπαλλήλων σε θέματα ασφάλειας μέσω της παρουσίασης και ανάλυσης πραγματικών περιστατικών ασφάλειας.
  3. Έλεγχος των πληροφοριών που δημοσιεύονται στις ιστοσελίδες των υπαλλήλων, τους λογαριασμούς κοινωνικών δικτύων ψάχνοντας για ονόματα υπαλλήλων, ονόματα χρηστών, κωδικούς ασφαλείας, λογαριασμούς ηλεκτρονικού ταχυδρομείου.
  4. Καταγραφή των κινήσεων των χρηστών και των συμβάντων του δικτύου σε αρχεία καταγραφής (Log Files)

- **Στάδιο 2ο - Weaponization (Εξοπλισμός):**

Οι χάκερς βρίσκουν αδυναμίες για το λειτουργικό σύστημα του server της εταιρείας σου και δημιουργούν αρχείο τύπου docx στο οποίο εισάγουν ιό τύπου δούρειο ίππο (Remote Access Trojan, RAT) για να εισβάλουν στο σύστημα της εταιρείας σου.

Λύση - Άμυνα του παίκτη

1. Συγκέντρωση πληροφοριών σχετικά με τους δυνητικούς αντιπάλους, τις τακτικές, τις τεχνικές και τις διαδικασίες που χρησιμοποιούν καθώς και των τάσεων που επικρατούν.
2. Ανάλυση των αρχείων καταγραφής κινήσεων των χρηστών και των συμβάντων του δικτύου με σκοπό να ανιχνευθούν τυχόν κινήσεις των επιτιθεμένων.
3. Ενημέρωση βάσης δεδομένων ιών του λογισμικού προστασίας Antivirus

Στάδιο 3ο - Delivery (Παράδοση):

Οι χάκερς δημιουργούν αληθοφανή spoofed e-mails από συνεργαζόμενη επιχείρηση και επισυνάπτουν το αρχείο. Επίσης, επικοινωνούν με την εταιρεία ώστε οι υπάλληλοι να περιμένουν το e-mail. Οι υπάλληλοι πέφτουν στην παγίδα και ανοίγουν το e-mail μαζί με το αρχείο, έτσι εκτελείται ο ιός και μολύνει τα συστήματα των υπαλλήλων.

Λύση - Άμυνα του παίκτη

1. Έλεγχος των εισερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου και των επισυναπτόμενων αρχείων στο διακομιστή ηλεκτρονικής αλληλογραφίας πριν σταλθούν στον τελικό χρήστη.
2. Χρήση Sender Policy Framework ώστε να ελέγχεται αν οι IP διευθύνσεις των αποστολέων e-mail, συμπίπτουν με τις IP διευθύνσεις που έχουν δηλωθεί στους DNS servers για τα domain του αποστολέα. Έτσι διενεργείται επαλήθευση του αποστολέα και μειώνονται τα πλαστά (spoofed) μηνύματα ηλεκτρονικού ταχυδρομείου.

3. Απαγόρευση λήψης e-mail που προέρχονται από γνωστές μη έμπιστες διευθύνσεις IP (blacklisting).
4. Χρήση προγραμμάτων Antivirus για σάρωση των e-mails

- **Στάδιο 4ο - Exploitation (Εκμετάλλευση):**

Οι χάκερς εκμεταλλεύονται την αδυναμία του λειτουργικού συστήματος Windows Server 2008 R2 για x64-based Systems Service pack. Πρόκειται για την ευπάθεια στην μνήμη των γραφικών. Ενσωματώνουν στο αρχείο ειδικά σχεδιασμένη γραμματοσειρά που επιτρέπει την εκτέλεση αυθαίρετου κώδικα, σύμφωνα με την αδυναμία του λειτουργικού συστήματος.

Λύση - Άμυνα του παίκτη

1. Έλεγχος και αναβάθμιση του λογισμικού στην τελευταία έκδοση.
2. Ενεργοποίηση αυτοματοποιημένων ενημερώσεων ασφαλείας του λογισμικού και περιοδικός έλεγχος από τον υπεύθυνο ασφάλειας.
3. Εφαρμογή καταλόγων ελέγχου πρόσβασης (Access Control Lists) για την επιβολή χρήσης ανάγνωσης και επεξεργασίας αρχείων κειμένου όπως docx και PDF με λογαριασμούς χρηστών που έχουν περιορισμένα δικαιώματα, και όχι με λογαριασμούς που έχουν δικαιώματα διαχειριστή.

- **Στάδιο 5ο -Installation (Εγκατάσταση):**

Μόλις ο υπάλληλος ανοίξει το αρχείο γίνεται αυτόματη εγκατάσταση του μολυσμένου κώδικα που είναι ενσωματωμένη στο αρχείο. Αυτό το πετυχαίνουν με την εγκατάσταση backdoor (μέθοδος, συχνά μυστική, για την παράκαμψη του ελέγχου αυθεντικοποίησης στα συστήματα υπολογιστών) στο σύστημα.

Λύση - Άμυνα του παίκτη

1. Έλεγχος των υπολογιστών του δικτύου με εργαλεία εντοπισμού και προστασίας από κακόβουλο λογισμικό.

2. Έλεγχος των υπολογιστών του δικτύου με εργαλεία που βασίζονται στον εντοπισμό ανωμαλιών στη συμπεριφορά των χρηστών σε πραγματικό χρόνο.

Στάδιο 6ο - Command & Control (Υποδομή εντολών ελέγχου):

Οι χάκερς με την εγκατάσταση του backdoor που έγινε στο προηγούμενο στάδιο δημιουργούν ένα αποκλειστικό κανάλι επικοινωνίας για την διαρκεί επικοινωνία με το σύστημα.

Λύση - Άμυνα του παίκτη

1. Έλεγχος της κίνησης στο εσωτερικό του δικτύου με τη δημιουργία συστημάτων υπηρεσιών διαδικτύου που χρησιμοποιούν τείχη προστασίας και διαμεσολαβητές.
2. Παραχώρηση πρόσβασης επικοινωνίας μόνο σε εγκεκριμένες διευθύνσεις (Whitelist).
3. Απαγόρευση peer-to-peer κίνησης (π.χ. Skype, Cisco Jabber κ.α.) για τυχόν παρεμπόδιση των σχεδίων του επιτιθέμενου για να χρησιμοποιήσει P2P υποδομή – bot master.

Στάδιο 7ο Actions on objectives:

Στο τελικό στάδιο, οι χάκερς κλέβουν πολύτιμες πληροφορίες από την εξόρυξη δεδομένων που ασχολείται η εταιρεία σου, στην συνέχεια τα κρυπτογραφούν σε συμπιεσμένο αρχείο RAR και τα μεταφέρουν μέσω FTP proxy server. Τέλος, σβήνουν ένα σημαντικό ποσοστό δεδομένων της εταιρείας σου. Η επίθεση τους έχει τελειώσει.

Λύση - Άμυνα του παίκτη

1. Η εξερχόμενη διαδικτυακή κίνηση που αφορά τα πρωτόκολλα μεταφοράς αρχείων (FTP ή SFTP) θα πρέπει να γίνεται μέσω proxy.
2. Εντοπισμός και έλεγχος εισερχόμενων συνδέσεων TCP που έχουν μεγάλη διάρκεια και πιθανότατα εξάγουν κρυπτογραφημένα δεδομένα.

3. Δημιουργία πλάνου για την τήρηση αντιγράφων ασφαλείας σε καθημερινή ή εβδομαδιαία βάση για την επαναφορά του συστήματος σε περίπτωση απώλειας δεδομένων.
4. Ασφαλής αποθήκευση των αντιγράφων ασφαλείας.
5. Ανίχνευση εξερχόμενων RAR αρχείων στο σύστημα

Γ.4.2 Δεύτερο εκπαιδευτικό σενάριο

- **Στάδιο 1ο - Reconnaissance:**

Οι χάκερς έχουν ως στόχο την εταιρεία που δουλεύεις και ασχολείται με την δημιουργία λογισμικών για ιατρικά μηχανήματα. Ξεκινούν να αναζητούν για πληροφορίες στο Διαδίκτυο και στην ιστοσελίδα της εταιρείας. Χαρτογραφούν την δημοσιευμένη ιστοσελίδα της εταιρείας και προσπαθούν να ανακαλύψουν μη δημοσιοποιημένες σελίδες και υπηρεσίες που χρησιμοποιεί η εταιρεία.

Λύση - Άμυνα του παίκτη

1. Διεξαγωγή αξιολόγησης του προσωπικού για να εξακριβωθεί ο βαθμός που ακολουθούνται οι πολιτικές ασφαλείας, όπως με την αποστολή δελεαστικών e-mails που καλούν το προσωπικό να ακολουθήσει κάποιο σύνδεσμο, ή τηλεφωνικές συνομιλίες που καλούν το προσωπικό να αποκαλύψει χρήσιμες πληροφορίες.
2. Εργαλείο τύπου Σύστημα Ανίχνευσης Εισβολής (Intrusion Detection System - IDS) το οποίο παρακολουθεί και ενημερώνει αν υπάρχει οποιαδήποτε ύποπτη σάρωση στο σύστημα με εργαλεία τύπου Nmap.
3. Εκπαίδευση σε θέματα ασφάλειας μέσω της παρουσίασης και ανάλυσης πραγματικών περιστατικών επιθέσεων.

- **Στάδιο 2ο - Weaponization:**

  Οι χάκερς, χρησιμοποιούν το εργαλείο Metasploit και δημιουργούν malware τύπου rootkit (λογισμικό που επιτρέπει την συνεχή πρόσβαση σε έναν υπολογιστή με προνόμια υπερχρήστη, ενώ κρύβει ενεργά την παρουσία του από τους διαχειριστές). Βάζουν στο rootkit μολυσμένο κώδικα, σύμφωνα με τις αδυναμίες που βρήκαν στην ανίχνευση για τις υπηρεσίες που χρησιμοποιεί η εταιρεία.

Λύση - Άμυνα του παίκτη

1. Εξέταση των αρχείων καταγραφής και των συμβάντων από τους υπεύθυνους ασφαλείας.
2. Συγκέντρωση πληροφοριών σχετικά με τους δυνητικούς αντιπάλους, τις τακτικές, τις τεχνικές και τις διαδικασίες που χρησιμοποιούν, καθώς και των τάσεων που επικρατούν.
3. Παρακολούθηση της συμπεριφοράς του υπολογιστή για ύποπτες δραστηριότητες (εγκατάσταση προγραμμάτων απρόοπτα, απενεργοποίηση λογισμικού για: Antivirus, task manager, registry editor)
4. Ενημέρωση όλων των λογισμικών στην τελευταία έκδοση, ειδικά του προγράμματος προστασίας από ιούς.

- **Στάδιο 3ο - Delivery:**

  Οι χάκερς δημιουργούν αληθοφανή ιστοσελίδα τράπεζας με τον ιό και στέλνουν e-mails στην ομάδα υπαλλήλων της εταιρείας σου. Στην συνέχεια περιμένουν. Αν κάποιος από τους υπαλλήλους ανοίξει την ιστοσελίδα τότε ξεκινάει η εγκατάσταση του rootkit. Ο στόχος τους είναι να ανοίξουν επικοινωνία με τον υπολογιστή του θύματος, για να αποσπάσουν πληροφορίες.

Λύση - Άμυνα του παίκτη

1. Αποκλεισμός χρήσης υπηρεσιών ηλεκτρονικού ταχυδρομείου, μεταφοράς αρχείων και ιστοσελίδες κοινωνικής δικτύωσης που παρέχονται από εξωτερικούς εξυπηρετητές
2. Χρήση Sender Policy Framework ώστε να ελέγχεται αν οι IP διευθύνσεις των αποστολέων e-mail συμπίπτουν με τις IP διευθύνσεις που έχουν δηλωθεί στους DNS servers για τα domain του αποστολέα. Έτσι διενεργείται επαλήθευση του αποστολέα και μειώνονται τα πλαστά (spoofed) μηνύματα ηλεκτρονικού ταχυδρομείου
3. Απαγόρευση λήψης e-mail που προέρχονται από γνωστές μη έμπιστες διευθύνσεις IP (blacklisting).

- **Στάδιο 4ο - Exploitation:**

Οι χάκερς από τις υπηρεσίες που βρήκαν εκμεταλλεύονται την εταιρική διεύθυνση e-mail που χρησιμοποιείται μόνο για τους υπάλληλους και έτσι εκτελείται η επίθεση με τα phishing e-mails και την πλαστή ιστοσελίδα.

Λύση - Άμυνα του παίκτη

1. Έλεγχος και αναβάθμιση του λογισμικού περιήγησης και ανάγνωσης μηνυμάτων ηλεκτρονικού ταχυδρομείου ώστε να χρησιμοποιείται στην τελευταία έκδοση
2. Ενεργοποίηση αυτοματοποιημένων ενημερώσεων ασφαλείας του λογισμικού περιήγησης στο διαδίκτυο και περιοδικός έλεγχος από τον υπεύθυνο ασφάλειας.
3. Εφαρμογή καταλόγων ελέγχου πρόσβασης (Access Control Lists) για την επιβολή χρήσης προγραμμάτων όπως οι φυλλομετρητές και τα προγράμματα ανάγνωσης ηλεκτρονικού ταχυδρομείου, με λογαριασμούς χρηστών που έχουν περιορισμένα δικαιώματα και όχι με λογαριασμούς που έχουν δικαιώματα υπερχρήστη.

- **Στάδιο 5ο - Installation:**

Μόλις ο υπάλληλος ανοίξει την μολυσμένη ιστοσελίδα τότε γίνεται αυτόματα εγκατάσταση του μολυσμένου κώδικα, που έχει ενσωματωθεί στον κώδικα της ιστοσελίδας. Στην συνέχεια με την εγκατάσταση του Remote Access Trojan έχουν πρόσβαση απομακρυσμένα στο σύστημα του υπολογιστή.

Λύση - Άμυνα του παίκτη

1. Ειδοποίηση ότι νέο πρόγραμμα εκτελέστηκε και δεν ήταν στην λίστα Whitelist (CAPEC 98 - Phishing) και εφαρμογή πολιτικής λίστας έμπιστων εφαρμογών που επιτρέπει την εκτέλεση μόνο εξουσιοδοτημένου λογισμικού.
2. Έλεγχος των υπολογιστών του δικτύου με εργαλεία εντοπισμού και προστασίας από κακόβουλο λογισμικό.
3. Έλεγχος των υπολογιστών του δικτύου με εργαλεία και μεθόδους που βασίζονται στις υπογραφές κακόβουλων αρχείων. Αυτοματοποιημένη ενημέρωση των υπογραφών αυτών των εργαλείων.

- **Στάδιο 6ο - Command and Control:**

Στο σημείο αυτό, με την εγκατάσταση του malware που έγινε στο προηγούμενο στάδιο δημιουργείται ένα αποκλειστικό κανάλι επικοινωνίας για την διαρκεί επικοινωνίας του συστήματος με τους χάκερς.

Λύση - Άμυνα του παίκτη

1. Έλεγχος της κίνησης στο εσωτερικό του δικτύου, με τη δημιουργία συστημάτων υπηρεσιών διαδικτύου που χρησιμοποιούν τείχη προστασίας και διαμεσολαβητές.
2. Παραχώρηση πρόσβασης επικοινωνίας μόνο σε εγκεκριμένες διευθύνσεις (Whitelist).
3. Απαγόρευση της peer-to-peer κίνησης (π.χ. Skype, Cisco Jabber κ.α.) για τυχόν παρεμπόδιση των σχεδίων του επιτιθέμενου ώστε να χρησιμοποιεί P2P υποδομή – bot master.

- **Στάδιο 7ο - Actions on objectives:**

  Στο τελικό στάδιο, οι χάκερς κλέβουν τον κώδικα των λογισμικών που φτιάχνει η εταιρεία σου. Στην συνέχεια, διακόπτουν την σύνδεση τους με το δίκτυο της εταιρείας σου. Η επίθεση τους έχει τελειώσει.

  Λύση - Άμυνα του παίκτη

  1. Προστασία δεδομένων για να εφαρμοστεί έλεγχος των δεδομένων με το File Integrity Monitoring (FIM), ώστε να ελέγχεται ποιος έχει πρόσβαση στα αρχεία και πότε
  2. Δημιουργία πλάνου για την τήρηση αντιγράφων ασφαλείας σε καθημερινή ή εβδομαδιαία βάση για την επαναφορά του συστήματος σε περίπτωση απώλειας δεδομένων.
  3. Ασφαλής αποθήκευση των αντιγράφων ασφαλείας.

Γ.4.3 Τρίτο εκπαιδευτικό σενάριο

Στάδιο 1 - Reconnaissance:

Οι χάκερς έχουν ως στόχο να ρίξουν την σελίδα e-banking της τράπεζας που δουλεύεις. Ανιχνεύουν για αδυναμίες στους εξυπηρετητές (hosts), με το εργαλείο NMAP σαρώνουν και χαρτογραφούν το δίκτυο ώστε να ανακαλύψουν hosts, λειτουργικά συστήματα και firewalls του δικτύου της τράπεζας. Χρησιμοποιούν tor ώστε οι διαχειριστές να μην μπορούν να ανακαλύψουν από που προέρχεται η κίνηση.

Άμυνα - λύση σταδίου:

1. Εφαρμογή πολιτικής τοπικού δικτύου που αποκλείει συγκεκριμένους τύπους κυκλοφορίας όπως είναι το Internet Control Message Protocol (ICMP)

2. Firewalls: Εγκατάσταση τείχου προστασίας (firewall) μπροστά από τους εξυπηρετητές του δικτύου για τον έλεγχο των πακέτων από και προς τον εξυπηρετητή.
3. Αποκλεισμός Tor κόμβων
4. Προγραμματισμένος έλεγχος θυρών (port scanning) στους εξυπηρετητές (servers) του συστήματος.
5. Εκπαίδευση των χρηστών σχετικά με τις τακτικές και τεχνικές που χρησιμοποιούν οι botmasters για να δημιουργήσουν το όπλο τους, για να αποτρέψουν την προσθήκη άλλων bots στον στρατό τους.

Στάδιο 2 - Weaponization:

Οι χάκερς ετοιμάζουν το malware τύπου bot που δημιουργείται για να εκτελέσει συγκεκριμένες διαδικασίες. Ενσωματώνουν τον κώδικα του bot μέσα σε μια εικόνα.

Άμυνα - λύση σταδίου:

1. Παρακολούθηση ομάδων συζητήσεων στο διαδίκτυο ή στο darknet για αιτήματα βοήθειας ή πληροφορίες σχετικά με τη δημιουργία ή την πρόσβαση σε botnets.
2. Βελτίωση των πρακτικών ασφαλείας που βοηθούν ώστε να μειώνονται πιθανές αδυναμίες που βρίσκονται διαθέσιμες και οι χάκερς μπορούν να στοχοποιήσουν.

Στάδιο 3ο - Delivery

Οι χάκερς μόλις ενσωματώσουν στο όπλο τον κακόβουλο κώδικα, παραδίδουν το μολυσμένο αρχείο με δύο τρόπους, πρώτα με καμπάνια spam που περιλαμβάνει το αρχείο και δεύτερον με μηνύματα phishing που παραδίδονται στα θύματα και αποτελούν links που τους ανακατευθύνουν στο μολυσμένο αρχείο.

Άμυνα - λύση σταδίου:

1. Ψηφιακές υπογραφές που αναγνωρίζουν κακόβουλο κώδικα και διακόπτουν την εγκατάσταση και εκτέλεση μολυσμένων αρχείων.
2. Απαγόρευση λήψης e-mail που προέρχονται από γνωστές μη έμπιστες διευθύνσεις IP (blacklisting).
3. Χρήση Sender Policy Framework ώστε να ελέγχεται αν οι IP διευθύνσεις των αποστολέων e-mail συμπίπτουν με τις IP διευθύνσεις που έχουν δηλωθεί στους DNS servers για τα domain του αποστολέα. Έτσι διενεργείται επαλήθευση του αποστολέα και μειώνονται τα πλαστά (spoofed) μηνύματα ηλεκτρονικού ταχυδρομείου.

Στάδιο 4ο - Exploitation:

Οι χάκερς εκτελούν την επίθεση με bots διότι έχουν ανακαλύψει διάφορες αδυναμίες στο σύστημα όπως, οι μη αποτελεσματικοί μέθοδοι ασφάλειας, τα μη ενημερωμένα λογισμικά και μη ασφαλές πρακτικές στον κώδικα του λογισμικού.

Άμυνα - λύση σταδίου:

1. Χρήση λογισμικών προστασίας από ιούς με ενημερωμένη βάση δεδομένων ψηφιακών υπογραφών των ιών
2. Εγκατάσταση εξειδικευμένου λογισμικού ασφαλείας στον διακομιστή, όπως το Host Based Security Systems (αναγνωρίζει και αποτρέπει την εγκατάσταση κακόβουλων πακέτων)
3. Ειδοποίηση στον διακομιστή για πολλά πακέτα και καταγραφή της κίνησης με τις IPs και τις χώρες που προέρχονται.

Στάδιο 5ο - Installation:

Μόλις ο υπάλληλος πατήσει το link ανοίγει την μολυσμένη εικόνα και γίνεται εγκατάσταση του μολυσμένου κώδικα στον υπολογιστή του υπαλλήλου. Στην

συνέχεια με την εγκατάσταση του bot έχουν πρόσβαση απομακρυσμένα στο σύστημα του υπολογιστή.

Άμυνα - Λύση σταδίου:

1. Εγκατάσταση εξειδικευμένου λογισμικού ασφαλείας στον διακομιστή όπως το Host Based Security Systems (αναγνωρίζει και αποτρέπει την εγκατάσταση κακόβουλων πακέτων)
2. Εφαρμογή πολιτικής “Λίστας έμπιστων εφαρμογών” Application whitelist που επιτρέπει την εκτέλεση μόνο εξουσιοδοτημένου λογισμικού

Στάδιο 6ο - Command and Control:

Μόλις γίνει εγκατάσταση του bot στο σύστημα, αυτό ελέγχεται από τον botmaster δηλαδή τους χάκερς. Στην συνέχεια τα bots κατεβάζουν την τελευταία έκδοση του ιού που επιθυμεί ο botmaster. Στην συνεχεία ο botmaster βρίσκεται μέσα στο σύστημα μέχρι να ανακαλύψουν οι διαχειριστές την παραβίαση.

Άμυνα - Λύση σταδίου:

1. Host Based Security Systems για την παρακολούθηση και πρόσβαση σε δεδομένα με κωδικοποιημένη μορφή.
2. Network Based Security Systems όπου παρακολουθούν την ροή κυκλοφορίας στο LAN ΚΑΙ WAN των δεδομένων και μετατρέπουν την πληροφορία για να αναγνωρίζουν μοτίβα.
3. Botminer πρωτόκολλο και ανεξάρτητο εργαλείο που αναγνωρίζει bots στο δίκτυο και εξακριβώνει την κακόβουλη δραστηριότητα.
4. Botswat το οποίο είναι εργαλείο host για αναγνώριση συμπεριφοράς.

Στάδιο 7 - Actions on Objectives:

Οι χάκερς μολύνουν τους υπόλοιπους υπολογιστές που βρίσκονται συνδεδεμένοι στο σύστημα και τους χρησιμοποιούν για botnets ώστε να στείλουν πακέτα στον κεντρικό server και ρίχνουν το σύστημα. Εκτελούν επίθεση Distributed Denial of Service με στόχο να ρίξουν τον κεντρικό server του e-banking. Έπειτα η τράπεζα χάνει την αξιοπιστία της και δημιουργεί πανικό στους πελάτες που δεν μπορούν να διεξάγουν τις συναλλαγές τους.

