ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ - WEBINTELLIGENCE

Ασφάλεια Συστημάτων Τηλεκπαίδευσης: Συγκριτική αξιολόγηση

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Βάιου Ζιώγα

Επιβλέπων : **Χρήστος Ηλιούδης**
Καθηγητής ΔΙ.ΠΑ.Ε.

Θεσσαλονίκη, Φεβρουάριος 2023

Η σελίδα αυτή είναι σκόπιμα λευκή.

Υπόδειγμα φύλλου τίτλου (μπροστινή σελίδα) του αντιτύπου ΜΔΕ

ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ – WEB INTELLIGENCE

Ασφάλεια Συστημάτων Τηλεκπαίδευσης: Συγκριτική αξιολόγηση

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Βάιου Ζιώγα

Επιβλέπων : **Χρήστος Ηλιούδης**
Καθηγητής ΔΙ.ΠΑ.Ε.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή στις Choose a date.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Όνομα Επώνυμο	Όνομα Επώνυμο	'Ονομα Επώνυμο
Choose an item. ΔΙ.ΠΑ.Ε.	Choose an item. ΔΙ.ΠΑ.Ε.	Choose an item. ΔΙ.ΠΑ.Ε.

Θεσσαλονίκη, Choose a date

(Υπογραφή)

.....

Click here to enter text.

Click here to enter text.

Περίληψη

Τα συστήματα τηλεκπαίδευσης αποτέλεσαν βασική επιλογή των εκπαιδευτικών ιδρυμάτων για τη συνέχιση της μαθησιακής διαδικασίας κατά την περίοδο της καραντίνας του COVID-19, καθώς τα περισσότερα σχολεία και κολέγια είχαν εφαρμόσει διαδικτυακά μαθήματα για να περιορίσουν την εξάπλωση του ιού. Η άμεση ανάγκη, όμως, για την εφαρμογή μιας πλατφόρμας τηλεκπαίδευσης είχε ως αποτέλεσμα θέματα ασφαλείας να μη λάβουν τη δέουσα προσοχή. Αντίθετα οι κυβερνοεπιθέσεις έχουν γίνει πιο συχνές από την εμφάνιση του COVID-19, καθώς τα δεδομένα που συλλέγουν και αποθηκεύουν οι πλατφόρμες προσελκύουν τους κακόβουλους εισβολείς.

Σκοπός αυτής της μεταπτυχιακής διπλωματικής εργασίας είναι η συγκριτική αξιολόγηση των συστημάτων τηλεκπαίδευσης από την οπτική της ασφάλειας. Ειδικότερα εξετάζονται ζητήματα ασφαλείας, ευπάθειες και πιθανές επιθέσεις στον κυβερνοχώρο που έχουν εντοπιστεί λόγω της χρήσης των πιο δημοφιλών συστημάτων τηλεκπαίδευσης (π.χ. Zoom, Microsoft Teams, Moolde και Blackboard). Αρχικά παρουσιάζονται τα χαρακτηριστικά ζητήματα ασφαλείας και οι τύποι επιθέσεων και ευπαθειών που παρατηρούνται στα συστήματα τηλεκπαίδευσης και τα πιθανά προβλήματα που ανακύπτουν. Για την κατηγοριοποίηση των επιθέσεων χρησιμοποιήθηκε η ταξινόμηση των πιο κοινών ευπαθειών εφαρμογών Ιστού που παρέχονται από το Common Weakness Enumeration (CWE) και το Open Web Application Security Project (OWASP). Ακολούθησε η συγκριτική ανάλυση των σύγχρονων και ασύγχρονων συστημάτων τηλεκπαίδευσης σύμφωνα με τη βάση δεδομένων ευπαθειών CVE Details. Επίσης προτείνονται στρατηγικές μετριασμού των κινδύνων για τη βελτίωση της ασφάλειας, ενώ παράλληλα δίνονται συμβουλές στους χρήστες των συστημάτων για ασφαλή χρήση των συστημάτων τηλεκπαίδευσης. Τέλος ορίζονται οι βέλτιστες πρακτικές για την ασφάλεια σε συστήματα τηλεδιάσκεψης.