Άμυνα - Λύση σταδίου

1. Intrusion Prevention Systems (IPS) και packet filtering, για την αναγνώριση κακόβουλης κίνησης μέσω της ανάλυση κίνησης στο δίκτυο.
2. Εργαλείο Arbor Peakflow SP Threat Management System, το οποίο αναγνωρίζει και απομακρύνει επιθέσεις DDoS αφήνοντας την νόμιμη κίνηση πακέτων στο δίκτυο.
3. Αύξηση των πηγών στους servers, για να επιτρέπουν περισσότερη κίνηση

Γ.4.4 Τέταρτο εκπαιδευτικό σενάριο

- **Στάδιο 1ο - Reconnaissance:**

Οι χάκερς έχουν ως στόχο το υπουργείο οικονομικών που δουλεύεις. Ξεκινούν να ανακαλύπτουν πληροφορίες για την υπηρεσία με τακτικές επισκέψεις στα κεντρικά γραφεία της υπηρεσίας. Χρησιμοποιούν τις υπηρεσίες του υπουργείου όπως το σύστημα της εφορίας και προκαλούν εσκεμμένα σφάλματα ώστε να ανακαλύψουν αδυναμίες στο σύστημα. Στην συνέχεια, συλλέγουν πληροφορίες με ονόματα υπαλλήλων, διευθύνσεις e-mails, κοινά ενδιαφέροντα των υπαλλήλων, και ανιχνεύουν τι λογισμικά συστήματα χρησιμοποιούν οι υπάλληλοι στην υπηρεσία.

Λύση - Άμυνα του παίκτη

1. Εκπαίδευση προσωπικού σε θέματα ασφαλείας προσαρμοσμένη στις γνώσεις και δεξιότητες των υπαλλήλων και την θέση εργασίας, με στόχο την ευαισθητοποίηση σε θέματα ασφαλείας.
2. Εκπαίδευση των υπαλλήλων σε θέματα ασφάλειας μέσω της παρουσίασης και ανάλυσης πραγματικών περιστατικών ασφάλειας.
3. Έλεγχος των ενεργειών του συστήματος (και των πληροφοριών που προβάλλονται) από τις υπηρεσίες του συστήματος σε περίπτωση που προκαλείται κάποιο λάθος από τον χρήστη.

- **Στάδιο 2ο - Weaponization:**

Οι χάκερς ετοιμάζουν το όπλο για να εισβάλουν στο σύστημα της δημόσιας υπηρεσίας. Η επίθεση θα πραγματοποιηθεί με μολυσμένα usb sticks. Προσθέτουν στα usb sticks malware τύπου Trojan Horse (Δούρειος ίππος) με διάφορες αδυναμίες του λειτουργικού συστήματος που ανίχνευσαν. Πραγματοποιούν διαγνωστικά tests ώστε τα προγράμματα προστασίας ιών να μην ειδοποιούν για κινδύνους που φέρει το usb stick.

Λύση - Άμυνα του παίκτη

1. Εγκατάσταση Συστημάτων Διαχείρισης Περιστατικών και Ασφάλειας Πληροφοριών (Security Information and Event Management - SIEM) και Ανάλυσης Αρχείων Καταγραφής (Log Analysis System).
2. Βεβαίωση ότι όλοι οι κατάλογοι και τα αρχεία εκτελούνται με περιορισμένα προνόμια, ώστε να προστατεύονται από απομακρυσμένες εκτελέσεις.
3. Εφαρμογή: Ανίχνευση ιών με εξειδικευμένα προγράμματα ασφάλειας.

- **Στάδιο 3ο - Delivery:**

Οι χάκερς παραδίδουν τα μολυσμένα usb sticks με απλό τρόπο. Εισέρχονται στα κεντρικά γραφεία της δημόσιας υπηρεσίας και αφήνουν σε στρατηγικά σημεία διάφορες συσκευές usb. Έπειτα, περιμένουν κάποιον από τους υπαλλήλους που θα ανακαλύψει τις φορητές συσκευές και θα το συνδέσει στον υπολογιστή του.

Λύση - Άμυνα του παίκτη

1. Απενεργοποίηση των θυρών usb των υπολογιστών του δικτύου, όπου αυτές δεν είναι απαραίτητες.
2. Κλείδωμα θυρών πρόσβασης στους υπολογιστές των υπαλλήλων
3. Ρύθμιση όλων των συστημάτων ώστε να μην εκτελείται αυτόματα το περιεχόμενο από τα USB sticks ή τις φορητές συσκευές usb sticks
4. Σε περίπτωση απαραίτητης χρήσης usb sticks, το σύστημα πρέπει να αναγνωρίζει και να τις ταυτοποιεί, με βάση τον σειριακό αριθμό της συσκευής

Στάδιο 4ο - Exploitation:

Οι χάκερς εκμεταλλεύονται την περιέργεια των ανθρώπων, καθώς γνωρίζουν ότι αν κάποιος έχει στην κατοχή του usb stick τότε θα το συνδέσει στον υπολογιστή του για να ανακαλύψει σε ποιον ανήκει και να το επιστρέψει. Στην προκειμένη περίπτωση οι χάκερς εκμεταλλεύονται την έκδοση του λειτουργικού συστήματος των υπολογιστών της δημόσιας υπηρεσίας. Πρόκειται για την αδυναμία στην ασφάλεια των Windows 7 Professional 64 bit που εκτελεί απομακρυσμένο κώδικα.

Λύση - Άμυνα του παίκτη

1. Περιορισμός των προνομίων που έχουν οι λογαριασμοί χρηστών, ώστε οι αλλαγές να μη πραγματοποιούνται από εξουσιοδοτημένους χρήστες. (CAPEC 551 - Modify Existing Service).
2. Διενέργεια ασκήσεων εικονικής επίθεσης στο σύστημα της εταιρείας με στόχο να εντοπιστούν ευπάθειες που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι.
3. Ενεργοποίηση αυτοματοποιημένων ενημερώσεων ασφαλείας του λογισμικού και περιοδικός έλεγχος από τον υπεύθυνο ασφάλειας.

Στάδιο 5ο - Installation:

Με την εισαγωγή του usb stick στον υπολογιστή, η εγκατάσταση του εκτελέσιμου μολυσμένου αρχείου γίνεται ακαριαία. Οι χάκερς εγκαθιστούν Remote Access Trojan στο δίκτυο της δημόσιας υπηρεσίας.

Λύση - Άμυνα του παίκτη

1. Περιορισμό των προνομίων που έχουν οι λογαριασμοί χρηστών, ώστε όταν δημιουργηθεί μια νέα υπηρεσία ή αλλάξουν τις ρυθμίσεις, να εκτελείται μόνο από εξουσιοδοτημένους διαχειριστές[6].
2. Πολιτική ώστε να δημιουργούνται ζώνες ασφαλείας με αυστηρό έλεγχο δικαιωμάτων και να ελέγχεται η κίνηση μεταξύ των διάφορων ζωνών. (Μοντέλο zero - trust)
3. Ειδοποίηση ότι νέο πρόγραμμα εκτελέστηκε και δεν ήταν στην λίστα whitelist (CAPEC 98 - Phishing).

- **Στάδιο 6ο - Command and Control:**

Οι χάκερς, με την εγκατάσταση του malware που πραγματοποιήθηκε στο προηγούμενο στάδιο, δημιούργησαν ένα αποκλειστικό κανάλι επικοινωνίας για την συνεχή επικοινωνία με το σύστημα.

Λύση - Άμυνα του παίκτη

1. Κατάτμηση του δικτύου σε ανεξάρτητα υποδίκτυα με διαφορετικές ζώνες ασφαλείας. Χρήση του τοίχου προστασίας και των καταλόγων ελέγχου πρόσβασης (access control lists), για να γίνει εμποδίσουν τις κακόβουλες ενέργειες στο δίκτυο.
2. Redirect σε ύποπτες κινήσεις του δικτύου που τους ανακατευθύνουν σε τοπικές παγίδες και ανάλυση του συστήματος ιών (honeypot).
3. Τοποθέτηση των εξυπηρετητών του δικτύου (π.χ. DNS, διαμοιρασμός αρχείων, βάσεις δεδομένων, ηλεκτρονικό ταχυδρομείο) σε χωριστά συστήματα.

- **Στάδιο 7ο - Actions on Objectives**

Στο σημείο αυτό οι χάκερς έχουν φτάσει στον αρχικό τους στόχο. Με την εμβάθυνση μέσα στο σύστημα συλλέγουν δεδομένα των πολιτών, τα κρυπτογραφούν σε αρχείο RAR και μέσω FTP μεταφέρουν τα αρχεία. Στην συνέχεια, διαγραφούν πολλά δεδομένα πολιτών από το σύστημα, με αποτέλεσμα να δημιουργηθεί πανικός στο κράτος.

6 CAPEC 550 - Install new service, CAPEC 551 - Modify Existing Service

Λύση - Άμυνα του παίκτη

1. Ορισμός πολιτικής και δικαιωμάτων για να μεταφέρονται αρχεία σε ελεγχόμενα κανάλια ώστε τα δεδομένα να μεταφέρονται ασφαλή.
2. Η εξερχόμενη διαδικτυακή κίνηση αφορά τα πρωτόκολλα μεταφοράς αρχείων (FTP ή SFTP) θα πρέπει να γίνεται μέσω proxy.
3. Εντοπισμός και έλεγχος των εξερχόμενων συνδέσεων TCP, που έχουν μεγάλη διάρκεια και πιθανότατα εξάγουν κρυπτογραφημένα ή απλά δεδομένα. Δημιουργία αντιγράφων ασφαλείας των αρχείων σε ξεχωριστά συστήματα μη συνδεδεμένα στο Διαδίκτυο.

Γ.4.4 Πέμπτο εκπαιδευτικό σενάριο

- **Στάδιο 1ο - Reconnaissance:**

Οι χάκερς έχουν ως στόχο την ασφαλιστική εταιρεία που δουλεύεις. Ξεκινούν να ανιχνεύουν για πληροφορίες. Εισέρχονται στα κεντρικά γραφεία της εταιρείας ως πελάτες και ανιχνεύουν τον χώρο, τους υπολογιστές που χρησιμοποιούν οι υπάλληλοι και το διαθέσιμο δίκτυο που είναι συνδεδεμένοι. Παρατηρούν την μάρκα του router που βρίσκεται σε εμφανή σημείο και την έκδοση του και φωτογραφίζουν τους κωδικούς που αναγράφονται στην συσκευή. Φεύγοντας από τον χώρο παρατήρησαν ότι η εμβέλεια του δικτύου είναι σε απόσταση ενός χιλιομέτρου.

Λύση - Άμυνα του παίκτη

1. Εκπαίδευση προσωπικού σε θέματα ασφαλείας προσαρμοσμένη στις γνώσεις και δεξιότητες των υπαλλήλων και τη θέση εργασίας με στόχο την ευαισθητοποίηση σε θέματα ασφαλείας.
2. Εκπαίδευση των υπαλλήλων σε θέματα ασφάλειας μέσω της παρουσίασης και ανάλυσης πραγματικών περιστατικών ασφάλειας
3. Μικρή εμβέλεια του ασύρματου δικτύου της εταιρείας

- **Στάδιο 2ο - Weaponization:**

  Οι χάκερς γνωρίζουν την ακριβή μάρκα του router και ανακαλύπτουν αδυναμίες της συσκευής στο WPS πρωτόκολλο. Ο στόχος τους είναι να εισβάλουν στο ασύρματο δίκτυο της εταιρείας. Έτσι, εκτελούν την επίθεση Pixie Dust για το WPS του router.

Λύση - Άμυνα του παίκτη

1. Καταγραφή των κινήσεων των χρηστών και των συμβάντων του δικτύου σε αρχεία καταγραφής (log files). Ανάλυση αυτών των πληροφοριών και συσχέτιση των αρχείων καταγραφής που προέρχονται από διαφορετικές συσκευές του δικτύου
2. Έλεγχος των ρυθμίσεων των συσκευών (π.χ. Απενεργοποίηση της ρύθμισης WPS μέσα από το router)
3. Αντικατάσταση εξοπλισμού που δεν ακολουθεί τις κατάλληλες προδιαγραφές ασφάλειας.

- **Στάδιο 3ο - Delivery:**

Οι χάκερς λόγω της μεγάλης εμβέλειας του δικτύου εκτελούν την επίθεση από διπλανό κτήριο. Ο στόχος τους είναι να εισβάλουν στο ασύρματο δίκτυο και αυτό το καταφέρνουν εξαιτίας της μεγάλης εμβέλειας του ασύρματου δικτύου.

Λύση - Άμυνα του παίκτη

1. Μικρή εμβέλεια του ασύρματου δικτύου μόνο στους χώρους της εταιρείας.
2. Χρήση ισχυρών κωδικών για το ασύρματο δίκτυο
3. Έλεγχος ότι δεν χρησιμοποιούνται οι εξ' ορισμού κωδικοί και τακτική αλλαγή των κωδικών αυτών.

- **Στάδιο 4ο - Exploitation**

  Οι χάκερς ουσιαστικά εκμεταλλεύονται την αδυναμία του WPS της συσκευής και συνδέονται στο ασύρματο δίκτυο της εταιρείας εκτελώντας επίθεση στο πρωτόκολλο για να συνδεθούν στην συσκευή.

Λύση - Άμυνα του παίκτη

1. Απενεργοποίηση της ρύθμισης WPS μέσα από το router
2. Αν η συσκευή router είναι παλιά, το WPS απενεργοποιημένο, έλεγχο με ειδικό λογισμικό για τα δίκτυα με ενεργοποιημένο WPS (Wash Software). Αν το router εμφανιστεί στην λίστα, τότε αγορά καινούργιας συσκευής.
3. Χρήση ισχυρών κωδικών στο ασύρματο δίκτυο

🕐 **Στάδιο 5ο - Installation:**

Οι χάκερς μέσα στο δίκτυο της εταιρείας ανακαλύπτουν τους συνδεδεμένους υπολογιστές στο δίκτυο και εγκαθιστούν κακόβουλο λογισμικό τύπου Remote Access Trojan με αποτέλεσμα να έχουν πρόσβαση στα συστήματα των υπολογιστών.

Λύση - Άμυνα του παίκτη

1. Έλεγχος των υπολογιστών του δικτύου με εργαλεία και μεθόδους που βασίζονται στις υπογραφές κακόβουλων αρχείων. Αυτοματοποιημένη ενημέρωση των υπογραφών αυτών των εργαλείων.
2. Εφαρμογή πολιτικής “Λίστας έμπιστων εφαρμογών” Application Whitelist που επιτρέπει την εκτέλεση μόνο εξουσιοδοτημένου λογισμικού

· **Στάδιο 6ο - Command and Control:**

Οι χάκερς με την εγκατάσταση του malware που έγινε στο προηγούμενο στάδιο δημιουργούν ένα αποκλειστικό κανάλι επικοινωνίας για την συνεχή επικοινωνία του συστήματος με τους χάκερς.

Λύση - Άμυνα του παίκτη

1. Έλεγχος της κίνησης στο εσωτερικό του δικτύου, με τη δημιουργία συστημάτων υπηρεσιών διαδικτύου που χρησιμοποιούν τείχη προστασίας και διαμεσολαβητές.
2. Κατάτμηση του δικτύου σε ανεξάρτητα υποδίκτυα με διαφορετικά Trust Zones με χρήση του τοίχου προστασίας και καταλόγων ελέγχου

πρόσβασης (Access Control Lists) για να γίνει παρεμπόδιση των κακόβουλων ενεργειών σε όλο το δίκτυο.

- **Στάδιο 7ο - Actions on Objectives**

Στο σημείο αυτό οι χάκερς έχουν φτάσει στον αρχικό του στόχο. Με την διείσδυσή στο σύστημα συλλέγουν δεδομένα των πελατών. Στην συνέχεια τα κρυπτογραφούν σε αρχείο RAR και μέσω FTP τα μεταφέρουν. Στην συνέχεια, στο Dark Web δημοσιεύουν τις ασφάλειες μαζί με στοιχεία των πολιτών (ταυτότητα, ΑΦΜ) για πώληση.

Λύση - Άμυνα του παίκτη

1. Ορισμός πολιτικής και δικαιωμάτων για να μεταφέρονται αρχεία σε ελεγχόμενα κανάλια ώστε τα δεδομένα να μεταφέρονται ασφαλή.
2. Η εξερχόμενη διαδικτυακή κίνηση που αφορά τα πρωτόκολλα μεταφοράς αρχείων (FTP ή SFTP) θα πρέπει να γίνεται μέσω proxy.
3. Δημιουργία αντιγράφων ασφαλείας των αρχείων σε ξεχωριστά συστήματα μη συνδεδεμένα στο Διαδίκτυο.
4. Παρακολούθηση συζητήσεων στο dark web για ενημέρωση επιθέσεων

Γ.5 Πως παίζεται το παιχνίδι αναλυτικότερα

Μόλις ο παίκτης εισέλθει στο παιχνίδι υπάρχει πεδίο για να βάλει το όνομα χρήστη. Στην συνέχεια, φορτώνει μια νέα σελίδα στην οποία εισέρχεται ο παίκτης και του εμφανίζει το τραπέζι. Το παιχνίδι ψάχνει τους υπόλοιπους παίκτες για να ξεκινήσει το μοίρασμα των καρτών. Μόλις φορτωθούν οι υπόλοιποι τρεις παίκτες ξεκινάει το μοίρασμα των καρτών με τους μηχανισμούς άμυνας και το πρώτο στάδιο του σεναρίου που έχει επιλεχθεί για να λύσει ο κάθε παίκτης. Κάθε παιχνίδι αποτελείται από τέσσερις παίκτες.

Στο τραπέζι του παιχνιδιού υπάρχουν οι τέσσερις παίκτες στους οποίους ο χρήστης βλέπει τις εικόνες του. Σε κάθε παίκτη υπάρχει η ίδια εικόνα ως φωτογραφία προφίλ αλλά με διαφορετικό χρωματισμό. Τα σενάρια στο παιχνίδι είναι πέντε, κάθε σενάριο έχει επτά στάδια από το μοντέλο cyber kill chain και η λύση στις επιθέσεις είναι

μηχανισμοί άμυνας και διαρθρωτικά μέτρα από την μεθοδολογία CAPEC ώστε να αποτρέψουν ή να προφυλάξουν τον οργανισμό που οι παίκτες “εργάζονται” από τέτοιες επιθέσεις.

Στον πρώτο γύρο μοιράζονται στους παίκτες, το πρώτο στάδιο που έχουν να αντιμετωπίσουν, το σύστημα διαλέγει τυχαία το σενάριο που δίνει στους παίκτες. Οι παίκτες πρέπει να συνδυάσουν τις κάρτες που έχουν στα χέρια τους ή να σηκώσουν από την στοίβα με τους μηχανισμούς άμυνας μια καινούργια κάρτα ώστε να βρεθεί λύση στο στάδιο που αντιμετωπίζουν με τον κατάλληλο συνδυασμό καρτών.

Μόλις το παιχνίδι ξεκινάει, επιλέγεται και δίνεται σε κάθε παίκτη ένα από τα πέντε σενάρια, τα οποία ο παίκτης καλείται να λύσει, με σκοπό να ολοκληρώσει πρώτος την λύση όλων των σταδίων και να νικήσει το παιχνίδι. Σε κάθε στάδιο πριν ξεκινήσουν οι παίκτες, τους δίνονται επτά κάρτες από τους μηχανισμούς άμυνας μαζί με την κάρτα του σταδίου καθώς και την κάρτα με την επιπλέον βοήθεια που χρειάζεται ο παίκτης για να λύσει το πρόβλημα του.

Το παιχνίδι ξεκινάει, ο πρώτος παίκτης διαβάζει το πρόβλημα από το πρώτο στάδιο του σεναρίου που του δόθηκε και αναζητά την λύση. Αν ο παίκτης διαθέτει όλες τις κάρτες στο χέρι για να λύσει το στάδιο, τότε επιλέγει τις κάρτες που θεωρεί ότι είναι η σωστή λύση και πατάει το κουμπί λύση. Αν ο συνδυασμός είναι ο σωστός το σύστημα ενημερώνει τον παίκτη ότι πέρασε το πρώτο στάδιο. Στην συνέχεια, του δίνονται επτά καινούργιες κάρτες από τους μηχανισμούς άμυνας μαζί με την κάρτα από το στάδιο δύο, που καλείται να λύσει ο παίκτης. Κάθε φορά που έρχεται η σειρά του κάθε παίκτη πρέπει να πατήσει το κουμπί πάρε μια κάρτα και στην συνέχεια να πετάξει μια κάρτα, πατώντας το αντίστοιχο κουμπί δώσε μια κάρτα. Έτσι πάντα οι παίκτες θα έχουν στο χέρι τους επτά κάρτες. Μόλις ο παίκτης θεωρήσει ότι βρήκε την λύση στο δεύτερο στάδιο, επιλέγει τις κάρτες και πατάει το κουμπί λύση. Αν η λύση είναι σωστή τότε ενημερώνει τους παίκτες ότι ο συγκεκριμένος αντίπαλος πέρασε στο στάδιο 3, αλλιώς δεν επιτρέπει τον παίκτη να περάσει στο επόμενο στάδιο και η σειρά δίνεται στον επόμενο παίκτη. Στην συνέχεια, στο παράδειγμα του παιχνιδιού, ο παίκτης που πέρασε στο στάδιο 3 λαμβάνει επτά καινούργιες κάρτες από τους μηχανισμούς άμυνας μαζί με την κάρτα του προβλήματος από το στάδιο τρία. Αντίστοιχα, κάθε φορά που παίζει κάθε παίκτης πρέπει αναγκαστικά να παίρνει μια καινούργια κάρτα από τους μηχανισμούς άμυνας και να διώχνει μια κάρτα, που συνήθως δεν χρειάζεται, επιλέγοντας την κάρτα και πατώντας το κουμπί δώσε μια κάρτα.

Στην συνέχεια, ο παίκτης με τον ίδιο τρόπο λύνει τα υπόλοιπα στάδια μέχρι να φτάσει στο έβδομο στάδιο. Έστω, ότι στο τελευταίο στάδιο του παιχνιδιού βρίσκονται και οι τέσσερις παίκτες του παιχνιδιού. Σε κάθε παίκτη δίνονται επτά καινούργιες κάρτες από τους μηχανισμούς άμυνας καθώς και η κάρτα από το έβδομο στάδιο του κάθε σεναρίου που αντιμετωπίζουν. Στην συνέχεια, όταν έρχεται η σειρά των παικτών, λαμβάνουν μια κάρτα από τους μηχανισμούς άμυνας και στην συνέχεια ρίχνουν μια κάρτα που δεν τους χρειάζεται και κρατούν στο χέρι τους. Αν κάποιος από τους παίκτες αφού έχει λάβει την καινούργια κάρτα από τους μηχανισμούς άμυνας, βρει την λύση για το τελευταίο στάδιο, τότε πατώντας το κουμπί λύση, το σύστημα επαληθεύει την απάντηση του και ενημερώνει όλους τους παίκτες ότι βρέθηκε νικητής. Έπειτα, το παιχνίδι τερματίζεται και επιστρέφει τους παίκτες στην αρχική σελίδα του παιχνιδιού.

Ο σκοπός του παιχνιδιού είναι ένας από τους τέσσερις παίκτες να νικήσει πρώτος. Επίσης, είναι σημαντικό όλοι οι παίκτες να έχουν ολοκληρώσει τα προηγούμενα στάδια, καθώς αποτελούν αλυσίδα της επίθεσης που αντιμετωπίζουν. Στο συγκεκριμένο παιχνίδι υπάρχει περίπτωση οι παίκτες να βρίσκονται στο ίδιο στάδιο πολύ χρόνο, ο σκοπός είναι να σκέφτονται την κάθε λύση με μεθοδικότητα, αλλά και να διαβάζουν προσεκτικά το πρόβλημα που αντιμετωπίζουν. Το παιχνίδι έχει ως στόχο οι παίκτες να σκέφτονται τις απαντήσεις τους, ανάλογα με το πρόβλημα τους, ώστε οι απαντήσεις να μην δίνονται με μηχανικό τρόπο. Φυσικά κύριος σκοπός του παιχνιδιού είναι οι παίκτες να αφουγκραστούν τα στάδια της επίθεσης που τους δίνονται και να ψάξουν τον κατάλληλο συνδυασμό με τις κάρτες ώστε να βρεθούν οι λύσεις και τα διαρθρωτικά μέτρα για την μελλοντική αποφυγή του συγκεκριμένου τύπου επίθεσης. Τα στάδια έχουν παρθεί από σενάρια επιθέσεων και η λύση για το κάθε στάδιο είναι από την μεθοδολογία CAPEC. Με την ολοκλήρωση του παιχνιδιού οι παίκτες έχουν εκπαιδευτεί σε βασικές έννοιες για μοτίβα επιθέσεων και τρόπους αντιμετώπισης σε παρόμοιες μελλοντικές επιθέσεις σε συστήματα, εφαρμογές και δίκτυα.

Κάθε παίκτης έχει τριάντα δευτερόλεπτα για να απαντήσει στον γύρο του, εκτιμάται ότι ο χρόνος για να βρεθεί νικητής είναι εξήντα λεπτά. Αυτό βέβαια εξαρτάται από τις γνώσεις των παικτών στο κομμάτι της ασφάλειας και στα πιθανά στάδια της επίθεσης.

Το παιχνίδι είναι εκπαιδευτικής και ψυχαγωγικής φύσης. Ο κάθε παίκτης αντιμετωπίζει διαφορετικό στάδιο από τους συμπαίκτες τους. Ακόμη, υπάρχει ο καλός ανταγωνισμός ώστε οι παίκτες γρήγορα να απαντήσουν και να κατεβάσουν

την σωστή λύση για να ολοκληρώσουν το στάδιο που βρίσκονται και τελικά να φθάσουν στο τελευταίο στάδιο του σεναρίου, ώστε να ανακαλύψουν την λύση και να νικήσουν το παιχνίδι .

Γ.6 Τεχνολογίες που υπάρχουν στο παιχνίδι

Οι τεχνολογίες που χρησιμοποιήθηκαν είναι:

- Web sockets για τους παίκτες
- React JS
- JavaScript
- Node JS
- JQuery
- CSS
- HTML

Γ.7 Οι κανόνες του παιχνιδιού

1. Κάθε παίκτης λύνει από ένα σενάριο επίθεσης με επτά στάδια από το μοντέλο Cyber Kill Chain.
2. Ο πρώτος παίκτης που θα λύσει τα επτά στάδια- προβλήματα κερδίζει στο παιχνίδι.
3. Σε κάθε παίκτη μοιράζονται επτά κάρτες από μηχανισμούς άμυνας που θα συνδυάσουν αυτές τις κάρτες, για να βρεθεί άμυνα σε κάθε στάδιο.
4. Αν ο παίκτης δεν προλάβει στον γύρο που βρίσκεται να κατεβάσει την λύση του προβλήματος τότε παραμένει στο ίδιο στάδιο και κρατάει το πρόβλημα που αντιμετωπίζει .
5. Αν ο παίκτης κατεβάσει τον σωστό συνδυασμό τότε περνάει στο επόμενο στάδιο του σεναρίου.
6. Μόλις ο παίκτης που κατεβάσει την λύση του προβλήματος τότε νικάει το παιχνίδι.
7. Στην αρχή του παιχνιδιού δίνονται επτά κάρτες και την κάρτα από το πρώτο στάδιο της επίθεσης.
8. Στο παιχνίδι μπορούν να υπάρξουν μέχρι 4 παίκτες.
9. Η συνιστώμενη ώρα του παιχνιδιού είναι 60 λεπτά αλλά ο χρόνος είναι απεριόριστος

10. Το παιχνίδι μπορεί να παιχτεί από φοιτητές και επαγγελματίες με βασικές γνώσεις στην ασφάλεια υπολογιστών.
11. Το παιχνίδι αποτελείται από επτά στάδια και αποτελεί μέρος του βασικού σεναρίου που αντιμετωπίζει ο κάθε παίκτης.
12. Ο σκοπός του παιχνιδιού είναι εκπαιδευτικός και ο στόχος του είναι οι παίκτες να αναγνωρίζουν τα στάδια του Cyber Kill Chain από μια cyber επίθεση.
13. Οι παίκτες έχουν τα στάδια και αναζητούν την σωστή λύση σε επιθέσεις ασφάλειας, ώστε με τον κατάλληλο συνδυασμό καρτών να ανακαλύψουν την άμυνα για κάθε στάδιο της επίθεσης.
14. Αν ο παίκτης δεν περάσει στο επόμενο στάδιο τότε κρατάει την κάρτα με το στάδιο που του δόθηκε.
15. Αν ο παίκτης περάσει στο επόμενο στάδιο πετάει την κάρτα με το πρόβλημα και του δίνεται ένα καινούργιο, που πρέπει να ανακαλύψει τους τρόπους αντιμετώπισης για την άμυνα του.
16. Σε κάθε γύρο ο παίκτης πετάει αναγκαστικά μόνο μία κάρτα όταν έρθει η σειρά του και μπορεί να κατεβάσει την λύση τότε.

Κεφάλαιο Δ

Εκπαιδευτική μεθοδολογία στα παιχνίδια με κάρτες

Δ.1 Μεθοδολογία επτά βημάτων για σχεδίαση παιχνιδιού καρτών

Τα παιχνίδια με κάρτες έχουν ως στόχο οι παίκτες να δημιουργούν διάφορους συνδυασμούς με κάρτες, λαμβάνοντας υπόψη συγκεκριμένα κριτήρια που τους δίνονται. Υπάρχουν διάφοροι τρόποι για να δημιουργηθούν παιχνίδια με κάρτες μερικοί από αυτές είναι η διαλογή διαφόρων καρτών, η ομαδοποίηση καρτών, η σύγκριση και η αντιστοίχιση καρτών.

Για την ανάπτυξη παιχνιδιών με κάρτες έχουν αναπτυχθεί διάφορες μεθοδολογίες, στην συγκεκριμένη διπλωματική εργασία χρησιμοποιήθηκε η μεθοδολογία επτά βημάτων της Κορδάκη, για την σχεδίαση του εκπαιδευτικού παιχνιδιού defender. Η μεθοδολογία επτά βημάτων λαμβάνει υπόψη τις κοινωνικές και σύγχρονες όψεις που έχει η εκπαίδευση.

Τα παιχνίδια με κάρτες αποτελούν ένα ακόμη τρόπο για ουσιαστική εκπαίδευση (Kamii and Devries 1980). Βοηθούν τους μαθητές να αναπτύξουν και να βελτιώσουν διάφορες βασικές γνώσεις στο μαθησιακό αντικείμενο προκειμένου να τους εισάγει σε νέες ορολογίες ανάλογα με το διδακτικό αντικείμενο του παιχνιδιού (Gardinger, 1987).

Κατά την διάρκεια του παιχνιδιού, όσο αυτό ξεκινάει να γίνεται απαιτητικό, οι παίκτες εφαρμόζουν όλες τις γνώσεις που έχουν διδαχτεί, αυτό έχει ως αποτέλεσμα να οργανώνουν τις κάρτες τους με συγκεκριμένες στρατηγικές για να κερδίσουν το παιχνίδι.

Τα παιχνίδια σοβαρού σκοπού με κάρτες οφείλουν να παρέχουν δυνατά εκπαιδευτικά εργαλεία με τον κατάλληλο σχεδιασμό ώστε να υποστηρίζουν την εκπαίδευση μέσα σε όρους (Oblinger, 2004).

Τα παιχνίδια σοβαρού σκοπού με κάρτες οφείλουν να προσφέρουν στους μαθητές:

1. Ενεργή και πειραματική εκπαίδευση.
2. Ενεργοποίηση και χρήση των εκ των προτέρων γνώσεων με σκοπό να αυξήσουν τις γνώσεις των μαθητών
3. Αυτό-διόρθωση από τον εκπαιδευτικό με την παροχή άμεσης ανταπόκρισης στους μαθητές παρατηρώντας τις αντιδράσεις τους στο παιχνίδι.
4. Αυτό-αξιολόγηση με τη αξιοποίηση μηχανισμών βαθμολόγησης

5. Οι παίκτες με τα παιχνίδια αποκτούν λογική και κριτική σκέψη καθώς ικανότητα επίλυσης προβλημάτων (Mcflarane, 2002).
6. Κίνητρα που βασίζονται στην αλληλεπίδραση με τον υπολογιστή.

Η μεθοδολογία επτά βημάτων για τον σχεδιασμό και την ανάπτυξη εκπαιδευτικών παιχνιδιών περιλαμβάνει (Maria Kordaki, 2010):

- Τον ορισμό του μαθησιακού μοντέλου και του μοντέλου των μαθητών. •
  Τον ορισμό των στόχων του παιχνιδιού με κάρτες .
- Τον ορισμό των κατάλληλων μαθησιακών δραστηριοτήτων για το παιχνίδι με κάρτες.
- Τον ορισμό συγκεκριμένων δραστηριοτήτων για το παιχνίδι, ώστε να βοηθήσει τους παίκτες να ξεπεράσουν οποιοσδήποτε μαθησιακές δυσκολίες αντιμετωπίζουν
- Τα κίνητρα που πρέπει το παιχνίδι να παρέχει στους μαθητές κατά την διάρκεια του παιχνιδιού.
- Τον ορισμό των κανόνων του παιχνιδιού.

Ωστόσο τα παιχνίδια με κάρτες πρέπει να δίνουν στους παίκτες κίνητρα για να συνεχίσουν να παίζουν το παιχνίδι. Τα κίνητρα αυτά είναι η πρόκληση, η περιέργεια, ο έλεγχος, η φαντασία, ο διαγωνισμός, η συνεργασία και η αναγνώριση (Maria Kordaki, 2010).

Βέβαια, τα παιχνίδια μπορούν να αναπτύξουν διάφορες ικανότητες των μαθητών όπως:

1. Στρατηγική σκέψη
2. Σχεδιασμός
3. Επικοινωνία
4. Μεγάλος αριθμός εφαρμογών
5. Ικανότητες για διαπραγμάτευση
6. Ομαδικές αποφάσεις
7. Διαχείριση δεδομένων

Έρευνες έχουν δείξει ότι τα παιχνίδια σοβαρού σκοπού έχουν θετικό ρόλο στην εκπαίδευση των μαθητών για ένα συγκεκριμένο μαθησιακό αντικείμενο . Ακόμη, τα παιχνίδια σοβαρού σκοπού παρέχουν σημαντικές επιδράσεις στις γνώσεις των μαθητών αλλά και των ενηλίκων σε συγκεκριμένους τομείς. Τα παιχνίδια σοβαρού σκοπού χρησιμοποιούνται στην επιστήμη, τα μαθηματικά, την γλώσσα και στην πληροφορική (Rajavivarma, 2005).

Δ.2 Αρχές για τον σχεδιασμό παιχνιδιών με κάρτες

Ο εκπαιδευτικός για τον σχεδιασμό του παιχνιδιού με κάρτες οφείλει να λάβει υπόψη του διάφορα χαρακτηριστικά όπως:

1. **Περιεχόμενο:**

   Γενικά τα παιχνίδια με κάρτες οφείλουν να δίνουν έμφαση στο περιεχόμενο για να παρακινήσουν τους μαθητές και τους εκπαιδευόμενους. Τα παιχνίδια ως πρωταρχικό στόχο έχουν την διασκέδαση των μαθητών (Prensky, 2001 p.179). Ειδικότερα, τα παιχνίδια πρέπει να είναι διασκεδαστικά και οι χρήστες που παίζουν, να βλέπουν τον εαυτό τους ως παίκτη και όχι ως μαθητευόμενο, με σκοπό να συνεχιστεί η επιθυμία για παιχνίδι. Όμως, ο στόχος των παιχνιδιών είναι να αυξάνονται οι γνώσεις τους στο μαθησιακό αντικείμενο, ανεξαρτήτως των αρχικών τους γνώσεων και ικανοτήτων. (Maria Kordaki, 2010).

2. **Ενεργή και εποικοδομητική συμμετοχή:**

   Οι μαθητές μέσω του παιχνιδιού μαθαίνουν καινούργιες γνώσεις στον τομέα που ειδικεύεται το παιχνίδι. Επομένως, οι μαθητές που παίζουν χρησιμοποιούν τις βασικές γνώσεις έχουν. Επιπλέον, στους μαθητευόμενους παρέχονται νέες ευκαιρίες για να χρησιμοποιήσουν τις παλιότερες γνώσεις τους προκειμένου να τις αυξήσουν.

3. **Επιπλέον βοηθήματα (Scaffolding):**

   Στην διαδικασία δημιουργίας ενός εκπαιδευτικού παιχνιδιού είναι σημαντικό να υπάρχουν κουμπιά για βοήθεια (Fisch, 2005). Ο ρόλος του καθηγητή στην επιπλέον βοήθεια παραμένει σημαντικός και μπορεί να εφαρμοστεί με διάφορους διδακτικούς τρόπος όπως είναι οι ερωταπαντήσεις των μαθητών στον καθηγητή και οι επεξηγήσεις για το παιχνίδι (Hays, 2005).

4. **Περιεχόμενο:**

   Το εκπαιδευτικό περιεχόμενο του παιχνιδιού πρέπει να σχετίζεται με την ηλικία των μαθητών που λαμβάνουν μέρος στο παιχνίδι (Fisch, 2005). Όταν οι παίκτες παίζουν το παιχνίδι, σκοπός είναι να ενεργοποιείται η κριτική σκέψη. Επίσης, το παιχνίδι οφείλει να ακολουθεί το εκπαιδευτικό περιεχόμενο του μαθήματος ώστε ο μαθητής να διδάσκεται ή να εξασκεί τις γνώσεις του μέσα από το παιχνίδι (Fabricature, 2000 p.15).

5. **Δομή:**

   Μερικές φορές η δομή δεσμεύει παίκτες να συνεχίσουν να παίζουν παρά το περιεχόμενο του. Επομένως, τα παιχνίδια οφείλουν να ακολουθούν την εξής δομή (Maria Kordaki, 2010):

- Παιχνίδι
- Κανόνες
- Στόχοι
- Αλληλεπίδραση
- Εξωτερικές επιδράσεις
- Νίκη
- Ανταγωνισμός
- Διαγωνισμός
- Αντίθεση

Για την κατασκευή του παιχνιδιού ο εκπαιδευτικός οφείλει να παρέχει μια ελκυστική και πρωτότυπη ιστορία με σκοπό να διασκεδάσεις τους μαθητές και να κρατήσει το ενδιαφέρον τους. Οι μαθητές κατά την διάρκεια του παιχνιδιού βρίσκονται σε ανταγωνισμό με τους συμπαίκτες τους. Τα παιχνίδια με κάρτες πρέπει να παρέχουν ενεργή συμμετοχή στο παιχνίδι και επιπλέον βοηθήματα για να πετύχουν τον εκπαιδευτικό στόχο τους. Το περιεχόμενο πρέπει να βρίσκεται στο κέντρο του εκπαιδευτικού παιχνιδιού προκειμένου το παιχνίδι να εκπαιδεύει τους παίκτες. Τέλος, κατά την διάρκεια σχεδίασης του παιχνιδιού ο εκπαιδευτικός πρέπει να ορίσει συγκεκριμένη δομή για να παρέχει στους μαθητές τις θεμελιώσεις πτυχές του μαθησιακού αντικειμένου (Maria Kordaki, 2010).

.3 Ανάλυση μεθοδολογίας επτά βημάτων

Η μεθοδολογία επτά βημάτων αποτελεί ένα σημαντικό εκπαιδευτικό εργαλείο, για την εκπαίδευση των μαθητών σε διάφορα θέματα και την εφαρμογή αυτών των βημάτων στον σχεδιασμό παιχνιδιών με κάρτες. Επίσης παρέχει μια δομημένη ανάλυση για τον σχεδιασμό εκπαιδευτικών παιχνιδιών με κάρτες. Σημαντικό στην εκπαίδευση μέσω ενός παιχνιδιού καρτών είναι το μαθησιακό αντικείμενο που περνάει ενεργητικά στους μαθητές με σκοπό να συμμετέχουν ενεργά μέσα στο παιχνίδι, έτσι ώστε να δέχονται την πληροφορία με ενεργητικό τρόπο και όχι με παθητικό (Maria Kordaki pp.2, 2010).

Ο σχεδιασμός των παιχνιδιών με κάρτες είναι ιδιαίτερα σημαντικός διότι παρέχει στους μαθητές διάφορα κίνητρα προκειμένου να συνεχίσουν να παίζουν το παιχνίδι. Το παιχνίδι μέσω της νίκης ή της ήττας κρατάει το ενδιαφέρον στους μαθητές. Τα εκπαιδευτικά παιχνίδια με κάρτες στην διάρκεια της σχεδίασης χρησιμοποιούν διάφορες τεχνικές εκπαίδευσης με καινοτόμους τρόπους προκειμένου να δημιουργήσουν ενδιαφέρον στους μαθητές (Maria Kordaki, pp.3, 2010).

Τα παιχνίδια αναπτύσσουν ικανότητες όπως η στρατηγική σκέψη, η οργάνωση, η επικοινωνία, οι μαθηματικές πράξεις, οι ικανότητες διαπραγμάτευσης, οι ομαδικές

αποφάσεις και ο χειρισμός διαφόρων δεδομένων. Βέβαια τα εκπαιδευτικά παιχνίδια αναπτύσσουν και άλλες ικανότητες όπως κοινωνικές και συναισθηματικές. (Maria Kordaki, pp.3, 2010)

Βήμα 1ο: Ορισμός μαθησιακού μοντέλου αντικειμένου και μοντέλο μαθητών

Το μαθησιακό μοντέλο αποτελεί τις βασικές έννοιες για το μοντέλο εκπαίδευσης με την προϋπόθεση ότι οι μαθητές θα εκπαιδευτούν πάνω σε αυτό μέσα από το εκπαιδευτικό παιχνίδι με κάρτες. Οι μαθητές μέσα από το παιχνίδι πρέπει να κατανοήσουν τις εκπαιδευτικές έννοιες (Maria Kordaki, pp. 114-123, 2016).

Το μοντέλο μαθητών περιλαμβάνει τις μη επιστημονικές αντιλήψεις των μαθητών για το εκπαιδευτικό περιεχόμενο και μπορούν να ξεπεραστούν μέσω της εκπαιδευτικής ικανότητας που τους παρέχει το εκπαιδευτικό παιχνίδι.

Βήμα 2ο: Ο ορισμός των στόχων για το παιχνίδι σοβαρού σκοπού με κάρτες

Σαφής ορισμός των στόχων του παιχνιδιού βάση του μαθησιακού μοντέλου.

Βήμα 3ο: Ο ορισμός των εκπαιδευτικών δραστηριοτήτων για τα παιχνίδια με κάρτες

Οι εκπαιδευτικές δραστηριότητες αποτελούν τα κίνητρα των μαθητών μέσα από την χρήση κατάλληλων μηχανισμών βαθμολόγησης των μαθητών και την δυνατότητα ανταγωνισμού. Επίσης, τα εκπαιδευτικά παιχνίδια πρέπει να λαμβάνουν υπόψη και το επίπεδο των μαθητών. Ακόμη, πρέπει να λαμβάνουν υπόψη τους και να ταξινομούν τις δραστηριότητες με την χρήση κατάλληλων ερωτήσεων για να αναπτύξουν την κριτική σκέψη των μαθητών (Maria Kordaki, pp. 114-123, 2016).

Τα εκπαιδευτικά παιχνίδια με κάρτες πρέπει να εστιάζουν στο επίπεδο δυσκολίας του μαθησιακού αντικειμένου που πρέπει να αλλάζει από στάδιο σε στάδιο προκειμένου οι παίκτες να κατανοούν το εκπαιδευτικό αντικείμενο. Με αυτό τον τρόπο οι μαθητές ξεπερνούν σημαντικές μαθησιακές δυσκολίες στο εκπαιδευτικό αντικείμενο (Maria Kordaki, pp. 114-123, 2016).

Για να το επιτύχει αυτό ο εκπαιδευτικός πρέπει να ακολουθήσει διάφορες προσεγγίσεις στο παιχνίδι όπως οι μαθητές να αντιστοιχούν παρόμοιες κάρτες ή να απορρίπτουν κάρτες που δεν τους χρησιμεύουν.

Βήμα 4ο: Ο ορισμός συγκεκριμένων δραστηριοτήτων στο παιχνίδι με σκοπό οι μαθητές να ξεπεράσουν τις δυσκολίες τους.

Σε αυτό το στάδιο, ο εκπαιδευτικός σχεδιάζει το παιχνίδι με τέτοιο τρόπο ώστε οι μαθητές να ξεπεράσουν τις μαθησιακές τους δυσκολίες (Maria Kordaki, pp. 114-123, 2016).

Βήμα 5ο: Ο ορισμός παροχής των κινήτρων που πρέπει να δίνεται στους μαθητές κατά την διάρκεια του παιχνιδιού.

Στην διάρκεια σχεδιασμού των καρτών οι εκπαιδευτικοί πρέπει να χρησιμοποιούν πάνω στις κάρτες εικόνες έτσι ώστε οι παίκτες να γνωρίζουν την κατηγορία της κάθε κάρτας που αντιπροσωπεύει (Maria Kordaki, pp. 114-123, 2016). Επίσης, ο εκπαιδευτικός πρέπει να σχεδιάσεις κάρτες Τζόκερ για να αυξήσει τα κίνητρα στους παίκτες όταν τυχαίνουν τις συγκεκριμένες κάρτες. Άλλο ένα κίνητρο είναι ο σχεδιασμός κατάλληλων μηχανισμών για την βαθμολογία στο παιχνίδι. Το συγκεκριμένο κίνητρο αποτελεί σημαντικό παράγοντα προκειμένου ο εκπαιδευτικός να κρατήσει το ενδιαφέρον των μαθητών κατά την διάρκεια του παιχνιδιού, αυξάνοντας το αίσθημα της . Ακόμη, οι σχεδιαστές πρέπει να χρησιμοποιούν bonus κάρτες έτσι ώστε όταν ο παίκτης τύχη τις συγκεκριμένες κάρτες, το παιχνίδι να τον επιβραβεύει με περισσότερους πόντους (Maria Kordaki, pp. 114-123, 2016).

Βήμα 6ο: Ο ορισμός του είδος των βοηθημάτων κατά την διάρκεια του παιχνιδιού με κάρτες

Το συγκεκριμένο βήμα αποτελεί τις βοηθητικές κάρτες που παρέχονται στους μαθητές με σκοπό να καλυφθούν χρήσιμες εκπαιδευτικές πληροφορίες για το μαθησιακό αντικείμενο (Maria Kordaki, pp. 114-123, 2016). Επίσης, οι συμβουλές και οι υποδείξεις του εκπαιδευτικού κατά την διάρκεια του παιχνιδιού είναι σημαντικές προκειμένου να βοηθήσει τους παίκτες να κατανοήσουν το μαθησιακό αντικείμενο και να λύσουν τα προβλήματα του παιχνιδιού.

Βήμα 7ο: Ο ορισμός των κανόνων του παιχνιδιού για το παιχνίδι με τις κάρτες

Ένα ακόμη σημαντικό βήμα για τον ορισμό της κατάλληλης στρατηγικής στο παιχνίδι με τις κάρτες είναι ο ορισμός των κανόνων και των στόχων στο παιχνίδι . Επίσης, οι εξωτερικοί παράγοντες και οι διαγωνισμοί για το ποιος θα βγει νικητής στο παιχνίδι αυξάνουν την αλληλεπίδραση των παικτών μεταξύ τους.

Κάθε παίκτης μέσω των παιχνιδιών καρτών εξελίσσει τις ικανότητες του στην στρατηγική σκέψη, τον σχεδιασμό, την λήψη αποφάσεων, την ομαδοποίηση, την σύγκριση, την κατάταξη, τις ικανότητες να ταιριάζει κάρτες για την λύση προβλημάτων και την ικανότητα να αντιμετωπίζει διάφορα σενάρια.

Σύμφωνα με την ιεραρχία Bloom οι παίκτες πρέπει να κατανοούν την ιδέα του παιχνιδιού ώστε να βρίσκονται σε θέση να αναγνωρίζουν τι θα συμβεί παρακάτω, ή να αντιμετωπίζουν τις κινήσεις των άλλων παικτών (Maria Kordaki, pp. 114-123,

2016). Έπειτα, όσο το παιχνίδι εξελίσσεται πρέπει να είναι σε θέση να εφαρμόσουν την γνώση που έλαβαν μέσα στο παιχνίδι . (Maria Kordaki, pp.3, 2010).

Δ.4 Εφαρμογή της μεθοδολογίας επτά βημάτων για την σχεδίαση του παιχνιδιού “Defender”

Το παιχνίδι έχει ως σκοπό να ψυχαγωγήσει και ταυτόχρονα να εκπαιδεύσει τους μαθητές σε σενάρια επιθέσεων από κακόβουλους χάκερς στο πλαίσιο του κυβερνοπόλεμου που συμβαίνει. Κάθε παίκτης είναι αμυνόμενος σε κάθε στάδιο της επίθεσης, και εφαρμόζει την μεθοδολογία cyber kill chain, ώστε οι μαθητές να αντιμετωπίζουν βασικά σενάρια επίθεσης στην κεβερνοασφάλεια και βασικούς τρόπους άμυνας σε αυτές τις επιθέσεις. Ο σκοπός είναι να συνδυάσουν τις κάρτες σωστά ώστε να δώσουν διαρθρωτικές λύσεις στο κάθε στάδιο της επίθεσης.
Στην συνέχεια αναλύονται τα βήματα της μεθοδολογίας επτά βημάτων για την σχεδίαση του εκπαιδευτικού παιχνιδιού.