Λέξεις Κλειδιά: Τηλεκπαίδευση, ασφάλεια, ευπάθεια, τηλεδιάσκεψη, αντίμετρα

Η σελίδα αυτή είναι σκόπιμα λευκή.

Abstract

E-learning systems have been a key choice of educational institutions to continue the learning process during the COVID-19 quarantine period, as most schools and colleges have implemented online courses to curb the spread of the virus. However, the immediate need to implement an e-learning platform resulted in security issues not receiving due attention. Instead, cyberattacks have become more common since the emergence of COVID-19, as the data collected and stored by platforms attracts malicious attackers.

The purpose of this master's thesis is the comparative evaluation of distance education systems from the perspective of security. In particular, security issues, vulnerabilities and potential cyber attacks that have been identified due to the use of the most popular e-learning systems (eg Zoom, Microsoft Teams, Moolde and Blackboard) are examined. First, the typical security issues and types of attacks and vulnerabilities observed in e-learning systems and the possible problems that arise are presented. The classification of the most common web application vulnerabilities provided by the Common Weakness Enumeration (CWE) and the Open Web Application Security Project (OWASP) was used to categorize the attacks. This was followed by the comparative analysis of synchronous and asynchronous e-learning systems according to the CVE Details vulnerability database. Risk mitigation strategies are also proposed to improve security, while at the same time advice is given to users of the systems for safe use of e-learning systems. Finally, the best practices for security in videoconferencing systems are

Keywords: e-learning, security, vulnerability, teleconferencing, countermeasures

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Συντομογραφίες

ΑεξΑΕ	Ανοικτή εξ Αποστάσεως Εκπαίδευση
εξΑΕ	εξ Αποστάσεως Εκπαίδευση
ODL	Open & Distance Learning
LMS	Learning Management Systems
MOOC	Massive Open Online Courses
Moodle	Modular Object-Oriented Dynamic Learning
XSS	Cross-site Scripting
SSL	Secure Socket Layer
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
GDPR	Γενικός Κανονισμός για την Προστασία Δεδομένων
BYOD	Bring Your Own Device
OWASP	Open Web Application Security Project
CWE	Common Weakness Enumeration
CVE	Common Vulnerability and Exposures
CVSS	Common Vulnerability Scoring System
DRM	Digital rights management
HIPAA	Health Insurance Portability and Accountability Act

1

Εισαγωγή

1.1 Η σπουδαιότητα της ασφάλειας των συστημάτων τηλεκπαίδευσης

Η ζωή των ανθρώπων έχει αλλάξει δραματικά από την εξέλιξη της τεχνολογίας. Υπολογιστές, κινητές συσκευές, δίκτυα υψηλής ταχύτητας και άλλα τεχνολογικά μέσα δίνουν τη δυνατότητα στους ανθρώπους να συμμετέχουν σε διάφορες δραστηριότητες ανεξαρτήτου τόπου και χρόνου. Γραφειοκρατικές διαδικασίες, αγορές και άλλες καθημερινές εργασίες δεν απαιτούν πλέον την φυσική παρουσία. Αναπόφευκτα και ο εκπαιδευτικός τομέας επηρεάζεται σε μεγάλο βαθμό από την πρόοδο της τεχνολογίας [1].

Τα συστήματα τηλεκπαίδευσης χρησιμοποιούνται όλο και περισσότερο από μαθητές και εκπαιδευτικούς σε όλο τον κόσμο σχεδόν σε καθημερινή βάση. Παρέχουν στους εμπλεκόμενους μια ευκολότερη μέθοδο επικοινωνίας που βοηθά την εκπαιδευτική διαδικασία όχι απλώς με την επικοινωνία αλλά και με κοινή χρήση εγγράφων, κουίζ, εκπαιδευτικών βίντεο, σημειώσεων και βαθμολογίας. Τα συστήματα τηλεκπαίδευσης δίνουν τη δυνατότητα σε ανθρώπους (όχι απαραίτητα μόνο μαθητές και φοιτητές) που αναζητούν γνώση και επιθυμούν να εκπαιδευτούν σε οποιοδήποτε θέμα να έχουν πρόσβαση στην εκπαίδευση απλώς μέσω υπολογιστή [2].

Τα συστήματα τηλεκπαίδευσης έχουν ανοίξει της πόρτες της γνώσης και έχουν δώσει ευκαιρίες σε ανθρώπους απ’ όλο τον κόσμο. Επίσης έχουν αλλάξει και βελτιώσει τον τρόπο μάθησης και

διδασκαλίας και είναι πολύ διαδεδομένα ανά τον κόσμο για την παροχή ποιοτικής εκπαίδευσης. Αυτού του είδους τα συστήματα εξαρτώνται εξ ολοκλήρου από το διαδίκτυο για την αναζήτηση πληροφοριών και ανταλλαγή γνώσεων [3].

Για την εκτέλεσή τους τα συστήματα τηλεκπαίδευσης βασίζονται και εξαρτώνται από το Διαδίκτυο. Ωστόσο, είναι γνωστό ότι υπάρχουν πολλές παράνομες δραστηριότητες και απειλές για την ασφάλεια που λαμβάνουν χώρα στο Διαδίκτυο. Αυτό έχει ως αποτέλεσμα τα συστήματα τηλεκπαίδευσης να είναι αναπόφευκτα εκτεθειμένα σε κινδύνους, συνεχείς απειλές και επιθέσεις για την ασφάλεια. Δυστυχώς όμως, πολλά σχολεία και πανεπιστήμια βιάζονται να υιοθετήσουν συστήματα τηλεκπαίδευσης χωρίς προσεκτικό σχεδιασμό και χωρίς ενδελεχή κατανόηση των πτυχών ασφάλειας [4].

Η έλευση της πανδημίας του COVID-19 την άνοιξη του 2020 διέκοψε πολλές από τις ανθρώπινες δραστηριότητες με αποτέλεσμα το κλείσιμο των εκπαιδευτικών ιδρυμάτων σε πολλές χώρες. Καθώς επικράτησε η πανδημία του COVID-19 τα πανεπιστήμια και τα σχολεία σε όλο τον κόσμο αναγκάστηκαν να κλείσουν τις πόρτες τους. Μέχρι τις 29 Απριλίου 2020, περισσότερα από 1,2 δισεκατομμύρια παιδιά σε 186 χώρες επλήγησαν από το κλείσιμο των σχολείων [5]. Η ζωή όμως έπρεπε να συνεχιστεί με κάποιο τρόπο. Η κοινωνική απόσταση προτάθηκε ως βασικό μέτρο για τη μείωση της εξάπλωσης του ιού και για τη συνέχεια των δραστηριοτήτων προτάθηκε η απομακρυσμένη εργασία. Είναι γνωστό ότι, όταν η εκπαίδευση διακόπτεται για κάποιο χρονικό διάστημα, τότε οι μαθητές δυσκολεύονται να επιστρέψουν στην εκπαιδευτική διαδικασία, γι' αυτό στον τομέα της εκπαίδευσης προτάθηκε η αξιοποίηση διάφορων εναλλακτικών μεθόδων διδασκαλίας που βασίζονται στο Διαδίκτυο έτσι ώστε, χωρίς τον κίνδυνο εξάπλωσης του ιού, οι μαθητές να παρακολουθήσουν τα μάθημα τους.