Βήμα 1ο

Το πρώτο βήμα είναι ο ορισμός του μαθησιακού μοντέλου και το μοντέλο του εκπαιδευόμενου. Η βασική ιδέα είναι να περιγράφει το εκπαιδευτικό μοντέλο και η βασική μορφή του εκπαιδευτικού παιχνιδιού. Όπως επίσης και τα βασικά κομβικά στοιχεία που πρέπει να διδαχτούν οι μαθητές προκειμένου να κατανοήσουν το μαθησιακό περιεχόμενο. Το μαθησιακό μοντέλο δίνεται στους παίκτες μέσα από την βασική θεωρία του cyber kill chain που καλούνται να διαβάσουν πριν ξεκινήσουν να παίζουν. Αυτό βοηθάει τους παίκτες προκειμένου να κατανοήσουν τα βασικά στοιχεία της συγκεκριμένης μεθοδολογίας. Το παιχνίδι αναφέρεται για φοιτητές πανεπιστημίου στην Πληροφορική. Το μαθησιακό μοντέλο που εκπαιδεύονται είναι η Κυβερνοασφάλεια, βασικές αρχές στην ασφάλεια, τεχνικές άμυνας και το μοντέλο cyber kill chain. Το subject matter model σύμφωνα με την μεθοδολογία επτά βημάτων της Κορδάκη είναι το μοντέλο cyber kill chain και η Κυβερνοασφάλεια. Ενώ, το learner model είναι βασικές γνώσεις του παίκτη για να ανταπεξέλθει στο παιχνίδι.
Ο παίκτης πρέπει να γνωρίζει βασικές γνώσεις ασφάλειας υπολογιστών. Γενικά, σκοπός του παιχνιδιού είναι οι παίκτες να αναγνωρίζουν μοντέλα επιθέσεων για να τους διευκολύνει ώστε να βρίσκουν τρόπους άμυνας σε αυτά.

Βήμα 2ο

Το δεύτερο βήμα αποτελεί τον ορισμό των στόχων του παιχνιδιού. Ουσιαστικά οι στόχοι πρέπει να είναι βασισμένοι στο μαθησιακό μοντέλο και το μοντέλο του εκπαιδευόμενου. Βασικός στόχος του παιχνιδιού είναι οι φοιτητές να αναγνωρίζουν βασικούς τύπους επιθέσεων με βάση το μοντέλο cyber kill chain και ανάλογα να αντιμετωπίζουν το κάθε στάδιο της επίθεσης που βρίσκονται δίνοντας τρόπους άμυνας.

Βήμα 3ο

Στο τρίτο βήμα είναι ο ορισμός των κατάλληλων δραστηριοτήτων που πρέπει να περιλαμβάνουν την εκπαιδευτική στρατηγική στο παιχνίδι. Η εκπαιδευτική στρατηγική είναι τα ενδιαφέροντα των μαθητών, ο ανταγωνισμός για την ανάδειξη του νικητή, η χρονική διάρκεια στο παιχνίδι, οι γνώσεις των μαθητών και οι ερωτήσεις που στοχεύουν στην ανάπτυξη της κριτικής σκέψης. Για την βοήθεια των φοιτητών είναι σημαντικό να μάθουν το εκπαιδευτικό αντικείμενο και να υπάρχουν διάφορες εξωτερικές δραστηριότητες που τους παρέχει το παιχνίδι. Μια τέτοια δραστηριότητα είναι να δημιουργούν μόνοι τους διάφορα εκπαιδευτικά σενάρια παρόμοια με αυτά του παιχνιδιού προκειμένου να εφαρμόζουν το cyber kill chain για κάθε στάδιο. Επίσης, μπορούν να ανατρέξουν στην λίστα CAPEC με τα μοτίβα επιθέσεων και να αναζητήσουν τις λύσεις για κάθε στάδιο του σεναρίου τους. Κάθε κάρτα έχει σχεδιαστεί ώστε να ταιριάζει με την άμυνα σε κάθε στάδιο.

Βήμα 4ο

Το τέταρτο βήμα αποτελεί τον ορισμό συγκεκριμένων δραστηριοτήτων για να βοηθήσει τους μαθητές να ξεπεράσουν τις μαθησιακές τους δυσκολίες. Σε αυτό το βήμα είναι σημαντικό να σχεδιαστεί ένας αριθμός καρτών που βασίζεται σε δραστηριότητες προκειμένου να βοηθήσουν να ξεπεράσουν τις μαθησιακές τους δυσκολίες. Το παιχνίδι είναι μια εισαγωγή στην Κυβερνοασφάλεια και σε διάφορες επιθέσεις που οι μαθητές αντιμετωπίζουν μέσα από τα διάφορα σενάρια επιθέσεων. Έτσι, οι μαθητές εκπαιδεύονται πάνω σε διάφορους τρόπους που μπορεί να εκτελεστεί μια επίθεση αλλά και τρόπους αντιμετώπισης που οι ίδιοι πρέπει να δώσουν.

Ουσιαστικά σε αυτό το βήμα ο στόχος είναι στο παιχνίδι να παρέχεται ένα είδος βοήθειας. Για να αντιμετωπίσουν αυτές τις δυσκολίες, σε κάθε στάδιο αναλύεται η

θεωρία του cyber kill chain. Επιπλέον, σε κάθε κάρτα λύση υπάρχει εκπαιδευτική διευκρίνιση που βοηθάει τους παίκτες να κατανοήσουν την άμυνα της συγκεκριμένης κάρτας που διαβάζουν. Ακόμη, στις περισσότερες κάρτες που ο εκπαιδευτικός όρισε ως δύσκολες, αναλύεται σε πιο στάδιο αναφέρεται η άμυνα της συγκεκριμένης κάρτας με αποτέλεσμα οι παίκτες να αποκλείουν τις κάρτες που δεν είναι οι σωστές.

Βήμα 5ο

Στο πέμπτο βήμα είναι ο ορισμός από τα κίνητρα που πρέπει να δοθούν στους μαθητές κατά την διάρκεια του παιχνιδιού. Σε αυτό το βήμα πρέπει να δοθεί ένας είδος κινήτρου στους μαθητές για να συνεχίσουν να παίζουν. Ένας τρόπος είναι με τον σχεδιασμό κατάλληλων καρτών που θα κάνουν τους μαθητές να ευχαριστιούνται το παιχνίδι. Άλλο ένα σημείο είναι η βαθμολογία των καρτών, για να δώσουν ένα έξτρα κίνητρο στους μαθητές.
Τα κίνητρα για να συνεχίσουν να παίζουν οι παίκτες είναι τα διαφορετικά σενάρια μαζί με τον οργανισμό που προστατεύει ο κάθε παίκτης. Μερικά σενάρια αποτελούν αληθινά περιστατικά με διάφορες τροποποιήσεις . Επίσης, για να κρατηθεί το ενδιαφέρον στους παίκτες, σε κάθε κάρτα ανάλογα με το στάδιο που αναφέρεται η επίθεση υπάρχει συγκεκριμένο εικονίδιο. Το εικονίδιο αυτό κατηγοριοποιείται ανάλογα με τις λύσεις. Έτσι, οι παίκτες μειώνουν τις απαντήσεις τους ανάλογα με την εικόνα που υπάρχει σε κάθε στάδιο.

Βήμα 6ο

Το έκτο βήμα είναι ο ορισμός του είδους των τεχνικών οδηγιών που θα χρησιμοποιηθούν στο παιχνίδι. Ένας αριθμός καρτών που θα δίνει στους μαθητές ένα είδος από οδηγίες για την λύση του κάθε προβλήματος - σεναρίου αλλά και λυμένες αναπαραστάσεις . Στο παιχνίδι υπάρχει το κείμενο της θεωρίας που δίνεται σε κάθε παίκτη ανάλογα με το στάδιο που αντιμετωπίζουν εκείνη την συγκεκριμένη στιγμή. Επίσης, κάθε κάρτα λύσης έχει την εκπαιδευτική επεξήγηση της ώστε οι παίκτες να κατανοούν την άμυνα και να διδάσκονται περισσότερες πληροφορίες για την συγκεκριμένη λύση.

Βήμα 7ο

Το έβδομο βήμα περιλαμβάνει τους κανόνες του παιχνιδιού. Κάθε παίκτης αλληλεπιδρά με τους υπόλοιπους συμπαίκτες του μέσω της συνομιλίας που μπορούν να επικοινωνήσουν μεταξύ τους. Επίσης, οι παίκτες για να νικήσουν το

παιχνίδι πρέπει να παίξουν με ένα είδος στρατηγικής προκειμένου να διώχνουν κάρτες από τις λύσεις που απευθύνονται σε στάδια που δεν τους ενδιαφέρουν. Η πρόκληση στους παίκτες είναι ο χρόνος σε συνδυασμό με τον ανταγωνισμό των άλλων παικτών καθώς μέσα σε τριάντα δευτερόλεπτα πρέπει να ολοκληρώσουν το στάδιο που βρίσκονται αλλιώς παραμένουν στο ίδιο στάδιο.

Κεφάλαιο Ε’

Ανάπτυξη παιχνιδιού

Ε.1 Ανάλυση τεχνολογιών στο παιχνίδι

Ε.1.1 Websockets

Για την ανάπτυξη του παιχνιδιού η κύρια τεχνολογία που χρησιμοποιήθηκε για να εμπεριέχονται στο παιχνίδι πολλοί παίκτες μαζί, είναι τα Websockets. Τα Websockets δημιουργήθηκαν για να αντιμετωπίσουν το πρόβλημα της HTTP. Το Διαδίκτυο έχει φτιαχτεί με τον τρόπο αίτησης και απάντησης, όπου ένας client φορτώνει μια ιστοσελίδα και περιμένει μέχρι ο χρήστης να πατήσει για να μεταφερθεί στην επόμενη σελίδα. Αυτή η διαδικασία είχε το πρόβλημα ότι όλες οι HTTP επικοινωνίες ξεκινούσαν από τον client και έπρεπε ο χρήστης να πατήσει κάτι στην ιστοσελίδα για να ανανεωθεί το περιεχόμενο της. Ένας άλλος τρόπος ήταν η χρήση κάποιας long polling τεχνικής.

Για τον λόγο αυτό, δημιουργήθηκαν τα Websockets ώστε να μην υπάρχει το συγκεκριμένο κόστος της HTTP που αναφέρθηκε παραπάνω. Τα Websockets είναι ένα μια αμφίδρομη, full-duplex και μόνιμη σύνδεση μεταξύ ενός περιηγητή και ενός server. Όταν δημιουργείται μια σύνδεση Websocket τότε αυτή παραμένει ανοιχτή μέχρι ο client ή ο server να κλείσουν την σύνδεση[7].

Τα Websockets χρησιμοποιούνται για διάφορους σκοπούς όπως είναι για παράδειγμα, τα διαδικτυακά παιχνίδια, ή την ενημέρωση πινάκων σε πραγματικό χρόνο, όπως είναι τα αποθέματα.[8]

Γενικά, οι λόγοι χρήσης των Websockets είναι πολλοί. Πιο συγκεκριμένα χρησιμοποιούνται για θέματα απόδοσης καθώς καθιστούν την επικοινωνία σε πραγματικό χρόνο να γίνεται πιο αποτελεσματική. Επίσης, με την χρήση των Websockets εξοικονομείτε εύρος ισχύος, CPU και χρόνος αναμονής. Ένας ακόμη λόγος είναι η απλότητα τους διότι διευκολύνουν την σύνδεση μεταξύ του client και του server, σε σχέση με την πολύπλοκη σύνδεση της HTTP, πριν την εμφάνιση των

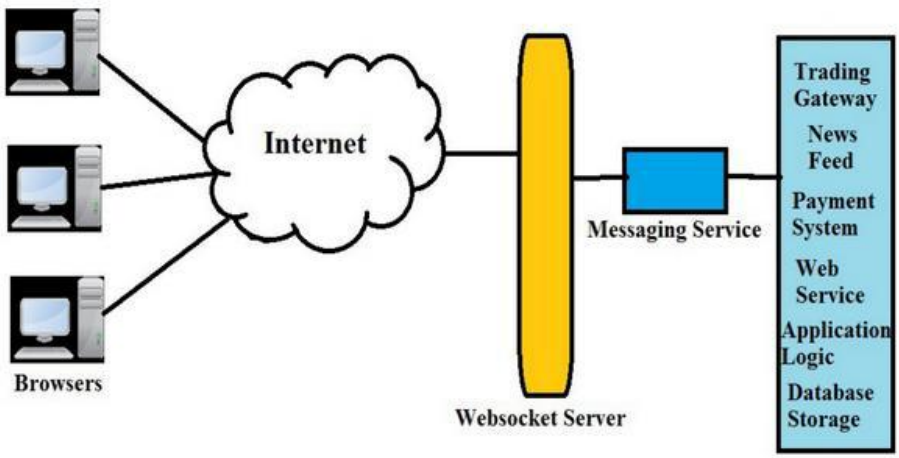
7 Web sockets, Introduction to Websockets, http://socketo.me/docs/ (last visit: 25/11/2018)
8 Web sockets, Introduction to Websockets, http://socketo.me/docs/ (last visit: 25/11/2018)

Websockets. Τα Websockets επιτρέπουν την απλοποίηση της σύνδεσης για την επικοινωνία εφαρμογών σε πραγματικό χρόνο. Ουσιαστικά, τα Websockets χρησιμοποιούνται λόγω ότι βασίζονται σε ένα βασικό πρωτόκολλο δικτύου που επιτρέπει την δημιουργία άλλων πρωτοκόλλων πάνω του. Τέλος, τα Websockets αποτελούν πολύτιμο λίθο για την δημιουργία διαδικτυακών εφαρμογών με την HTML5 (Wang, Salim, Moskovits, 2012).

Σύμφωνα με την HTML5 προσδιορίζει στα έγγραφα της, ότι τα Websockets είναι σαν ένα API που επιτρέπουν στις ιστοσελίδες να χρησιμοποιούν το πρωτόκολλο της, για την διπλή κατεύθυνση της επικοινωνίας με έναν απομακρυσμένο πάροχο. Επίσης, εισάγει την διεπαφή με τα Websockets και προσδιορίζει ένα full duplex κανάλι επικοινωνίας. Τα Websockets δημιουργούν εύφορο έδαφος για το streaming ώστε οποιαδήποτε σύνδεση να είναι δυνατόν να πραγματοποιηθεί. Ακόμη, παρέχουν την δυνατότητα να ανεβάζουν και να κατεβάζουν δεδομένα χρησιμοποιώντας μόνο μια σύνδεση (Wang, Salim, Moskovits, 2012).

Γενικά, τα Websockets επιτρέπουν την πλήρη αμφίδρομη σύνδεση με ένα socket μεταξύ του client και του server (Kulshrestha, pp.14-18, 2013).

Αν μια εφαρμογή χρησιμοποιεί τα Websockets τότε επιβαρύνει λιγότερο τον server, και επιτρέπει στις μηχανές να υποστηρίζουν περισσότερες ταυτόχρονες συνδέσεις.



Εικόνα 1, Βασική αρχιτεκτονική Websockets

Η αλλαγή των δύο πρωτοκόλλων πραγματοποιείται με αίτημα του περιηγητή στον server, το οποίο δείχνει την επιθυμία να αλλάξει το πρωτόκολλο από HTTP σε Websocket. Ουσιαστικά, ο client εκφράζει αυτή την επιθυμία μέσω της αναβάθμισης του header, όπως φαίνεται παρακάτω:

```
GET ws://echo.websocket.org/?encoding=text HTTP/1.1
Origin: http://websocket.org
Cookie: __utma=99as
Connection: Upgrade
Host: echo.websocket.org
Sec-WebSocket-Key: uRovscZjNol/umbTt5uKmw==
Upgrade: websocket
Sec-WebSocket-Version: 13
```

Στην συνέχεια, εάν ο server κατανοήσει αυτή την αλλαγή στο Websocket πρωτόκολλο, τότε συμφωνεί με την συγκεκριμένη αλλάγη, μέσω του Upgrade header, όπως φαίνεται παρακάτω:

```
HTTP/1.1 101 WebSocket Protocol Handshake
Date: Fri, 10 Feb 2012 17:38:18 GMT
Connection: Upgrade
```

```
Server: Kaazing Gateway
Upgrade: WebSocket
Access-Control-Allow-Origin: http://websocket.org
Access-Control-Allow-Credentials: true
Sec-WebSocket-Accept: rLHCkw/SKsO9GAH/ZSFhBATDKrU=
Access-Control-Allow-Headers: content-type
```

E.1.2 React JS

Η ReactJS είναι βιβλιοθήκη της JavaScript που δημιουργήθηκε από την Facebook, χρησιμοποιείται για να διαχειρίζεται το μπροστινό επίπεδο των ιστοσελίδων και των εφαρμογών για κινητό. Ουσιαστικά, η ReactJS επιτρέπει να δημιουργηθούν και να επαναχρησιμοποιηθούν κομμάτια της διεπαφή με τον χρήστη (UI). Μέχρι στιγμής είναι η πιο δημοφιλής βιβλιοθήκη της JavaScript και έχει πολύ δυνατά θεμέλια και

μεγάλη κοινότητα που την υποστηρίζει. Το ουσιαστικό πλεονέκτημα της ReactJS είναι ότι δεν ανανεώνει ολόκληρη την σελίδα αλλά μόνο τα κομμάτια που άλλαξαν με αποτέλεσμα να προσφέρει καλύτερη απόδοση και ένα πιο απλό μοντέλο προγραμματισμού. Η ReactJS μπορεί να χρησιμοποιηθεί στον server με την χρήση της NodeJS[9]

Τι προσφέρει η React:

- JSX: Το JSX είναι συντακτικό της JavaScript φυσικά δεν απαιτείται να χρησιμοποιηθεί στην ανάπτυξη εφαρμογών με React αλλά συνήθως την επιλέγουν.
- Components: Η React χρησιμοποιεί τα components, ουσιαστικά αποτελούν κομμάτια συγκεκριμένου κώδικα που βοηθούν να διατηρείται ο κώδικας όταν πρόκειται για μια μεγάλη εργασία.
- Μονόδρομη ροή δεδομένων: Η React ενεργεί σε μονόδρομη ροή δεδομένων και καθιστά εύκολη την διατήρηση των εφαρμογών καθώς το μοτίβο της ροής βοηθάει να διατηρηθούν τα δεδομένα
- Άδεια: Η React έχει άδεια από την Facebook Inc.

Πλεονεκτήματα της ReactJS:

- Χρησιμοποιεί το virtual DOM το οποίο αποτελεί αντικείμενο της JavaScript με αποτέλεσμα να βελτιώνει την απόδοση των εφαρμογών, καθώς το virtual DOM της JavaScript είναι πιο γρήγορη τακτική από το κλασσικό DOM.
- Υπάρχει στην πλευρά του client και του server μαζί με άλλα frameworks.
- Τα component και τα μοτίβα δεδομένων βοηθούν στην ανάγνωση των εφαρμογών με αποτέλεσμα να ενισχύει την δημιουργία και διατήρηση μεγάλων εφαρμογών.

E.1.2.1 ReactJS - JSX

Η ReactJS χρησιμοποιεί το μοντέλο JSX αντί των τακτικών της JavaScript φυσικά αυτό δεν είναι απαραίτητο αλλά προσφέρει μερικά από τα παρακάτω πλεονεκτήματα:

- Είναι γρηγορότερη διότι εκτελεί βελτιστοποίηση κατά την εκτέλεση του κώδικα της JavaScript.

9 Tutorials Point, https://www.tutorialspoint.com/reactjs/index.htm, (last visit: 25/12/2018)

- Επίσης, προσφέρει ασφάλεια κατά την σύνταξη του κώδικα καθώς τα περισσότερα λάθη μπορούν να διορθωθούν στην σύνταξη.
- Προσφέρει ιδιαίτερη βοήθεια για την συγγραφή εύκολων και γρήγορων προτύπων με την βοήθεια της HTML.

Η JSX μοιάζει με την κλασσική HTML, σε πολλές περιπτώσεις βέβαια υπάρχουν κάποιες διαφορές. Βοηθάει να γράφονται τα components της React, με την συγγραφή της HTML καθώς και διάφορα events της JavaScript. Παρακάτω δίνεται ένα κλασσικό περίγραμμα της React χρησιμοποιώντας την JSX.

```
import React from 'react';

class App extends React.Component {
      render() {
                  return (
                        <div>
                       Hello World!!!
                        </div>
                  );
        .       }
        }
export default App;
```

E.1.2.2 ReactJS - Components

Ο λόγος που η ReactJS είναι ιδιαίτερα διάσημη βιβλιοθήκη της JavaScript είναι διότι χρησιμοποιεί components, τα οποία βοηθούν για να διατηρηθούν οι εφαρμογές καθώς επιτρέπει την ενημέρωση και την αλλαγή τους χωρίς να επηρεάζεται ολόκληρη η σελίδα. Η σύνταξη των components ξεκινάει με όνομα της κλάσης του component και στην συνέχεια καλεί την React.Component. Παρακάτω δίνεται η σύνταξη ενός component χρησιμοποιώντας την React.

```
import React from 'react';

   class App extends React.Component {
          render() {
                  return (
                        <div>
                           <Header/>
                           <Content/>
                        </div>
                  );
              }
}
```

Για να εμφανιστεί ο παραπάνω κώδικας πρέπει να το καλέσουμε στο αρχείο main.js την εντολή ReactDOM.render(<App />, document.getElementById('app')).

E.1.3 Node JS

Η NodeJS αποτελεί πλατφόρμα ανάπτυξης λογισμικού για τους διακομιστές σε JavaScript, η πρώτη έκδοση της έγινε το 2009. Ο κυριότερος στόχος της NodeJS είναι να παρέχει τρόπους για την δημιουργία κλιμακωτών διαδικτυακών εφαρμογών. Πιο συγκεκριμένα, μια διεργασία node δεν στηρίζεται στην πολυνηματικότητα αλλά στο μοντέλο ασύγχρονης επικοινωνίας εισόδου εξόδου.

Τα χαρακτηριστικά της NodeJS:

- Η NodeJS είναι ανοιχτού κώδικα περιβάλλον για server.
- Παρέχεται δωρεάν στο κοινό.
- Τρέχει σε διάφορες πλατφόρμες όπως Windows, Linux, Unix, Mac OS X.
- Χρησιμοποιεί την JavaScript για τον server.

Γενικά η NodeJS χρησιμοποιεί τον ασύγχρονο προγραμματισμό. Μια βασική εργασία ενός web server είναι να ανοίξει ένα αρχείο στον server και να επιστρέψει το περιεχόμενο στον client. Ο τρόπος που η NodeJS χειρίζεται ένα αίτημα είναι ο εξής. Αρχικά στέλνει την εργασία στο υπολογιστικό σύστημα, στην συνέχεια είναι έτοιμο να διαχειριστεί το επόμενο αίτημα και τέλος όταν το σύστημα ανοίξει και διαβάσει το αρχείο ο server επιστρέφει το περιεχόμενο στον client. Αποτελεί πιο αποτελεσματικό τρόπο επικοινωνίας client και server σε σχέση με τις βασικές γλώσσες προγραμματισμού όπως η PHP διότι η NodeJS εξαλείφει την αναμονή, καθώς συνεχίζει με το επόμενο αίτημα και δεν περιμένει να έρθει με αποτέλεσμα να την κάνει πιο αποτελεσματική στο θέμα του χρόνου. Ένα ακόμη πλεονέκτημα της NodeJS είναι ότι λειτουργεί με single-threaded, non blocking και ασύγχρονο προγραμματισμό με αποτέλεσμα να είναι πολύ αποτελεσματική στην μνήμη.

Οι λειτουργίες της NodeJS:

- Δημιουργεί περιεχόμενο για δυναμικές σελίδες.
- Μπορεί να δημιουργήσει, να ανοίξει, να διαβάσει, να γράψει, να διαγράψει και να κλείσει αρχεία στον server.
- Μπορεί να συλλέξει δεδομένα από φόρμες.
- Μπορεί να προσθέσει, να διαγράψει και να τροποποιήσει δεδομένα από την βάση δεδομένων.

Παρακάτω, υπάρχει ένα αρχείο NodeJS που εμφανίζει στην σελίδα ένα μήνυμα, όταν κάποιος προσπαθήσει να εισέλθει από τον φυλλομετρητή στην θύρα 8080.

```
var http = require('http');

http.createServer(function (req, res) {
        res.writeHead(200, {'Content-Type': 'text/html});
            res.end('Hello World\n');
      }).listen(8080);
```

Η NodeJS προσφέρει:

- Καλύτερη απόδοση και παραγωγικότητα στους προγραμματιστές
- Διαμοιρασμό του κώδικα και επαναχρησιμοποίηση
- Ταχύτητα και απόδοση
- Ευκολία ανταλλαγή γνώσεων στις ομάδες
- Μεγάλο αριθμό δωρεάν εργαλείων

Η node δίνει έμφαση στην ασύγχρονη επικοινωνία μεταξύ των υπολογιστικών πόρων. Ουσιαστικά αυτό το επιτυγχάνει με την χρήση συμβάντων (events) που προσφέρει η JavaScript τα οποία ονομάζονται callbacks.

Ένα απλό παράδειγμα για την λειτουργία της Node σε ένα απλό HTTP εξυπηρετητή είναι ο παρακάτω κώδικας. Ο κώδικας αυτός δημιουργεί εξυπηρετητή που τρέχει τοπικά στην θύρα 8001. Έπειτα στον φυλλομετρητή όταν δίνεται η παρακάτω διεύθυνση του εμφανίζει μια σελίδα Hello World.

```
var http = require('http');
http.createServer(function (req, res) {
        res.writeHead(200, {'Content-Type': 'text/plain'});
        res.end('Hello World\n');
   }).listen(1337, '127.0.0.1');
console.log('Server running at http://127.0.0.1:8001/');
```

E.1.4. JavaScript

Ακόμη μια γλώσσα προγραμματισμού που χρησιμοποιήθηκε για την ολοκλήρωση του παιχνιδιού με κάρτες είναι η JavaScript. Η JavaScript είναι αντικειμενοστραφής γλώσσα προγραμματισμού που δεν χρειάζεται μεταγλώττιση. Στην αρχή της δημιουργίας της χρησιμοποιούνταν κυρίως για την δημιουργία ιστοσελίδων στους φυλλομετρητές, ωστόσο τα δεδομένα έχουν αλλάξει καθώς χρησιμοποιείται για διάφορες χρήσεις όπως η επικοινωνία με τον χρήστη, η ανταλλαγή ασύγχρονων δεδομένων και η δυναμική αλλαγή του περιεχομένου των διαδικτυακών εφαρμογών.

Αποτελεί μαζί με την HTML και την CSS την βάση για την δημιουργία του περιεχομένου στο Διαδίκτυο. Ουσιαστικά η HTML ορίζει το περιεχόμενο της διαδικτυακής σελίδας, η CSS την διαμόρφωση της ιστοσελίδας και η JavaScript την συμπεριφορά της ιστοσελίδας.

Η JavaScript είναι scripting γλώσσα προγραμματισμού, η σύνταξη της είναι επηρεασμένη από την γλώσσα προγραμματισμού C. Κυρίως χρησιμοποιείται ως γλώσσα σεναρίου (scripting language) για ιστοσελίδες και διαδικτυακές εφαρμογές. Το πρότυπο της JavaScript ονομάζεται ECMAScript, γενικά από το 2012 οι περισσότεροι φυλλομετρητές χρησιμοποιούν την ECMAScript. Η πρόσφατη επίσημη έκδοση της ονομάζεται ECMAScript 6 ή ES6. Η JavaScript θεωρείται μια εύκολη γλώσσα προγραμματισμού για να μάθει ο ενδιαφερόμενος την συγγραφή της.

Που χρησιμοποιείται η JavaScript:

- Στις ιστοσελίδες
- Σε διαδικτυακές εφαρμογές όπως τα έγγραφα PDF
- Σε εξειδικευμένους φυλλομετρητές
- Σε εφαρμογές για την επιφάνεια εργασίας (desktop widgets)
- Σε εικονικές μηχανές
- Σε διάφορα πλαίσια ανάπτυξης όπως η NodeJS

Πλεονεκτήματα της JavaScript:

1. Η ταχύτητα αποτελεί ένα από τα βασικά πλεονεκτήματα της JavaScript διότι είναι πολύ γρήγορη στον client.
2. Είναι εύκολη στην εκμάθηση της και στην εφαρμογή της
3. Είναι πολύ διάσημη καθώς χρησιμοποιείται παντού στο Διαδίκτυο.
4. Αποτελεί μια λειτουργική γλώσσα προγραμματισμού καθώς μπορεί να χρησιμοποιηθεί σε διάφορες εφαρμογές ανεξαρτήτως του αρχείου.
5. Διαθέτει πολλές διεπαφές
6. Χρησιμοποιείται ως διακομιστής με αποτέλεσμα να μειώνεται ο χρόνος αναμονής του server της ιστοσελίδας
7. Διαθέτει συνεχής ενημέρωσης.

Ε.2 Οθόνες

Ε.2.1 Πρώτη οθόνη

Στην πρώτη οθόνη μόλις εισέρχεται ο νέος παίκτης στο παιχνίδι υπάρχει μια φόρμα για την εισαγωγή του ονόματος του, στην συνέχεια πατώντας το κουμπί "Go" εισέρχεται στην επόμενη σελίδα και περιμένει να τους υπόλοιπους παίκτες.

Στην αρχική οθόνη υπάρχει το εισαγωγικό κείμενο που αναλύει τον σκοπό του παιχνιδιού στους παίκτες. Επίσης, στο κάτω μέρος της σελίδας βρίσκεται το μενού του παιχνιδιού. Το μενού δημιουργήθηκε με σκοπό να βοηθήσει τους παίκτες να κατανοήσουν τον τρόπο που παίζεται το παιχνίδι, τους κανόνες τις οδηγίες και την θεωρία του Cyber Kill Chain που οφείλουν οι παίκτες να διαβάσουν για να κατανοήσουν τον σκοπό του παιχνιδιού.

Οι κατηγόριες που υπάρχουν στο μενού είναι:

1. Οδηγίες
2. Κανόνες
3. Μοτίβα επιθέσεων
4. Βοήθεια

Παρακάτω, είναι ο κώδικας της αρχικής σελίδας σε html. Το συγκεκριμένο κομμάτι φορτώνεται στην αρχή του παιχνιδιού το οποίο καλεί τα διάφορα scripts για να παίξει το παιχνίδι. Στο body της html σελίδας υπάρχουν τέσσερα μοναδικά id τα οποία εκτελούνται στην αρχή της σελίδας. Το script bundle.js είναι ένα αρχείο το οποίο περιέχει όλο τον κώδικα που πρέπει να εκτελεστεί χωρίς να διαβάζει κάθε φορά το μονοπάτι του κάθε αρχείου και να εκτελείται. Αυτό έχει ως αποτέλεσμα να φορτώνεται πιο γρήγορα η σελίδα.

```
<!DOCTYPE
html> <html>
<head>
    <title>Defender | Home</title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, intitial-scale=1">

    <link rel="stylesheet"
href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css">
```

```
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.2.0/jquery.min.js"></script>
    <script
src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>

    <link rel="stylesheet" href="./styles/style.css">
    <link rel="stylesheet" href="./styles/timer.css">
    <link rel="stylesheet" href="./styles/chat.css">
    <link rel="stylesheet" href="./Libraries/sweetalert2/dist/sweetalert2.css">
    <!--<link rel="import" href="AcidJs.XDeck/classes/XDeck.html"/>-->
    <script src="/jquery/dist/jquery.js"></script> <script
    src="/socket.io/socket.io.js"></script>
</head>
<body>
<div id="firstScreenContainer"></div>
<div id="helpScreenContainer"></div>
<div id="secondScreenContainer"></div>
<div id="thirdScreenContainer"></div>
<script src="./dist/bundle.js"></script>

</body>
</html>
```

Ε.2.2 Μενού

Το μενού δημιουργήθηκε στο παιχνίδι ως μέσο επεξήγησης του παιχνιδιού για τον παίκτη. Οι παίκτες καθώς περιηγούνται στην σελίδα, στο κάτω μέρος της αρχικής οθόνης υπάρχουν οι οδηγίες για το πως παίζεται το παιχνίδι. Το μενού περιέχει τέσσερις βασικές κατηγορίες τις: Οδηγίες, Κανόνες, Μοτίβα Επιθέσεων και την βοήθεια.

Εικόνα 2, Μενού για το παιχνίδι

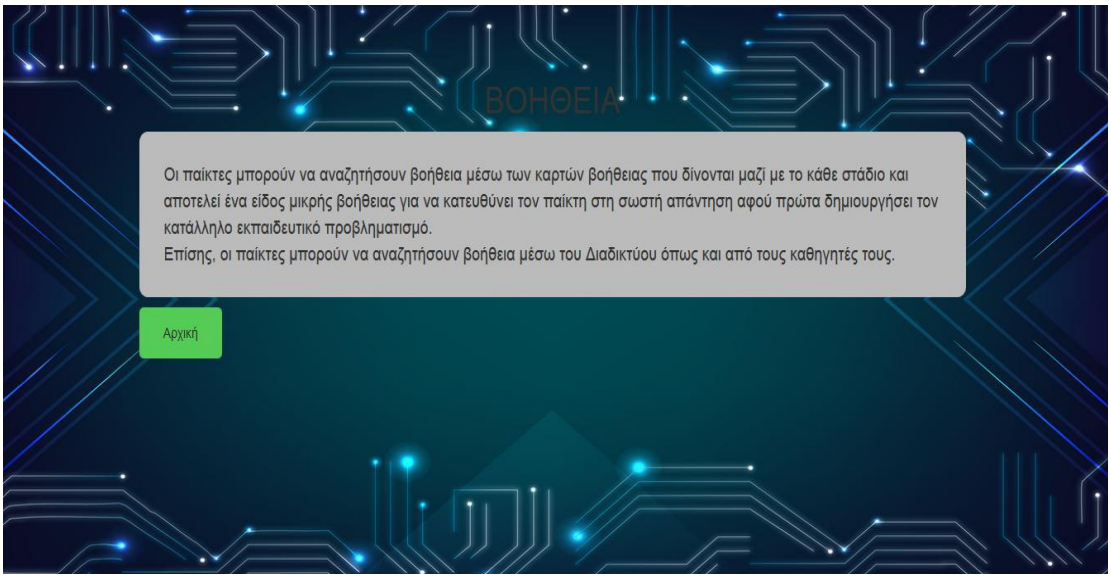
Για την δημιουργία του συγκεκριμένου μενού δημιουργήθηκε η κλάση NavBar η οποία κληρονομεί όλα τα component από την react. Όπως όλες οι κλάσεις έτσι και αυτή περιέχει τον κατασκευαστή της. Στην συνέχεια, υπάρχει το μοναδικό id helpScreenContainer το οποίο καλείται μόλις πατηθεί η λίστα από το μενού. Κάθε κομμάτι του μενού είναι μια λίστα το οποίο περιέχει μοναδικά id, με αποτέλεσμα

μόλις πατηθεί η συγκεκριμένη κατηγορία του μενού, ανοίγει το παράθυρο με την επιλογή του χρήστη. Η λίστα περιέχει τις οδηγίες, τους κανόνες, τα μοτίβα επιθέσεων και την βοήθεια, το οποίο βρίσκεται με ξεχωριστό id μέσα σε αντικείμενο που καλείται μόλις ο χρήστης το πατήσει.

```
import React from "react";
import ReactDOM from "react-dom";
import HelpPage from "./HelpPage";

export default class NavBar extends React.Component {
   constructor(){
      super();
   }

   helpPage(type){
      ReactDOM.render(<HelpPage
type={type}/>,document.getElementById("helpScreenContainer"));

ReactDOM.unmountComponentAtNode(document.getElementById('firstScreenContainer'));
   }

   render() {
      return (
            <nav className="nav nav--active" id="navbar">
               <ul className="nav__list">
                  <li className="nav__item" onClick={()=>this.helpPage("instructions")}>
                     <a className="nav__link">
                        <div className="nav__thumb color1" data-letter="O"></div>
                        <p id="instructions" className="nav__label">ΟΔΗΓΙΕΣ</p>
                     </a>
                  </li>
                  <li className="nav__item"
                     onClick={()=>this.helpPage("rules")}> <a
                     className="nav__link">
                        <div className="nav__thumb color2" data-letter="K"></div>
                        <p id="rules" className="nav__label">ΚΑΝΟΝΕΣ</p>
                     </a>
                  </li>
                  <li className="nav__item">
                     <a className="nav__link" onClick={()=>this.helpPage("attacks")}>
                        <div className="nav__thumb color3" data-letter="M"></div>
                        <p id="motiva" className="nav__label">ΜΟΤΙΒΑ ΕΠΙΘΕΣΕΩΝ</p>
```

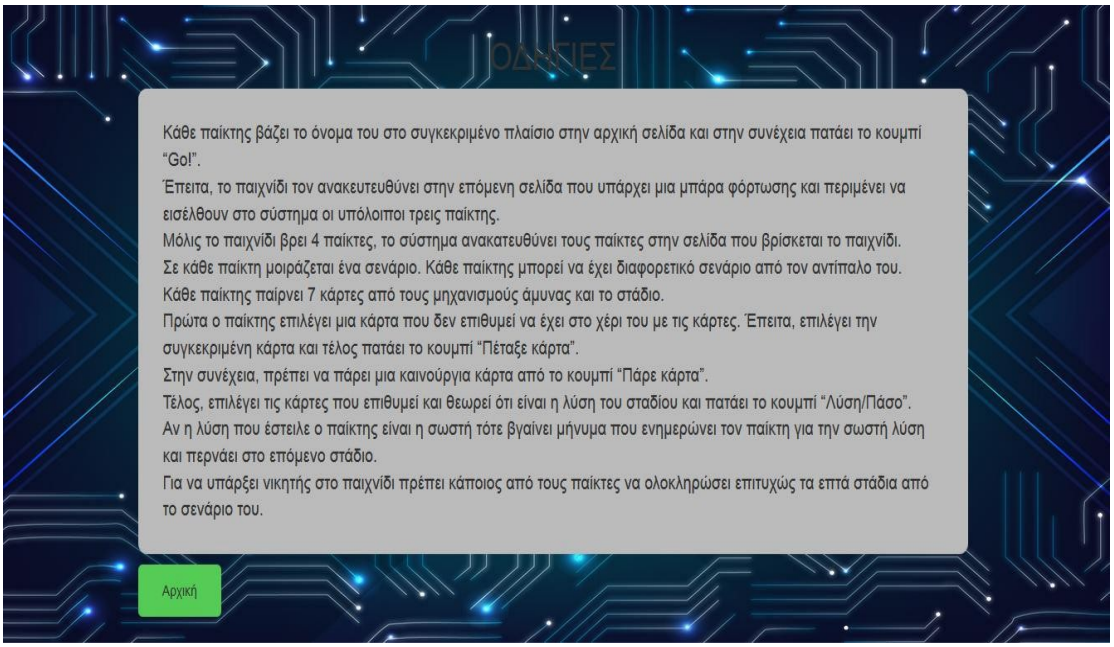
```
                    </a>
                </li>
                <li className="nav__item" onClick={()=>this.helpPage("help")}> <a
                    className="nav__link">
                    <div className="nav__thumb color4" data-letter="B"></div>
                    <p id="help" className="nav__label">ΒΟΗΘΕΙΑ</p>
                </a>
                </li>
            </ul>
        </nav>
    );
  };
};
module.exports=NavBar;
```

Παρακάτω, υπάρχουν εικόνες με τις υποκατηγορίες του μενού, στην συγκεκριμένη εικόνα παρατηρούμε ότι ο χρήστης διαβάζει την υποκατηγορία του μενού Βοήθεια.



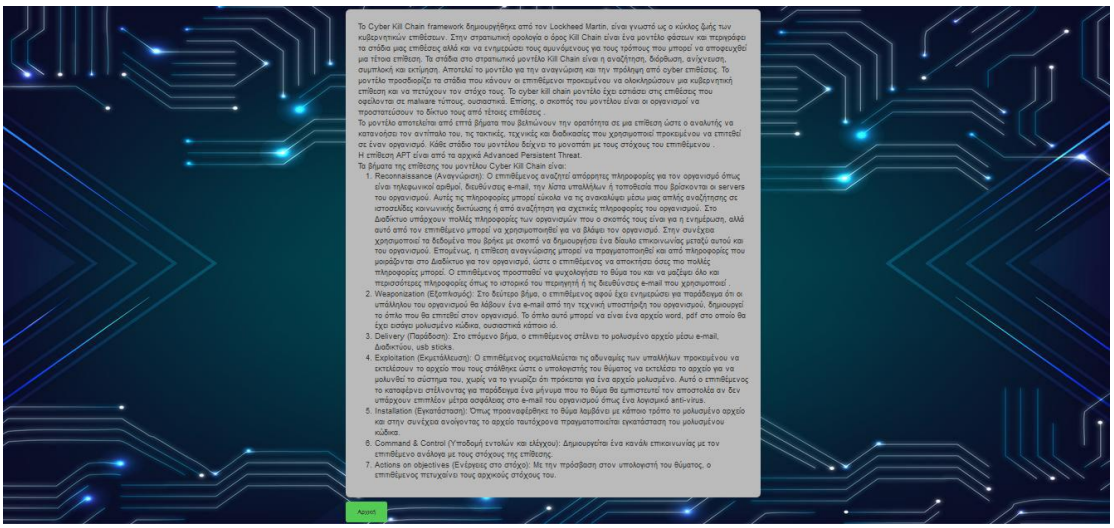
Εικόνα 3, Κατηγορία Βοήθεια από το μενού

Παρακάτω, υπάρχουν εικόνες με τις υποκατηγορίες του μενού, στην συγκεκριμένη εικόνα παρατηρούμε ότι ο χρήστης διαβάζει την υποκατηγορία του μενού Οδηγίες.



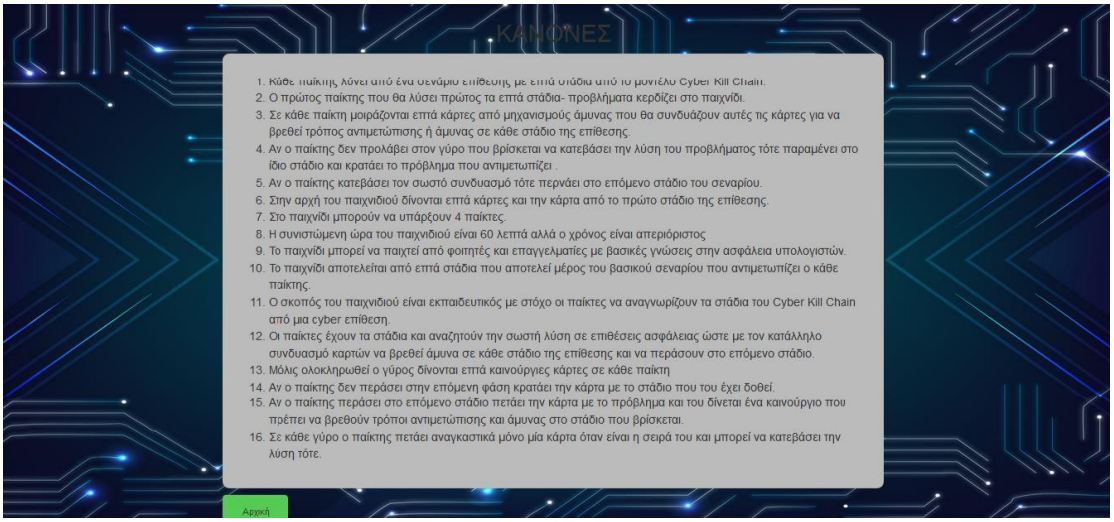
Εικόνα 4, Κατηγορία Οδηγίες από το μενού

Παρακάτω, υπάρχουν εικόνες με τις υποκατηγορίες του μενού, στην συγκεκριμένη εικόνα παρατηρούμε ότι ο χρήστης διαβάζει την υποκατηγορία του μενού Μοτίβα επιθέσεων που επεξηγεί την μεθοδολογία cyber kill chain.



Εικόνα 5, Κατηγορία Μοτίβα επιθέσεων από το μενού

Παρακάτω, υπάρχουν εικόνες με τις υποκατηγορίες του μενού, στην συγκεκριμένη εικόνα παρατηρούμε ότι ο χρήστης διαβάζει την υποκατηγορία του μενού Κανόνες. Οι κανόνες επεξηγούν τους τρόπους που οφείλουν οι παίκτες να συμμορφωθούν για το παιχνίδι, τον εκτιμώμενο χρόνο που παίζεται το παιχνίδι, τον σκοπό του, καθώς και τον τρόπο που λειτουργούν τα τρία βασικά κουμπιά του παιχνιδιού.



Εικόνα 6, Κατηγορία Κανόνες από το μενού

Ε.2.3 Κάρτες

Η κλάση card παίρνει ως παράμετρο τις κάρτες που του έστειλε ο server και στην συνέχεια ελέγχει τον αριθμό καρτών που έχει ο παίκτης στο χέρι του. Δημιουργεί τον πίνακα cards in hand στον οποίο παίρνει το μονοπάτι που είναι αποθηκευμένες οι κάρτες, τοποθετεί για κάθε κάρτα το όνομα που έχει και στην συνέχεια την κατάληξη svg που είναι ο τύπος αρχείου της κάθε κάρτα. Στην συνέχεια, δημιουργεί react elements για να εμφανίζονται οι κάρτες στον παίκτη. Ένα ακόμη σημείο που πρέπει να αναλυθεί για τις κάρτες είναι το checkbox το οποίο λειτουργεί ως επιλογή πολλών καρτών. Χρησιμοποιήθηκε έτσι ώστε οι παίκτες να μπορούν να επιλέξουν πολλές κάρτες, ο τίτλος του checkbox βρίσκεται κρυμμένος και στην θέση του μπαίνει η εικόνα της κάθε κάρτας.

```
import React from "react";

export default class Card extends React.Component
  { constructor(props) {
      super(props);
      this.cards = [];
  }
```

```
  render() {
    this.cards.length = 0;
    for (let i = 0; i < this.props.cardsInHand.length; i++)
      { let card=this.props.cardsInHand[i];
      let src="./images/deck/" + card + ".svg";
      this.cards.push(<React.Fragment key={i}>
        <label htmlFor={"card" + i + "_check"}
onClick={this.props.handleCards.bind(this)}>
          <img className="myImg zoom card" id={"card" + i} src={src}/>
        </label>
        <input type="checkbox" hidden id={"card" + i +
"_check"} checked={this.props.selectedCards["card" + i]}
name="card" disabled={this.props.cardsDisabled}/>
      </React.Fragment>)
    }
    return <React.Fragment>{this.cards}</React.Fragment>;
  };
};

module.exports = Card;
```

E.2.4 Αρχική οθόνη

Η αρχική οθόνη αποτελεί την πρώτη οθόνη που βλέπει ο παίκτης όταν εισέρχεται στην σελίδα. Ξεκινάει με την κλάση welcome screen η οποία κληρονομεί τα components από την react. Στην συνέχεια, ελέγχει αν το input για το username δεν είναι κενό, τότε με τα Websockets δημιουργεί τον πρώτο παίκτη, αφού ο παίκτης έχει πληκτρολογήσει το όνομα του, το σύστημα τον ανακατευθύνει στην δεύτερη σελίδα, την συγκεκριμένη στιγμή το αντικείμενο player κρατάει το όνομα του παίκτη, και του δίνει τυχαίο σενάριο, τέλος το στάδιο έχει αρχικοποιηθεί ως ένα, διότι όλοι οι παίκτες ξεκινούν από το ίδιο επίπεδο. Αν ο παίκτης δεν συμπληρώσει το όνομα του τότε του εμφανίζεται το συγκεκριμένο μήνυμα " Προσοχή! , "Παρακαλώ συμπληρώστε το όνομά σας."