Ως εκ τούτου, οι φορείς εκπαίδευσης επέλεξαν γρήγορα διαδικτυακά μαθήματα, συμπεριλαμβανομένων σχολείων, πανεπιστημίων, σεμιναρίων και κέντρων κατάρτισης. Τα συστήματα τηλεκπαίδευσης υποστηρίζουν τη διδασκαλία χωρίς τη φυσική παρουσία των συμμετεχόντων στον ίδιο χώρο με αποτέλεσμα την αλματώδη αύξηση τους κατά την διάρκεια της πανδημίας. Πολλοί εκπαιδευτικοί τα έχουν χρησιμοποιήσει πολύ, ειδικά τις σύγχρονες πλατφόρμες επειδή μπορούσαν να προσομοιώσουν το μάθημα που λαμβάνει χώρα σε μια αίθουσα διδασκαλίας και να επικοινωνήσουν απευθείας με τους μαθητές. Τα ευρήματα αυτά ισχύουν για όλες τις βαθμίδες εκπαίδευσης (πανεπιστήμιο, γυμνάσιο και δημοτικό) και κάθε ηλικίας μαθητές (ενήλικες, έφηβοι και ανήλικοι).

Σύντομα έγινε σαφές ότι πολλά σχολεία όταν άρχισαν να μεταβαίνουν στην έκτακτης ανάγκης εξ αποστάσεως εκπαίδευση δεν ήταν έτοιμα για το είδος της πλήρους απασχόλησης ψηφιακής εκπαίδευσης που απαιτούνταν. Οι μαθητές αλλά ακόμη και εκπαιδευτικοί δεν είχαν όλη την απαιτούμενη τεχνολογία, από υπολογιστές έως σταθερή σύνδεση στο Διαδίκτυο. Παράλληλα

οι εκπαιδευτικοί και οι γονείς ανησυχούσαν ότι οι μαθητές αναπόφευκτα θα μείνουν πίσω στην μόρφωσή τους.

Αν και οι περισσότεροι συμφωνούν για τα πολλά οφέλη που προσφέρουν τα συστήματα τηλεκπαίδευσης, ορισμένοι υποστηρίζουν και τα μειονεκτήματα που τα συνοδεύουν δεν είναι λίγα με πιο σημαντικό να είναι αναδεικνύονται οι κίνδυνοι ασφάλειας. Οι περισσότεροι εκπαιδευτικοί δεν είχαν επαρκή εμπειρία στα συστήματα τηλεκπαίδευσης και έπρεπε γρήγορα να προσαρμοστούν στις ιδιαιτερότητες και τα εργαλεία της εξ αποστάσεως εκπαίδευσης [6]. Επιπλέον σε πολλά σχολεία και πανεπιστήμια δεν είχαν εφαρμόσει κατάλληλα μέτρα κυβερνοασφάλειας, με αποτέλεσμα να υπάρχει αυξημένος κίνδυνος κυβερνοεπιθέσεων στις διαδικτυακές τάξεις. Δυστυχώς, η ασφάλεια και η προστασία των μαθητών έχουν αντιμετωπιστεί βιαστικά για την εξεύρεση λύσεων, ειδικά σε χώρες όπου οι ΤΠΕ στην εκπαίδευση δεν ήταν πολύ ενεργές.

Η αύξηση της τηλεκπαίδευσης λόγω της πανδημίας COVID-19, είχε ως αποτέλεσμα και την αύξηση των επιθέσεων στον κυβερνοχώρο και των παραβιάσεων δεδομένων [7]. Τα εμπλεκόμενα μέρη (μαθητές, εκπαιδευτικοί, διαχειριστές) δεν ήταν προετοιμασμένα για μια τέτοια πρόκληση. Αυτός είναι λόγος που προέκυψαν πολλά προβλήματα τα οποία περιλάμβαναν μαθητές που δεν είχαν τον απαραίτητα τεχνολογικό εξοπλισμό και γρήγορη σύνδεση στο διαδίκτυο, μη εκπαιδευμένους καθηγητές για εξ' αποστάσεως εκπαίδευση και χρήση τεχνολογιών και λογισμικών των οποίων δεν είχαν γίνει οι απαραίτητοι έλεγχοι για τρωτά σημεία. Επίσης δεν υπήρχαν συγκεκριμένες πολιτικές ασφαλείας στα εκπαιδευτικά ιδρύματα ώστε να προστατευθούν οι μαθητές και οι εκπαιδευτικοί αλλά και τα περιουσιακά στοιχεία των ιδρυμάτων Στην πραγματικότητα, τον Ιούνιο του 2020, η Microsoft Security Intelligence ανέφερε ότι ο κλάδος της εκπαίδευσης αντιπροσώπευε το 61% των 7,7 εκατομμυρίων περιστατικών κακόβουλου λογισμικού που αντιμετώπισαν οι επιχειρήσεις τις προηγούμενες 30 ημέρες – περισσότερο από οποιονδήποτε άλλο τομέα [8].

Εν τω μεταξύ, τα προσωπικά δεδομένα εμπλέκονται στην διαδικτυακή μάθηση και τα μεταδεδομένα που δημιουργούνται είναι ευαίσθητα και προσελκύουν τους χάκερ. Στη διαδικτυακή μάθηση, που εφαρμόζεται με τα συστήματα τηλεκπαίδευσης, ασφάλεια σημαίνει ότι «οι πόροι μάθησης είναι διαθέσιμοι και χωρίς προβλήματα σε όλους τους εξουσιοδοτημένους χρήστες όταν χρειάζονται» [9]. Επειδή η διαδικτυακή μάθηση πραγματοποιείται μέσω του Διαδικτύου, στόχος πειρατείας ή επιθέσεων μπορεί να είναι κάθε στοιχείο στο διαδικτυακό σύστημα εκμάθησης και αυτό αποτελεί απειλή για τα εκπαιδευτικά περιουσιακά στοιχεία που μπορεί να οδηγήσει σε μη εξουσιοδοτημένη τροποποίηση ή/και καταστροφή. Τα συστήματα τηλεκπαίδευσης πρέπει να λαμβάνουν υπόψη τους εγγενείς κινδύνους ασφάλειας στο Διαδίκτυο, όπως η πλαστοπροσωπία, ο ανεπαρκής έλεγχος ταυτότητας, και η κλοπή ταυτότητας. Γίνεται σαφές ότι τα συστήματα τηλεκπαίδευσης έχουν

προσελκύσει την προσοχή των εγκληματιών του κυβερνοχώρου. Ο κίνδυνος είναι μεγάλος καθώς οι λειτουργίες και τα χαρακτηριστικά των συστημάτων τηλεκπαίδευσης γίνονται πιο πολύπλοκα [4].

Όσοι χρησιμοποιούν συστήματα τηλεκπαίδευσης θα πρέπει να προστατεύουν τα δεδομένα από μη εξουσιοδοτημένους χρήστες. Τα εκπαιδευτικά περιουσιακά στοιχεία, όπως μαθησιακό υλικό, γραπτά ερωτήματα, διαλέξεις ήχου και βίντεο, πιστοποιητικά κ.λπ., που διαμοιράζονται από τους εκπαιδευτικούς και τα ιδρύματα πρέπει να προστατεύονται από την καταστροφή. Το πρωταρχικό μέλημα αυτής της εργασίας είναι να εντοπίσει σοβαρές απειλές και ευπάθειες για τα συστήματα τηλεκπαίδευσης και να προτείνει καλές πρακτικές και μηχανισμούς προστασίας μέσω της πιστοποίησης ταυτότητας, της εμπιστευτικότητας, της ακεραιότητας των δεδομένων και της διατήρησης της ιδιωτικής ζωής [10].

1.2 Σκοπός και στόχοι της εργασίας

Η αύξηση των χρηστών συστημάτων τηλεκπαίδευσης έχει ως φυσικό επακόλουθο την αύξηση του αριθμού των επιθέσεων γι' αυτό η ασφάλεια και προστασία των περιουσιακών πόρων είναι απαραίτητη. Τα ερωτήματα που προκύπτουν είναι: Ποιες είναι οι απειλές που αντιμετωπίζουν τα συστήματα τηλεκπαίδευσης; Ποια είναι τα τρωτά σημεία που αξιοποιούνται από τους επιτιθέμενους; Είναι τα συστήματα τηλεκπαίδευσης αρκετά ασφαλής; Ποιοι είναι οι κίνδυνοι για την ασφάλεια; Ποιες είναι οι επιπτώσεις των επιθέσεων; Το πρωταρχικό μέλημα αυτής της εργασίας είναι να εντοπίσει σοβαρές απειλές για τα συστήματα τηλεκπαίδευσης και να προτείνει ένα πλαίσιο προστασίας μέσω της εμπιστευτικότητας, της πιστοποίησης ταυτότητας, της ακεραιότητας των δεδομένων και της διατήρησης της ιδιωτικής ζωής.