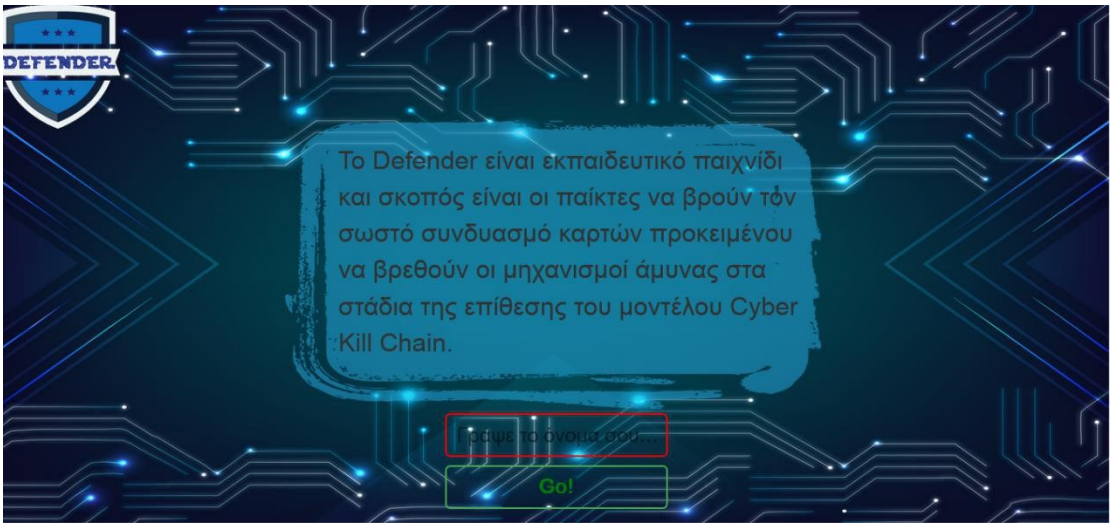
Για την πρώτη σελίδα αρχικά δημιουργείται το λογότυπο του παιχνιδιού που έχει το μοναδικό id logodiv. Έπειτα, υπάρχει το κομμάτι που επεξηγεί το παιχνίδι. Το συγκεκριμένο κομμάτι αποτελεί ένα background ενός πλαισίου εικόνας που μέσα υπάρχει το κείμενο επεξήγησης. Κάτω από το κείμενο επεξήγησης βρίσκεται το

πλαίσιο στο οποίο ο παίκτης συμπληρώνει το όνομα του και έπειτα το κουμπί "Go" το οποίο μεταφέρει τον παίκτη στην επόμενη σελίδα που περιμένει τους υπόλοιπους παίκτες για να ξεκινήσει το παιχνίδι. Στο τελευταίο μέρος της σελίδας υπάρχει το μενού με τις κατηγορίες, οδηγίες, κανόνες, μοτίβα επιθέσεων και βοήθεια, στα οποία ο παίκτης όταν επιλέξει την κάθε κατηγορία η react αλλάζει το πλαίσιο της σελίδας ανάλογα με την κατηγόρια που επέλεξε.

```
import React from "react";
import ReactDOM from "react-dom";
import NavBar from "./NavBar";
import "./MainApp";
import "./SocketListener";
import swal from "../../Libraries/sweetalert2";

export default class WelcomeScreen extends React.Component
  { constructor(props) {
    super(props);
    this.state = {value: ''};
    this.handleChange = this.handleChange.bind(this);
    this.handleSubmit = this.handleSubmit.bind(this);
  }

  handleChange(event) {
    this.setState({value: event.target.value});
  }

  handleSubmit(event) {
    event.preventDefault();
    let username = this.state.value;
    if (username !== "") {
      MainApp.socket.emit('join', username);
    }else{
      swal ( "Προσοχή!" ,  "Παρακαλώ συμπληρώστε το όνομά σας." ,  "error" )
    }
  }

  render() {
    MainApp.inFirstScreen = true;
    return (
      <div>
```

```
            {/*Logo */}
            <div id="logodiv">
               <a href="./index.html" id="logo">
                  <img src="./images/game_logo_new.png"
               id="starlogo"/> </a>
            </div>

            <div id="firstScreen">



               {/*Παράγραφος */}
               <div id="paragraph">
                  <p id="welcomeParagraph">Το Defender είναι εκπαιδευτικό παιχνίδι και
σκοπός είναι οι
                     παίκτες να βρούν τον σωστό συνδυασμό καρτών προκειμένου να βρεθούν
οι μηχανισμοί άμυνας στα
                     στάδια της επίθεσης του μοντέλου Cyber Kill
               Chain.</p> </div>

               <div id="placeholder">
                  <form onSubmit={this.handleSubmit}>
                     <input type="text" name="username" id="placeholder1" placeholder="Γράψε
το όνομα σου..." value={this.state.value} onChange={this.handleChange}/>
                     <br/>
                     <input type="submit" value="Go!"
                  id="btnSubmit"/> </form>
               </div>
            </div>
            <NavBar/>
         </div>
      );
   };
};
ReactDOM.render(<WelcomeScreen/>,
document.getElementById("firstScreenContainer")); // module.exports = WelcomeScreen;
```

Στην εικόνα , βλέπουμε την αρχική όταν εισέρχεται ο παίκτης στο παιχνίδι.



Εικόνα 7, Αρχική οθόνη του παιχνιδιού

Ε.2.5 Δεύτερη οθόνη

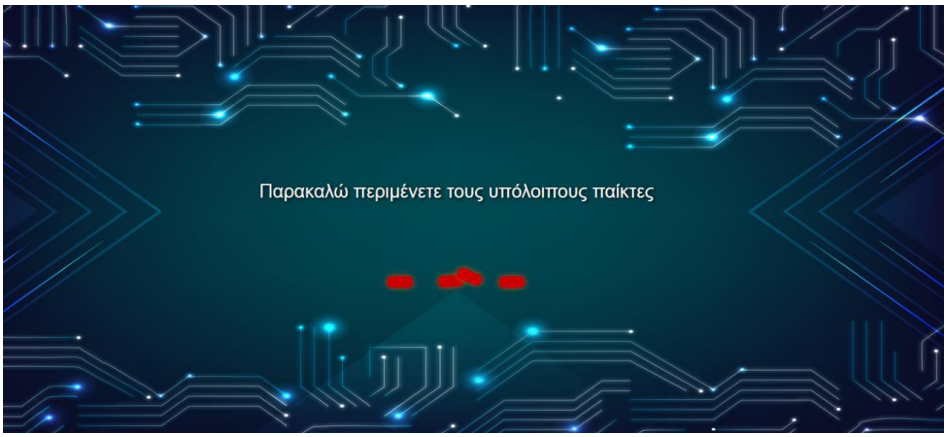
Στην δεύτερη οθόνη οι παίκτες περιμένουν για να εισέλθουν στο παιχνίδι. Το παιχνίδι λειτουργεί ως τραπέζι το οποίο περιέχει τέσσερις θέσεις για τους παίκτες. Κάθε παίκτης μόλις συμπληρώσει το όνομα του στην πρώτη οθόνη του δίνεται ένα μοναδικό id, ώστε το παιχνίδι να αναγνωρίζει όταν οι θέσεις συμπληρωθούν. Ο τέταρτος παίκτης έχει διαφορετικό κώδικα, καθώς μόλις εισέλθει στο παιχνίδι και πληκτρολογήσει το όνομα του, πατώντας το κουμπί "Go", τότε εισέρχεται κατευθείαν στην τελικά οθόνη. Η δεύτερη σελίδα αποτελεί μια από τις σελίδες με τις λιγότερες λειτουργίες καθώς είναι ένα μεταβατικό στάδιο για να εισέλθουν οι παίκτες στο κανονικό παιχνίδι.

```
import React from "react";
import ReactDOM from "react-dom";
```

```
class SecondScreen extends React.Component {
  render() {
    return (
      <div id="secondScreen">

        <h2 id="playerWait">Παρακαλώ περιμένετε τους υπόλοιπους παίκτες</h2>

        <div className="loader">
          <div className="dash one"></div>
          <div className="dash two"></div>
```

```
                <div className="dash three"></div>
                <div className="dash four"></div>
            </div>


        </div>
    );
  };
};

module.exports=SecondScreen;
```

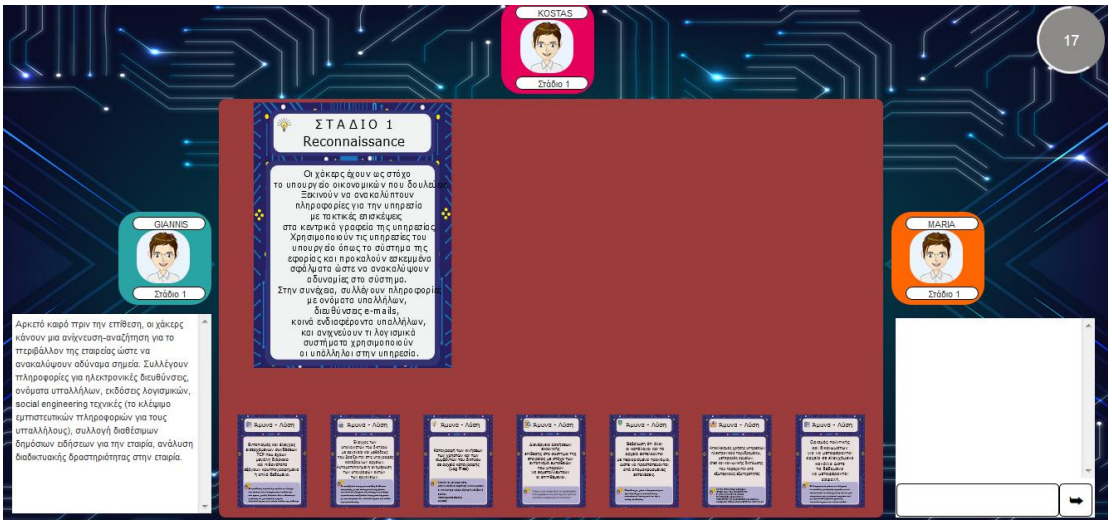
Στην εικόνα , βλέπουμε την δεύτερη οθόνη που περιμένει τους υπόλοιπους παίκτες για να συμπληρωθεί το τραπέζι με τους τέσσερις παίκτες.



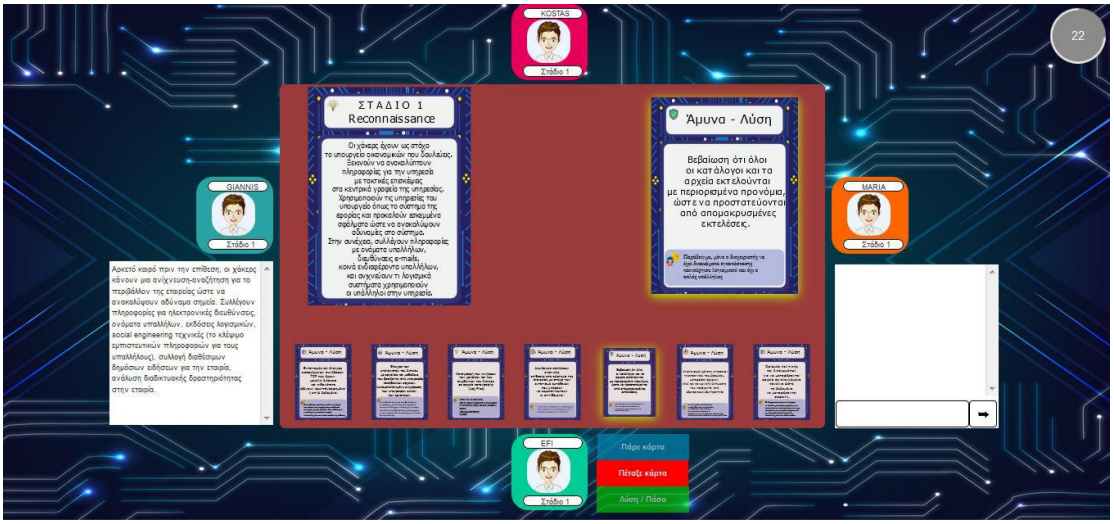
Εικόνα 8, Δεύτερη οθόνη που περιμένει τους υπόλοιπους παίκτες

Ε.2.6 Τρίτη οθόνη

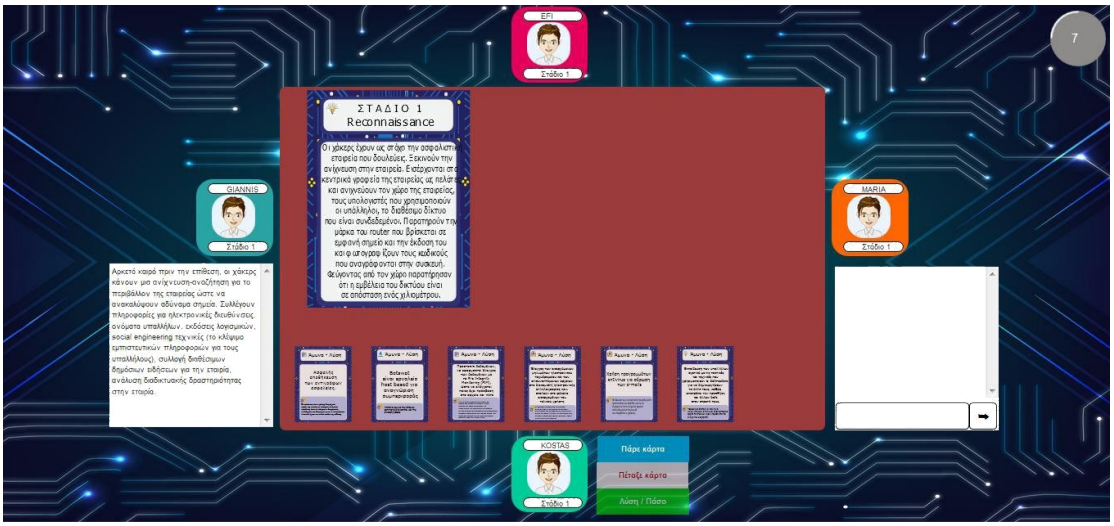
Παρακάτω υπάρχουν εικόνες πως φαίνεται στον παίκτη η τρίτη οθόνη που αποτελεί την βασική οθόνη του παιχνιδιού.



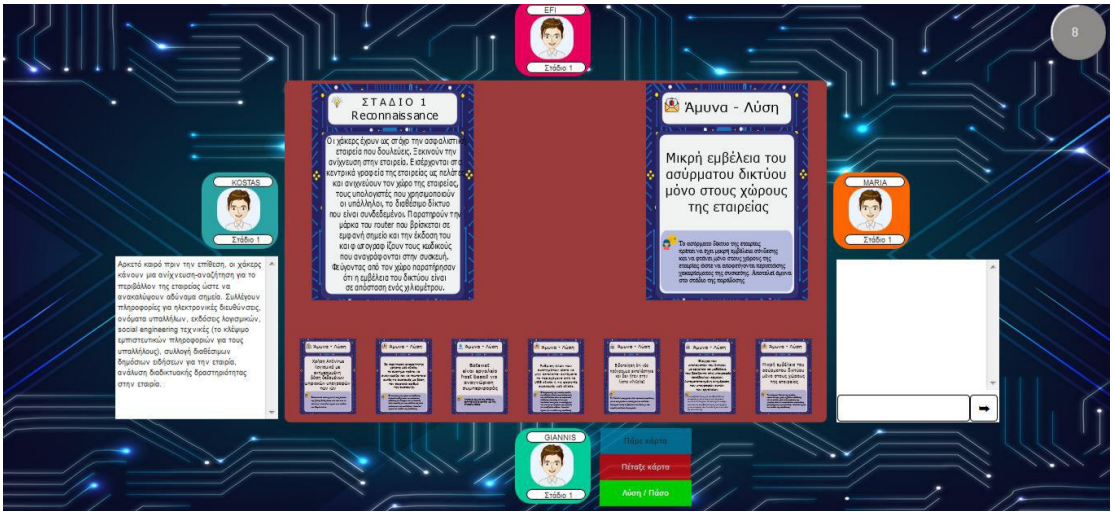
Εικόνα 9, Η κεντρική οθόνη για το παιχνίδι



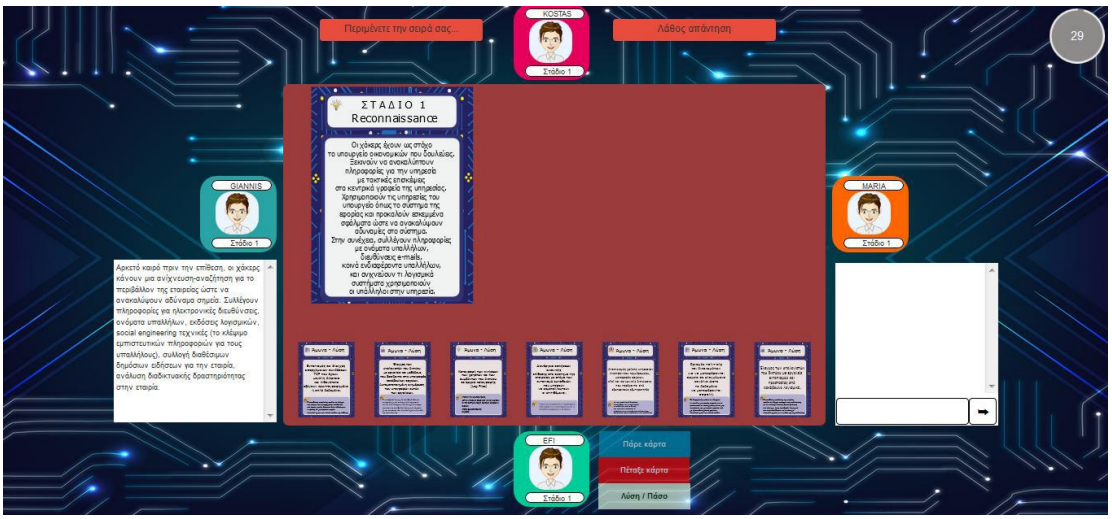
Εικόνα 10, Ο παίκτης έχει επιλέξει μια κάρτα



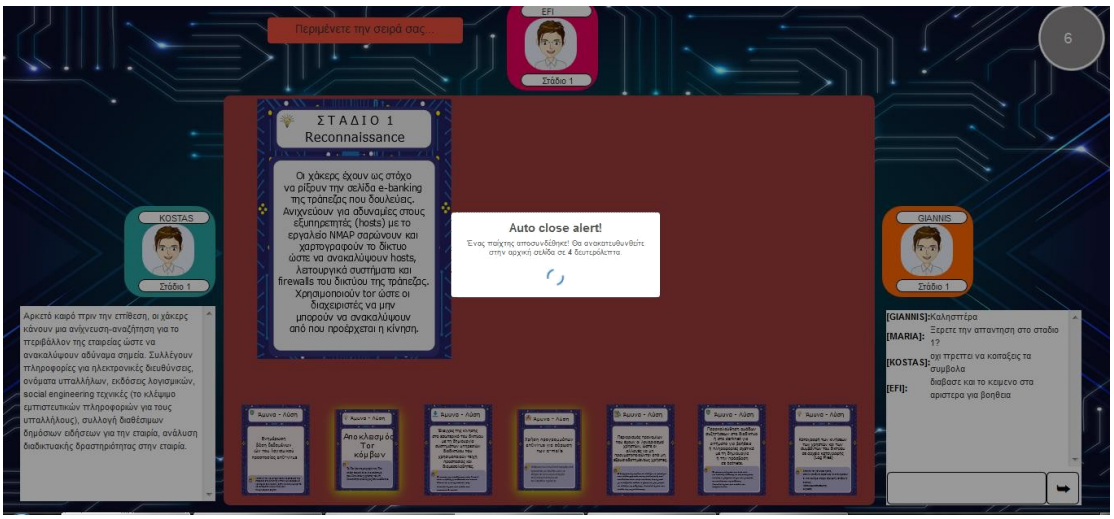
Εικόνα 11, Ο παίκτης πετάει την κάρτα



Εικόνα 12, Ο παίκτης παίρνει μια κάρτα



Εικόνα 13, Ο παίκτης δίνει την απάντηση που είναι λανθασμένη



Εικόνα 14, Αποσύνδεση χρήστη και auto close alert

Ε.2.7 Οι λύσεις για κάθε στάδιο

Κάθε παίκτης για να περάσει στο επόμενο στάδιο πρέπει να επιλέξει των αριθμών καρτών που θεωρεί ότι είναι η σωστή απάντηση και στην συνέχεια να πατήσει το κουμπί "Λύση-Πάσο". Μόλις πατηθεί το συγκεκριμένο κουμπί στέλνονται στον server οι απαντήσεις, δηλαδή οι κάρτες που επέλεξε ο χρήστης μαζί με το σενάριο του και το στάδιο που βρίσκεται. Στην συνέχεια ελέγχονται τα δεδομένα που έστειλε ο client μέσα από το αντικείμενο solution που περιέχει όλες τις σωστές απαντήσεις για κάθε σενάριο και κάθε στάδιο. Έστω και μια κάρτα ο παίκτης να βρει σωστή τότε περνάει στο επόμενο στάδιο. Έτσι, αυξάνει κατά ένα το stage και του επιστρέφει το μήνυμα στην κονσόλα "Good Job". Έπειτα, το παιχνίδι, αφού ο παίκτης περάσει στο επόμενο στάδιο, επιστρέφει ένα καινούργιο deck για να ξεκινήσει το επόμενο στάδιο. Στην συνέχεια, ελέγχει αν το στάδιο του παίκτη είναι μικρότερο του οκτώ. Αν είναι τότε χειρίζεται την απάντηση που έδωσε ο παίκτης, αν δεν είναι τότε εμφανίζει στον παίκτη ότι είναι νικητής και μηδενίζει όλους τους παίκτες, τα σενάρια τους καθώς και το στάδιο τους, ώστε το παιχνίδι να ξεκινήσει από την αρχή.

```
client.on("answer", function (answerObj) {
    let currentPlayer = Players.handlePlayerTurn();
    let newAnswerObject = {
        player: answerObj.player,
        scenario: answerObj.scenario,
        stage: answerObj.stage,
        playerIndex: answerObj.playerIndex
    };
    clearInterval(interval);
    timer(io);
    if (Solution.checkSolution(answerObj)) {
        console.log("good job");
        newAnswerObject.stage++;
        if (newAnswerObject.stage < 8) {
            client.emit('cards', deck.giveCards(), answerObj.playerIndex, newAnswerObject.stage,
Tips["senario" + newAnswerObject.scenario]["st" + newAnswerObject.stage]);
        }
```

```
    } else if (answerObj.selectedCards.length > 0) {
        console.log("try again");
        client.emit('wrongAnswer');
    }
    if (newAnswerObject.stage < 8) {
        io.sockets.emit('handleAnswer', currentPlayer, newAnswerObject);
    } else {
        winner = true;
        io.sockets.emit('winner', newAnswerObject.player.id);
    }
});
```

E.3 Server παιχνιδιού

E.3.1 Deck παιχνιδιού

Κάθε παιχνίδι με κάρτες οφείλει να περιλαμβάνει ένα είδος deck έτσι ώστε οι παίκτες να μπορούν να πετάξουν κάρτες που δεν τους βοηθούν για να ολοκληρώσουν το παιχνίδι τους. Αυτό συμβαίνει και στο Defender. Περιλαμβάνει 85 κάρτες ως deck, οι οποίες ανακατεύονται και στην συνέχεια δίνονται στον κάθε παίκτη, επτά κάρτες. Μόλις ο παίκτης δώσει μια κάρτα στον κάδο τον αχρήστων τότε επιστρέφεται από το deck μια άλλη καινούργια κάρτα, με σκοπό να βοηθήσει τον παίκτη να ολοκληρώσει το παιχνίδι.

Αρχικά, για την δημιουργία του συγκεκριμένου κομματιού στον κώδικα δημιουργήθηκαν οι μεταβλητές playerDeck, που είναι ένας πίνακας με τις κάρτες που έχει ο παίκτης στο χέρι του. Δημιουργήθηκε η μεταβλητή playerHand που ελέγχει πόσες κάρτες δόθηκαν στον παίκτη όταν ξεκίνησε το νέο στάδιο. Η μεταβλητή stageStarted έχει δηλωθεί ως false για να γνωρίζουμε πότε το στάδιο έχει ξεκινήσει ή όχι. Η μεταβλητή playerStage έχει δηλωθεί με ένα, το οποίο είναι το πρώτο στάδιο που ξεκινάει κάθε παίκτης. Μόλις ο παίκτης περάσει στο επόμενο στάδιο τότε αυτό αυξάνεται κατά ένα. Ο πίνακας deck περιλαμβάνει όλα τα αρχεία με τις κάρτες-λύσεις και τέλος η μεταβλητή myDeck περιλαμβάνει τις κάρτες-λύσεις που έχει ο παίκτης στο χέρι του.

Στη συνέχεια, υπάρχει η συνάρτηση initializeDeck ο σκοπός της είναι να δημιουργήσει ένα πίνακα από το ένα έως το ογδόντα πέντε το οποίο ουσιαστικά δημιουργεί το deck του παιχνιδιού. Έπειτα, η συνάρτηση giveCards δημιουργήθηκε για να δίνει στους παίκτες τις επτά κάρτες που χρειάζονται για να παίξουν, πριν δώσει τις κάρτες ανακατεύει το deck προκειμένου να δοθούν οι κάρτες με άλλη σειρά.

Τέλος, επιστρέφει στον κάθε παίκτη τις επτά κάρτες που επιλέχθηκαν και βρίσκονται στον συγκεκριμένο πίνακα. Η συνάρτηση one Card χρησιμοποιείται για να επιστρέψει μια κάρτα στον παίκτη, συγκεκριμένα όταν ο παίκτης επιλέξει μια κάρτα που δεν χρειάζεται, πατήσει το κουμπί give card και μετά δώσει εντολή να του επιστρέψει μια καινούργια κάρτα, πατάει το κουμπί take card. Η συγκεκριμένη συνάρτηση απλώς επιστρέφει μια καινούργια κάρτα από το deck αφού πρώτα ανακατέψει ξανά το deck. Η συνάρτηση shuffle ανακατεύει το deck το οποίο έχει δημιουργηθεί ξεχωριστά και καλείται όποτε χρειαστεί.

```
var playerDeck = [];
var playerHand = 0; //Checks how many deck has been giving when stage
starts var stageStarted = false; //Whether a stage has been started or not var
playerStage = 1; // keeps track of player stage
var deck = []; //Define array pictures
var myDeck;

var Deck = {
   initializeDeck: function () {
      deck.length = 0;
      for (let i = 1; i <= 85; i++) {
         deck.push(i);
      }
      //Shuffles the deck
      myDeck = shuffle(deck);
   },

   giveCards: function () {
      var count = 7;
      playerDeck.length = 0;
      for (let i = 0; i <= 6; i++) {
         playerDeck.push(Math.floor(Math.random() * myDeck.length) + 1);

      }
      return playerDeck;
   },
   oneCard: function () {
      return Math.floor(Math.random() * myDeck.length);
   }
};
```

```
//---------------------------
function shuffle(deck) {
    let toSwap, temp;
    for (let i = 1; i < deck.length; i++) {
        toSwap = Math.floor(Math.random() * i);
        temp = deck[i - 1];
        deck[i - 1] = deck[toSwap];
        deck[toSwap] = temp;
    }
    return deck;
}
```

Ε.3.2 Σειρά των παικτών

Στο συγκεκριμένο κομμάτι, ο server ελέγχει ποιος παίζει την συγκεκριμένη στιγμή. Η μεταβλητή currentPlayer ορίζεται με ένα. Αν η συγκεκριμένη μεταβλητή είναι τέσσερα, τότε ορίζει την μεταβλητή με ένα, για να παίξει ο πρώτος παίκτης πάλι. Αν η μεταβλητή έχει διαφορετικό αριθμό τότε αυξάνει κατά ένα την μεταβλητή και επιστρέφει τον αριθμό αυτό, ο οποίος αποτελεί την σειρά που παίζει ο επόμενος παίκτης.

```
currentPlayer = 1;
var Players = {
    handlePlayerTurn: function () {
        if (currentPlayer === 4) {
            currentPlayer = 1;
        } else {
            currentPlayer++;
        }
        return currentPlayer;
    }
};

module.exports = Players;
```

Ε.3.3 Οι λύσεις των σταδίων

Τα εκπαιδευτικά σενάρια στο παιχνίδι με κάρτες είναι πέντε. Γενικά δημιουργήθηκαν σενάρια τα οποία καλύπτουν μερικές περιπτώσεις κυβερνητικών επιθέσεων. Υπάρχουν σενάρια με επίθεση που γίνεται με phishing e-mails, με μολυσμένο usb και επίθεση DDoS.

Κάθε σενάριο έχει τις λύσεις του. Οι λύσεις είναι αποθηκευμένες σε ένα αντικείμενο (solutions) στο οποίο είναι αποθηκευμένα τα ονόματα των καρτών, οι οποίες ορίζονται οι πιθανές λύσεις για κάθε στάδιο. Η συνάρτηση solution δέχεται ως παράμετρο ένα αντικείμενο obj που περιέχει το στάδιο, το σενάριο, και τις επιλεγμένες κάρτες του παίκτη. Στην συνέχεια ελέγχει αν έστω μια από τις επιλεγμένες κάρτες του χρήστη είναι σωστή και με βάση το αντικείμενο solutions επιστρέφει true ή false.

```
const solutions = {
  scenario1: {
    stage1: [1, 2, 3, 4],
    stage2: [8, 14, 10],
    stage3: [19, 20, 21, 22],
    stage4: [29, 30, 31],
    stage5: [38, 39],
    stage6: [48, 50, 51],
    stage7: [58, 59, 60, 61, 62]
  },
  scenario2: {
    stage1: [28, 41, 2],
    stage2: [8, 11, 12, 13],
    stage3: [20, 21, 23],
    stage4: [42, 30, 31],
    stage5: [37, 38, 43, 40],
    stage6: [48, 50, 51],
    stage7: [60, 61, 63]
  },
  scenario3: {
    stage1: [44, 45, 49, 52, 56],
    stage2: [57, 64],
    stage3: [65, 20, 21],
    stage4: [66, 67, 68],
    stage5: [69, 71, 40],
```

```
        stage6: [72, 74, 76, 77],
        stage7: [78, 79, 80]
    },
    scenario4: {
        stage1: [2, 5, 6],
        stage2: [15, 16, 81],
        stage3: [24, 25, 26, 82],
        stage4: [32, 33, 30],
        stage5: [46, 47, 37],
        stage6: [53, 54, 55],
        stage7: [70, 73, 58, 59]
    },
    scenario5: {
        stage1: [5, 2, 7],
        stage2: [9, 17, 18],
        stage3: [27, 83, 84],
        stage4: [34, 35, 36],
        stage5: [85, 40],
        stage6: [48, 53],
        stage7: [70, 58, 73, 75]
    }
};


var Solution = {
    checkSolution: function (obj) {
        let scenario = "scenario" + obj.scenario;
        let stage = "stage" + obj.stage;
        for (let i = 0; i < obj.selectedCards.length; i++) {
            for (let j = 0; j < obj.selectedCards.length; j++) {
                if (obj.selectedCards[i] == solutions[scenario][stage][j]) {
                    return true;
                }
            }
        }
    }
};

module.exports = Solution;
```

Ε.4 Chat για το παιχνίδι

Το chat αποτελεί μια επιπλέον βοήθεια για τον παίκτη για να επικοινωνεί με τους άλλους παίκτες σε περίπτωση που χρειαστεί βοήθεια για κάποιο στάδιο. Ο σκοπός δημιουργίας είναι καθαρά εκπαιδευτικός καθώς οι παίκτες μπορούν να βοηθηθούν μεταξύ τους. Το chat στο παιχνίδι είναι απλό, μόλις ο παίκτης γράψει κάτι τότε αυτό στέλνεται στον server και με την σειρά του, ο server το στέλνει στους υπόλοιπους συνδεδεμένους χρήστες.

Το σημείο που γράφει ο παίκτης είναι μια μικρή φόρμα με ένα input element και κουμπί submit. Η φόρμα στέλνει στον server το περιεχόμενο που έγραψε ο χρήστης μαζί με το event receiveMessage που περιέχει το όνομα του χρήστη που έστειλε το μήνυμα, και με την σειρά του ο server το στέλνει σε όλους τους συνδεδεμένους χρήστες. Στην συνέχεια, ο server στέλνει το όνομα του χρήστη μαζί με το event new message και το μήνυμα, σε όλους τους χρήστες. Οι παίκτες δέχονται τα δεδομένα, και αυτά τοποθετούνται σε έναν πινάκα html.

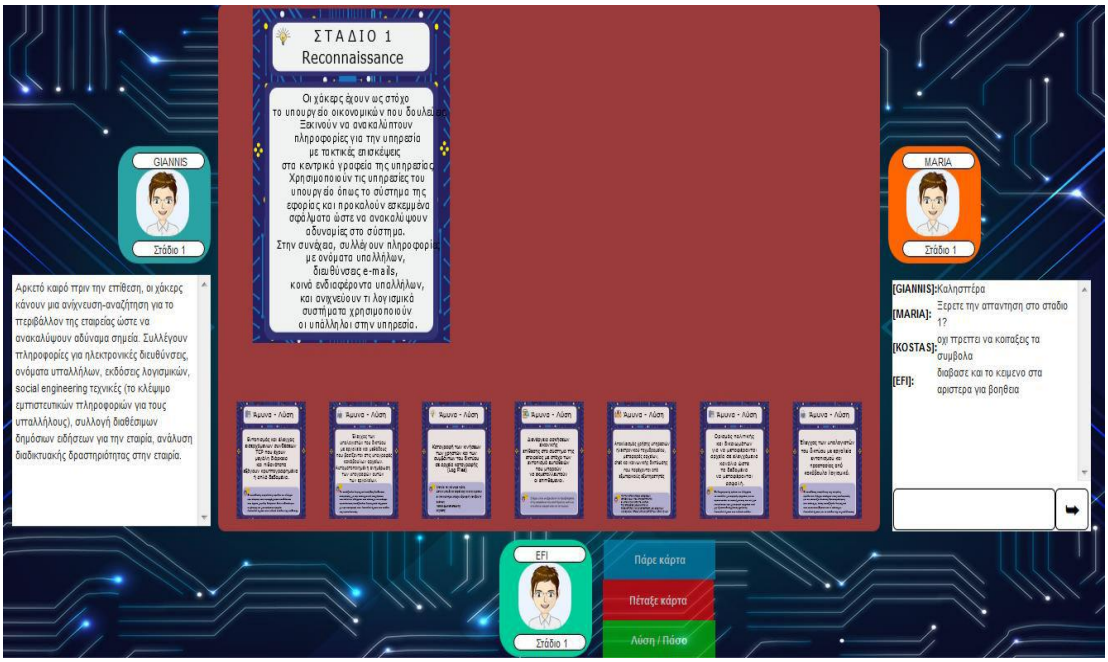
```
import React from "react";

class Chat extends React.Component {
   constructor(props) {
      super(props);
      this.state = {
         message: "",
         from: "",
         newMessage: "",
         allMessages: []
      };
      this.handleSubmit = this.handleSubmit.bind(this);
      this.handleInput = this.handleInput.bind(this);
   }

   componentDidMount() {
      MainApp.socket.on("newMessage", (data) => {
         this.addNewMessage(data);
         document.getElementById("messages").scrollTop =
document.getElementById("messages").scrollHeight;

      });
   }
```

```
  componentWillUpdate(nextProps, nextState, nextContext) {
    this.messages = nextState.allMessages.map((item, i) => {
      return (<tr key={i}>
        <td className={"sender"}>[{item.sender}]:</td>
        <td className={"message"}>{item.message}</td>
      </tr>)
    });
  }

  handleInput(event) {
    this.setState({message: event.target.value})
  }

  handleSubmit(event) {
    MainApp.socket.emit("receiveMessage", {sender: MainApp.player.username, message:
this.state.message});
    this.setState({message: ""})
    event.preventDefault();
  }

  addNewMessage(data) {
    const {sender, message} = data;
    let allMessages = this.state.allMessages;
    allMessages.push({sender, message});
    this.setState({allMessages: allMessages});
  }

  render() {
    return (
      <div id={"chatContainer"}>
        <div id={"messages"}>
          <table id={"messageTable"}>
            {this.messages}
          </table>
        </div>
        <div id={"inputDiv"}>
          <form onSubmit={this.handleSubmit} id={"newMessageForm"}>
            <input type="text" id={"chatInput"} value={this.state.message}
onChange={this.handleInput}/>
            <input type="submit" value="➥" id={"chatSubmit"}/>
```

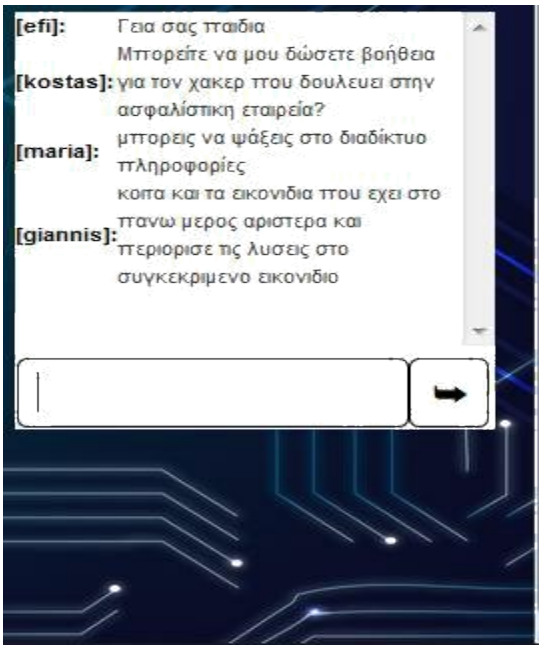
```
                </form>
            </div>
        </div>
    );
  };
}

module.exports = Chat;
```

Παρακάτω, υπάρχει η συνάρτηση στον server η οποία λαμβάνει και χειρίζεται τα μηνύματα δηλαδή τα δεδομένα που στέλνει ένας χρήστης.

```
client.on("receiveMessage", function (data) {
    io.sockets.emit("newMessage", data);
});
```



Εικόνα 15, Το chat πως φαίνεται σε όλους τους παίκτες



Εικόνα 16, Το Chat με την συνομιλία των παικτών

Ε.5 Εκπαιδευτική βοήθεια στον παίκτη

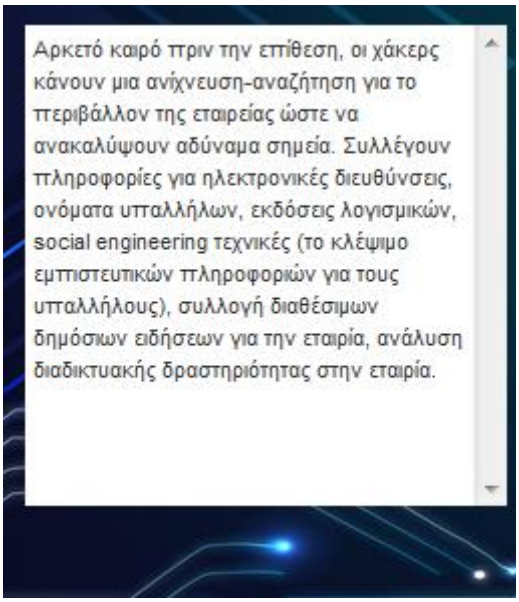
Το κομμάτι της εκπαιδευτικής βοήθειας είναι πολύ σημαντικό για το παιχνίδι με κάρτες. Σε κάθε στάδιο που βρίσκεται ο παίκτης εμφανίζεται στο κάτω μέρος της σελίδας το άσπρο πλαίσιο που περιλαμβάνει την εκπαιδευτική βοήθεια. Ανάλογα με το στάδιο που βρίσκεται ο παίκτης το κείμενο αλλάζει και επεξηγεί στους παίκτες τι συμβαίνει σε κάθε στάδιο. Ο κύριος σκοπός είναι οι παίκτες να διαβάσουν το κείμενο και να κατανοήσουν τον στόχο του κάθε σταδίου ώστε να μπορέσουν να λύσουν το στάδιο.

Για την δημιουργία της εκπαιδευτικής βοήθειας στο παιχνίδι, δημιουργήθηκε μια μεταβλητή η οποία λειτουργεί ως ένα αντικείμενο που μέσα βρίσκεται το κάθε στάδιο. Έπειτα, η συγκεκριμένη μεταβλητή καλείται στην τρίτη σελίδα του κώδικα και ανάλογα με το στάδιο που βρίσκεται ο παίκτης αλλάζει και το κείμενο. Για όλα τα εκπαιδευτικά σενάρια η επεξήγηση του σταδίου είναι η ίδια, διότι ο γενικός σκοπός του cyber kill chain δεν αλλάζει ανάλογα με το σενάριο.

```
var StagesExplained = {
   stage1: "Αρκετό καιρό πριν την επίθεση, ... στην εταιρία.",
   stage2: "Σε αυτό το στάδιο οι επιτιθέμενοι ... της επίθεσης.",
   stage3: "Μόλις οι χάκερς ... άτομα που βεβαιώνουν ότι το σύστημα είναι ενημερωμένο
με πρόσφατες εκδόσεις.\n",
   stage4: "Με την εκμετάλλευση της ... μιας αδυναμίας στο hardware ή στο software της
```

```
εταιρείας.\n",
    stage5: "Ο επιτιθέμενος ... να τρέχει.",
    stage6: "Δημιουργία καναλιού ... απομακρυσμένο έλεγχο.\n",
    stage7: "Μόνο όταν τα προηγούμενα ... τους στόχους τους.",
};

module.exports = StagesExplained;
```

Παρακάτω υπάρχουν εικόνες για την εκπαιδευτική βοήθεια στο παιχνίδι, αναλυτικά επεξηγείται το στάδιο ένα στην συγκεκριμένη περίπτωση.



Εικόνα 17, Εκπαιδευτική βοήθεια για το στάδιο 1

Ε.6 Χρονόμετρο για το παιχνίδι

Το χρονόμετρο δημιουργήθηκε στο παιχνίδι έτσι ώστε οι παίκτες να έχουν συγκεκριμένη χρονική διάρκεια που πρέπει να απαντήσουν κάθε φορά που έρχεται η σειρά τους. Με τον συγκεκριμένο τρόπο μειώνεται η ώρα που παίζει ο κάθε παίκτης και έτσι το παιχνίδι έχει μια πιο γρήγορη ροή. Σε κάθε παίκτη δίνονται τριάντα δευτερόλεπτα για να πετάξει μια κάρτα, να πάρει μια καινούργια και να δώσει την απάντηση που θεωρεί ότι είναι η σωστή.

Για την δημιουργία του χρονομέτρου δημιουργήθηκε η κλάση timer η οποία κληρονομεί τα component της react μαζί με τον κατασκευαστή της, και στην συνέχεια με την html δημιουργείται το timer.

Η συνάρτηση timer λειτουργεί στον server. Αρχικά αρχικοποιεί την μεταβλητή countdown με τριάντα. Έπειτα ξεκινάει το interval, αποτελεί το χρονικό διάστημα, που μειώνει την μεταβλητή countdown κατά ένα κάθε ένα δευτερόλεπτο και στέλνει στους παίκτες τον καινούργιο αριθμό του χρονομέτρου. Όταν η τιμή της μεταβλητής countdown είναι μηδέν ξανά αρχίζει από το τριάντα και στέλνει στους παίκτες ότι είναι η σειρά του επόμενου.

```
import React from "react";
class Timer extends React.Component {
   constructor(props) {
      super(props);
   }
   componentDidMount(){
   }
   render() {
      return (
         <div id="countdown">
            <div id="countdown-number">30</div>
            <svg>
               <circle id="svgCircle" className={"countdownAnimation"} r="49" cx="109"
cy="109"></circle>
            </svg>
         </div>
      );
   };
}

module.exports = Timer;
```

```
function timer(io) {
   var countdown = 30;
   interval = setInterval(() => {
      countdown--;
      if (countdown <= 0) {

         countdown = 30;
         io.sockets.emit('nextPlayer', Players.handlePlayerTurn());
      }
      io.sockets.emit("updateTimer", countdown);
```

```
    }, 1000);
}
```

Ε.7 Τα κουμπιά του παιχνιδιού

Το εκπαιδευτικό παιχνίδι στην τρίτη οθόνη αποτελεί και την τελική οθόνη που παίζουν οι παίκτες στο κάτω μέρος της σελίδας υπάρχουν τα τρία βασικά κουμπιά. Τα συγκεκριμένα κουμπιά αποτελούν την βασική λειτουργικότητα του παιχνιδιού. Ο παίκτης μόλις έρθει η σειρά του, πρώτα πρέπει να επιλέξει μια κάρτα που θεωρεί ότι δεν τον βοηθάει για να ολοκληρώσει το στάδιο που βρίσκεται, μετά την επιλογή της κάρτας επιλέγει το κουμπί "Πέταξε κάρτα". Μόλις η κάρτα απομακρυνθεί από το deck του παίκτη, τότε ο παίκτης πρέπει να επιλέξει "Πάρε κάρτα". Έπειτα στο deck του παίκτη εμφανίζεται μια νέα κάρτα η οποία επιστρέφει την συνάρτηση που αναλύθηκε παραπάνω. Τέλος, όταν ο παίκτης επιλέξει τις κάρτες που θεωρεί ότι είναι η σωστή απάντηση πατάει το κουμπί "Λύση-Πάσο". Το συγκεκριμένο κουμπί λειτουργεί ως απάντηση στο στάδιο.

Για τον έλεγχο των κουμπιών δημιουργήθηκε μια if-else η οποία λειτουργεί ως έλεγχος για την λειτουργία των τριών κουμπιών. Αρχικά, για το κουμπί "Πέταξε κάρτα" γίνεται έλεγχος για τον αριθμό των επιλεγμένων καρτών που έχει επιλέξει ο παίκτης καθώς και τον αριθμό καρτών που έχει ο παίκτης στο deck του. Επίσης ελέγχει αν το throwCounter είναι ίσο με μηδέν, αυτό σημαίνει ότι ο παίκτης δεν έχει πετάξει καμία κάρτα. Έτσι, μόλις πραγματοποιηθεί αυτός ο έλεγχος και γίνει θετικός τότε ενεργοποιείται το κουμπί "Πέταξε κάρτα" και ο παίκτης μπορεί να πετάξει την κάρτα που δεν χρειάζεται.

Αντίστοιχα λειτουργεί το κουμπί "Πάρε κάρτα" το οποίο ελέγχει τον αριθμό καρτών που έχει ο παίκτης στο χέρι του και πρέπει να είναι μικρότερο του επτά. Επίσης ελέγχει αν ο παίκτης έχει ξανά πάρει κάρτα. Αν ο συγκεκριμένος έλεγχος είναι θετικός τότε ενεργοποιείται το κουμπί "πάρε κάρτα".

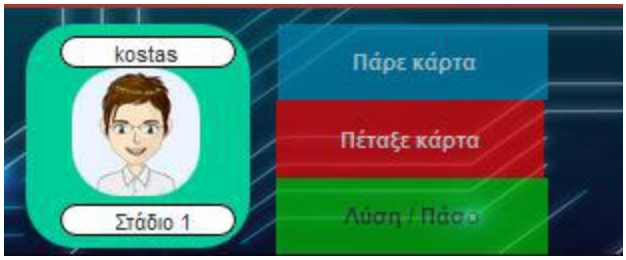
```
static toggleButtons(throwCounter, takeCounter) {
    $("#answer").attr("disabled", MainApp.playerCards.length < 7 || takeCounter!=1);

    if (MainApp.selectedCardsNum == 1 && MainApp.playerCards.length == 7
&& throwCounter == 0) {
        $("#buttonThrow").attr("disabled", false);
        window.throwButton = false;
```

```
    }
    else {
        $("#buttonThrow").attr("disabled", true);
        window.throwButton = true;
    }

    if (MainApp.playerCards.length < 7 && takeCounter == 0) {
        $("#buttonTake").attr("disabled", false);
        window.takeButton = false;
    }
    else {
        $("#buttonTake").attr("disabled", true);
        window.takeButton = true;
    }
}

client.on('giveCards', function (data) {
    client.emit('cards', deck.giveCards(), 1, 1, Tips["senario" + data]["st1"]);
});
```

Η παραπάνω συνάρτηση βρίσκεται στον server και στέλνει στους παίκτες τις κάρτες.

```
client.on('oneCard', function () {
    client.emit('takeOneCard', deck.oneCard());
});
```

Η παραπάνω συνάρτηση βρίσκεται στον server και δίνει μια κάρτα στον παίκτη που πάτησε το κουμπί "Πάρε κάρτα".



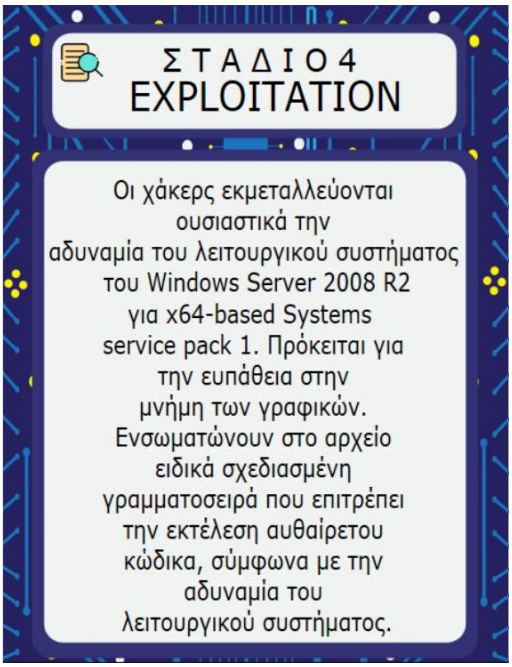
Εικόνα 18, Τα κουμπιά του παιχνιδιού

Ε.8 Οι εκπαιδευτικές κάρτες στάδια

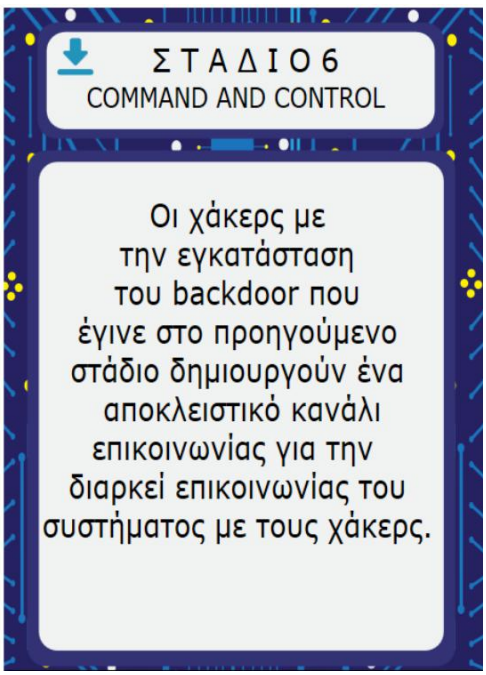
Το παιχνίδι περιλαμβάνει πέντε εκπαιδευτικά σενάρια από επιθέσεις των χάκερς σε εταιρείες και κυβερνητικούς οργανισμούς. Κάθε σενάριο περιλαμβάνει επτά εκπαιδευτικά στάδια από την μέθοδο cyber kill chain. Για τον σχεδιασμό των καρτών χρησιμοποιήθηκε ιδιαίτερη λεπτομέρεια καθώς το πίσω μέρος της κάρτας περιλαμβάνει ένα γραφικό σχεδιασμό από δίκτυο. Στο πάνω μέρος της κάρτας υπάρχει ο τίτλος του κάθε εκπαιδευτικού σταδίου καθώς και ένα εικονίδιο. Το εικονίδιο αποτελεί εκπαιδευτική βοήθεια για τους παίκτες. Κάθε κάρτα στάδιο έχει το ίδιο εικονίδιο ανάλογα με το στάδιο που βρίσκεται ο παίκτης. Στην συνέχεια, στο κύριο μέρος της κάρτας υπάρχει το κείμενο με το εκπαιδευτικό στάδιο που βρίσκεται ο κάθε παίκτης και καλείται να λύσει.

Παρακάτω, υπάρχει το πρώτο εκπαιδευτικό σενάριο για το παιχνίδι με τις κάρτες, από το στάδιο ένα έως το στάδιο επτά.

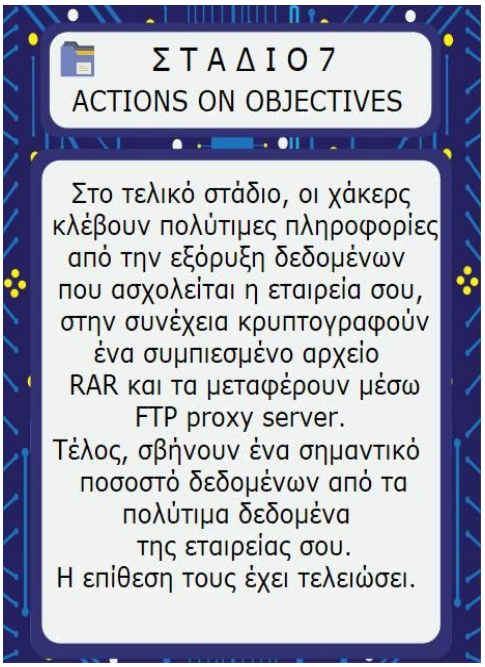
Εικόνα 19, Στάδιο 1 και στάδιο 2 από το σενάριο 1



Εικόνα 20, Στάδιο 3 και στάδιο 4 από το σενάριο 1



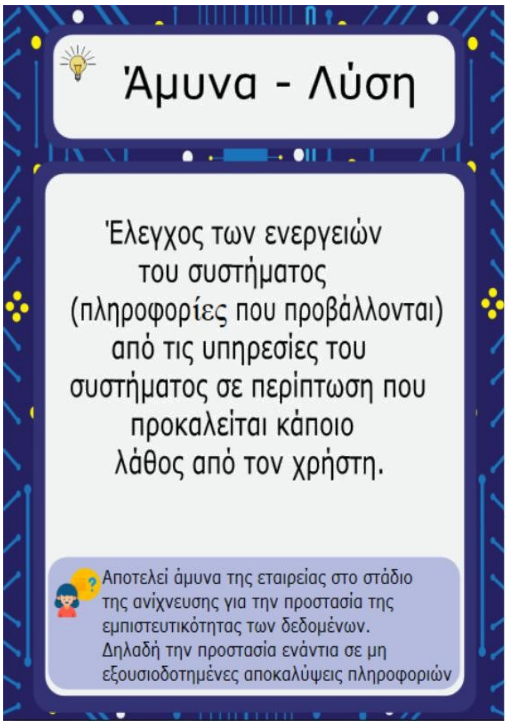
Εικόνα 21, Στάδιο 5 και στάδιο 6 από το σενάριο 1

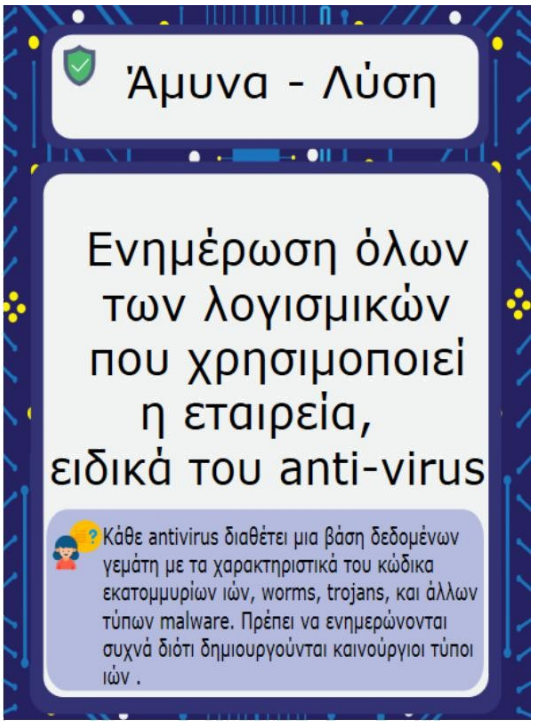


Εικόνα 22, Στάδιο 7 από το σενάριο 1

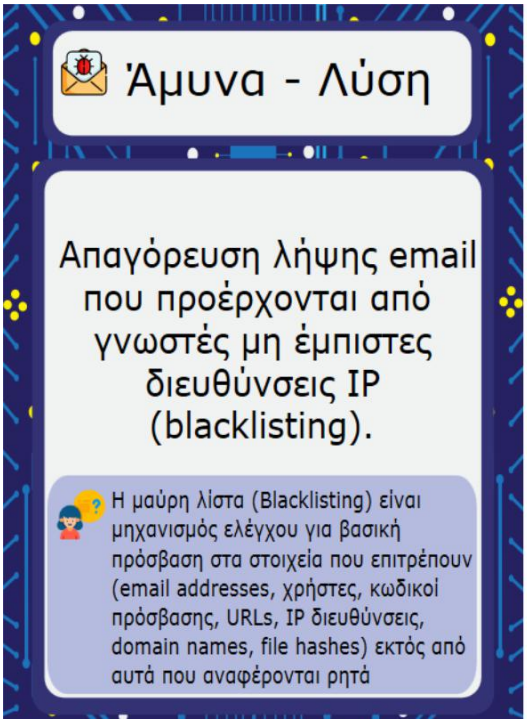
Κάθε στάδιο έχει την δική του λύση και οι παίκτες καλούνται να ανακαλύψουν τις λύσεις για να περάσουν στο επόμενο στάδιο. Οι εκπαιδευτικές κάρτες λύσεις ή αλλιώς το deck του παιχνιδιού, περιλαμβάνει 85 κάρτες. Στο deck με τις κάρτες δεν υπάρχουν διπλές ίδιες κάρτες καθώς οι λύσεις του παιχνιδιού υπάρχουν σε πολλά στάδια από τα σενάρια. Κάθε κάρτα λύση περιλαμβάνει τον ίδιο γραφικό σχεδιασμό με τις κάρτες στάδιο, το οποίο είναι το γραφικό με το δίκτυο. Επίσης, ο τίτλος της κάθε κάρτας-λύσης είναι η άμυνα-λύση για να κατανοεί ο παίκτης ότι με αυτές τις κάρτες πρέπει να βρει την λύση για το παιχνίδι. Σε κάθε τίτλο υπάρχει το ίδιο εικονίδιο που έχει τοποθετηθεί στις κάρτες στάδια. Ο λόγος είναι ότι κάθε κάρτα άμυνα περιλαμβάνει αυτό το εικονίδιο σαν βοήθεια στον παίκτη για να μειώνει το εύρος των σωστών απαντήσεων για το κάθε στάδιο. Λειτουργεί περισσότερο ως υποσυνείδητη βοήθεια στον παίκτη. Στην συνέχεια, στο κεντρικό κείμενο της κάθε κάρτας υπάρχει η λύση. Στο κάτω μέρος της κάθε κάρτας υπάρχει το μπλε πλαίσιο με το εικονίδιο το οποίο λειτουργεί ως επεξήγηση σε κάθε κάρτα-λύση για τον παίκτη. Επίσης, οι παίκτες με την συγκεκριμένη βοήθεια μαθαίνουν περισσότερα για κάθε κάρτα λύση.

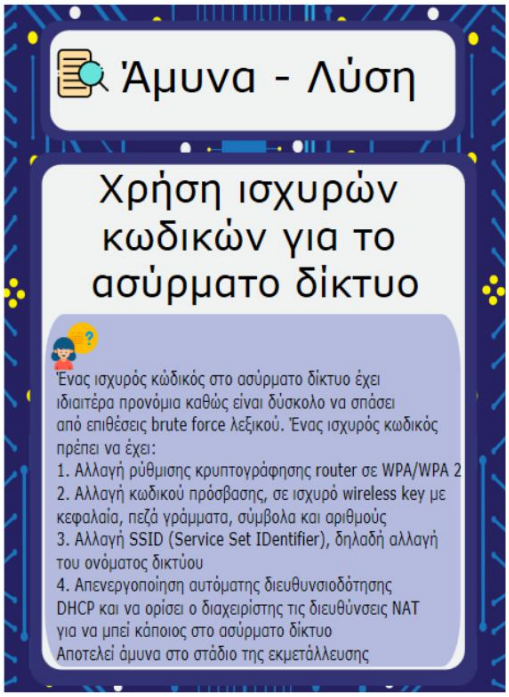
Παρακάτω, υπάρχουν ενδεικτικές λύσεις από κάθε στάδιο με τα διαφορετικά εικονίδια που επεξηγήθηκαν παραπάνω:



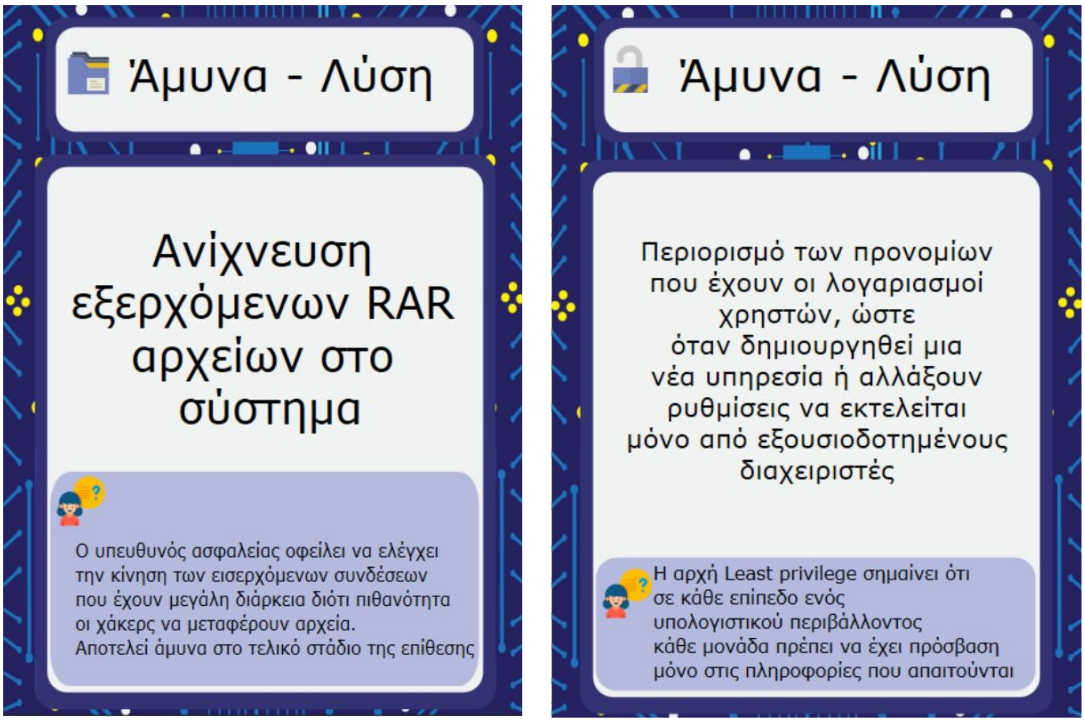


Εικόνα 23, Κάρτα-λύση για το παιχνίδι

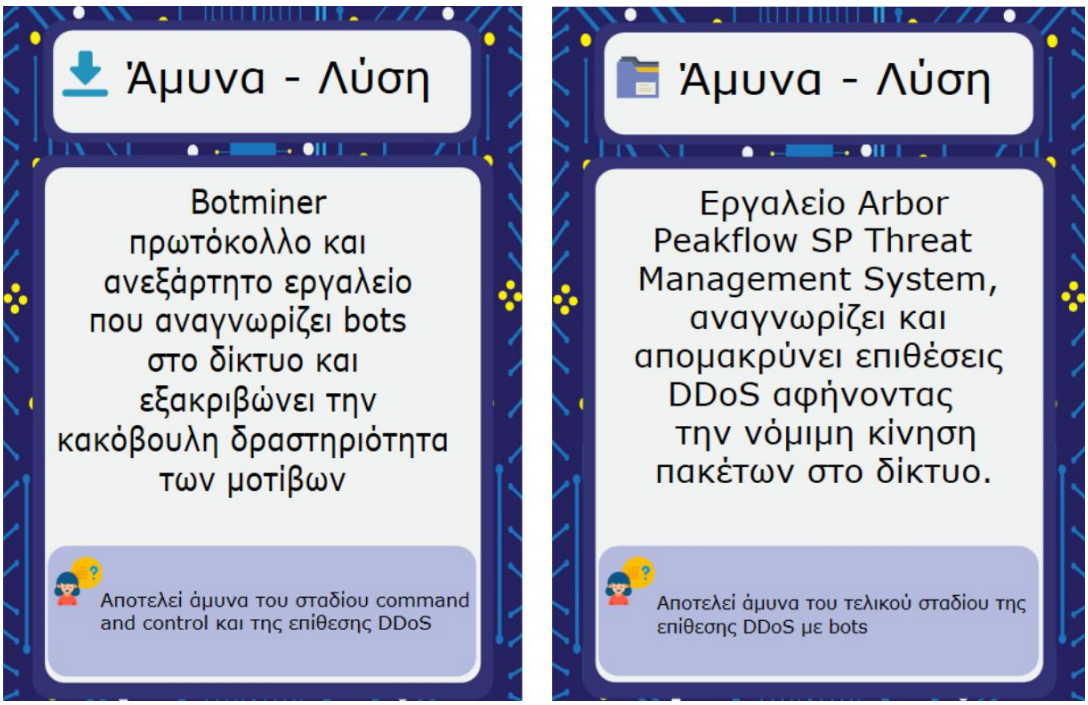




Εικόνα 24, Κάρτα-λύση για το παιχνίδι



Εικόνα 25, Κάρτα-λύση για το παιχνίδι



Εικόνα 26, Κάρτα-λύση για το παιχνίδι

Εικόνα 27, Κάρτα-λύση για το παιχνίδι

Κεφάλαιο ΣΤ'

Επίλογος

ΣΤ.1 Συμπέρασμα

Οι επιχειρήσεις και οι οργανισμοί οφείλουν να έχουν ως προτεραιότητα την ασφάλεια των συστημάτων και να δημιουργήσουν στρατηγικά μοτίβα άμυνας για τα συστήματα τους, καθώς βρίσκονται σε έναν κυβερνητικό πόλεμο. Η άμυνα του κέντρο δεδομένων των επιχειρήσεων είναι ζωτικής σημασίας για την επιβίωση της επιχείρησης. (Oracle Corporetion, 2018)

ΣΤ.2 Προτάσεις για βελτίωση

Το παιχνίδι με τις κάρτες χρησιμεύει ως ένα εκπαιδευτικό εργαλείο για να κατανοήσει ο παίκτης την βασική μεθοδολογία του cyber kill chain με πραγματικά παραδείγματα. Βέβαια υπάρχουν πολλά περιθώρια για να βελτιωθεί το παιχνίδι. Μια βελτίωση που θα βοηθούσε τους παίκτες να λύσουν γρήγορα τα σενάρια είναι η χρήση του καθηγητή μέσα στην συνομιλία. Ο κάθε παίκτης θα μπορούσε να ρωτάει τον καθηγητή στην συνομιλία και αυτός να μπορεί να απαντάει και να εμφανίζει την απάντηση του μόνο στον παίκτη με την απορία. Επίσης, άλλη μια βελτίωση είναι προστεθούν περισσότερα σενάρια πέρα των πέντε.

Μια ακόμη προσθήκη θα ήταν το ακουστικό κομμάτι που αποτελεί σημαντικό πλεονέκτημα και θα ωθεί τους παίκτες να παίζουν με περισσότερη όρεξη. Ακόμη, το παιχνίδι θα μπορούσε να μεταφραστεί και σε άλλες γλώσσες όπως τα αγγλικά για να προσεγγίσει μεγαλύτερο εύρος κοινού. Τέλος θα μπορούσε να ενταχθεί στο κυρίως παιχνίδι διάφορες κινήσεις όπως όταν δίνει στον παίκτη μια καινούργια κάρτα, όταν του δίνεται καινούργιο σενάριο ή όταν δίνει την λύση.

Βιβλιογραφία

Vik, E. (2009, Σεπτέμβριος) State of the art report on serious games: Blurring the lines between recreation and reality. The euro graphics Association σσ 1-7

Susi T., Johannesson, M., & Backlund P. (2007) Serious Games An overview. Technical report HS-IKITR-07-001 School Of Humanities and Informatics, University Of Skovde, Sweden σσ. 1-24

Xinogalos S., Satratzemi M. (2004, July 21-25). Introducing Novices to Programming: A review of Teaching Approaches and Education Tools. Proceedings of the 2nd International Conference on Education and Information Systems, Technologies and Applications, EISTA, 2004, Orlando, Florinda, USA, July 21-25 σσ 60-65

Lance Spitzner,(2018, Φεβρουάριος) Applying Security Awareness to the Cyber Kill Chain Ανάκτηση από https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain (Τελευταία επίσκεψη: 4/2018)

Tarun Yadav, Arvind Mallari Rao (2015, Αύγουστος),Technical aspects of cyber kill chain, Conference Paper

Oracle Linux, (2017, Δεκέμβριος) Anatomy of a Cyber Attack: The Lifecycle of a Security Breanch, Oracle White Paper

Control-alt-hack http://www.controlalthack.com/ (Τελευταία επίσκεψη: 20/2/2018)

Tamara Denning, Tadayoshi Kohno, Adam Shostack, (2012, July), Control-Alt-HackTM: A Card Game for Computer Security Outreach, Education, and Fun, Department of Computer Science and Engineering University of Washington Technical Report UW-CSE-12-07-01

Laurie Williams, Andrew Meneely, Grant Shipley (2010, May-June), Protection Poker: The New Software Security "Game", North Carolina State University, paper

Laurie Williams, (2012, August), Protection Poker: An agile Security Game, North Carolina, State University, Conference presentation

Shane Stelgar, (2016, August), Maelstrom: Are you playing with a full deck? Using an Attack Lifecycle to Educate Demonstrate and Evangelize, Def Con 24

Cyber Threat Defender, (2019), Ανάκτηση από http://cias.utsa.edu/ctd.php (Τελευταία επίσκεψη: 26/1/2019)

Hannah Hickey, (2012, July), Control Alt Hack game let players try their hand at computer security, Education article, ανάκτηση από http://www.washington.edu/news/2012/07/24/control-alt-hack-game-lets-players-try-their-hand-at-computer-security/, (Τελευταία επίσκεψη: 20/2/2018)

Deloitte, (2017), 7 stages of Cyber Kill Chain, Supplementary Reading

Maria Kordaki, A 7-step Modeling Methodology for the design of Education constructivist computer card games, November 2016, pp.114-123, University of Aegean

Maria Kordaki, A computer card game for the learning of basic aspects of the binary system in primary education Design and pilot evaluation, 06-2010

Vanessa Wang, Frank Salim, Peter Moskovits (2012), The Definitive Guide to HTML5 Websockets Builds Real time applications with HTML5, Apress, Book

Maria Kordaki, A computer card game for the learning of basic aspects of the binary system in primary education Design and pilot evaluation, 06-2010

Crawford, C. (1982). The art of computer game design, available as a free download from a site maintained by Washington State University at www.vancouver.wsu.edu/fac/peabody/game-book/ Coverpage.html Accessed 10/02/ 2018.

Fisch, M. S. (2005). Making educational computer games educational. Proceedings of the 2005 conference on Interaction, design and children, Boulder, Colorado, pp. 56–61.

Hays, R. T. (2005). The effectiveness of instructional games: a literature review and discussion. Storming Media, pp 1–63

Kirriemuir, J., & McFarlane, C.A. (2004). REPORT 8: Literature Review in Games & Learning. http:// www.futurelab.org.uk/research/reviews/08_16.htm

McFarlane, A., & Sakellariou, S. (2002). The role of ICT in science education. Cambridge Journal of Education, 32(2), 219–232.

Kamii, C., & DeVries, R. (1980). Group games in early education: Implications of Piaget's theory. Washington: National Association for the Education of Young Children

Oblinger, D. (2004). The next generation of educational engagement. Journal of Interactive Media in Education, 2004(8), 1–18.

Prensky, M. (2001). Digital game-based learning. New York: Mc Graw-Hill

Rajaravivarma, R. (2005). A games-based approach for teaching the introductory programming course. Inroads ACM SIGCSE Bulletin, 37(4), 98–102.

Randel, J., Morris, B., Wetzel, C., & Whitehill, B. (1992). The effectiveness of games for educational purposes: a review of recent research. Simulation and Gaming, 23(3), 261–276.

Smith, D. R., & Muhro, E. (2009). Educational card games. Physics Education, 44(5), 479–483

Gardinger, A. (1987). Discovering mathematics: The art of investigation. NY: Oxford University Press

McGraw, I., Yoshimoto, B., & Seneff, S. (2009). Speech-enabled card games for incidental vocabulary acquisition in a foreign language. Speech Communication, 51, 1006–1023