Βασικός σκοπός αυτής της εργασίας είναι να καταγράψει τις σοβαρές απειλές, τους κινδύνους και τα τρωτά σημεία που σχετίζονται με τα συστήματα τηλεκπαίδευσης και να γίνει ανάλυση του καθενός από αυτά Ορισμένοι από τους στόχους που θα καλύψουμε σε αυτή την εργασία είναι ο εντοπισμός κινδύνων και απειλών, η ανάλυση και αξιολόγηση αυτών, η παρουσίαση των ευπαθειών που έχουν εντοπισθεί και καταγραφεί στα συστήματα τηλεκπαίδευσης τα τελευταία χρόνια και τέλος η πρόταση ενός πλαισίου μηχανισμών και διαδικασιών για τη θωράκιση της ασφάλειας και την ελαχιστοποίηση των επιπτώσεων των κυβερνοεπιθέσεων. Αυτή η εργασία θα προσφέρει τις απαραίτητες γνώσεις και συμβουλές, ώστε οι εμπλεκόμενοι στην τηλεκεπαίδευση (μαθητές, εκπαιδευτικοί, διαχειριστές) να μπορούν να γίνουν πιο προσεκτικοί και ενημερωμένοι καθώς και να λαμβάνουν μέτρα μετριασμού των κινδύνων ασφαλείας.

1.3 Διαμόρφωση κειμένου

Η παρούσα εργασία εστιάζει στα θέματα ασφάλειας συστημάτων τηλεκπαίδευσης καθώς και σε καλές πρακτικές για τον μετριασμό των κινδύνων. Το δεύτερο κεφάλαιο, παρουσιάζει τα δημοφιλέστερα συστήματα τηλεκπαίδευσης χωρισμένα σε δύο κατηγορίες, τα σύγχρονα και τα ασύγχρονα, καθώς και την σημασία του Cloud Computing στα συστήματα τηλεκπαίδευσης.

Στο τρίτο κεφάλαιο, περιγράφονται τα χαρακτηριστικά ασφαλείας καθώς και οι τύποι επιθέσεων στη πλευρά του χρήστη, του περιβάλλοντος και στον διακομιστή της βάσης δεδομένων τους συστήματος τηλεκπαίδευσης. Επισημαίνεται η προσοχή σε ζητήματα απορρήτου και προσωπικών δεδομένων και αναλύεται η επέκταση του BYOD με τα πλεονεκτήματα αλλά και τα μειονεκτήματά της.

Στο τέταρτο κεφάλαιο, παρατίθενται οι κυριότερες ευπάθειες με βάση το CWE Top 25 και το OWASP Top 10 – 2021. Με βάση τις καταγεγραμμένες ευπάθειες του CVE Details αντιπαραβάλλονται συγκριτικά τα συστήματα τηλεκπαίδευσης ως προς τις επιθέσεις που δέχτηκαν και τα στοιχεία προβάλλονται μέσα από τα αντίστοιχα γραφήματα.

Στο πέμπτο κεφάλαιο, αναλύονται οι στρατηγικές μετριασμού των κινδύνων σε συστήματα τηλεκπαίδευσης και παρέχονται χρήσιμες συμβουλές για ασφαλή τηλεκπαίδευση και πρακτικές οδηγίες για την ασφάλεια των τηλεδιασκέψεων.

Στο έκτο και τελευταίο κεφάλαιο της παρούσας εργασίας, παρατίθενται τα συμπεράσματα της αξιολόγησης των συστημάτων τηλεκπαίδευσης, και γίνονται προτάσεις για μελλοντικές επεκτάσεις.

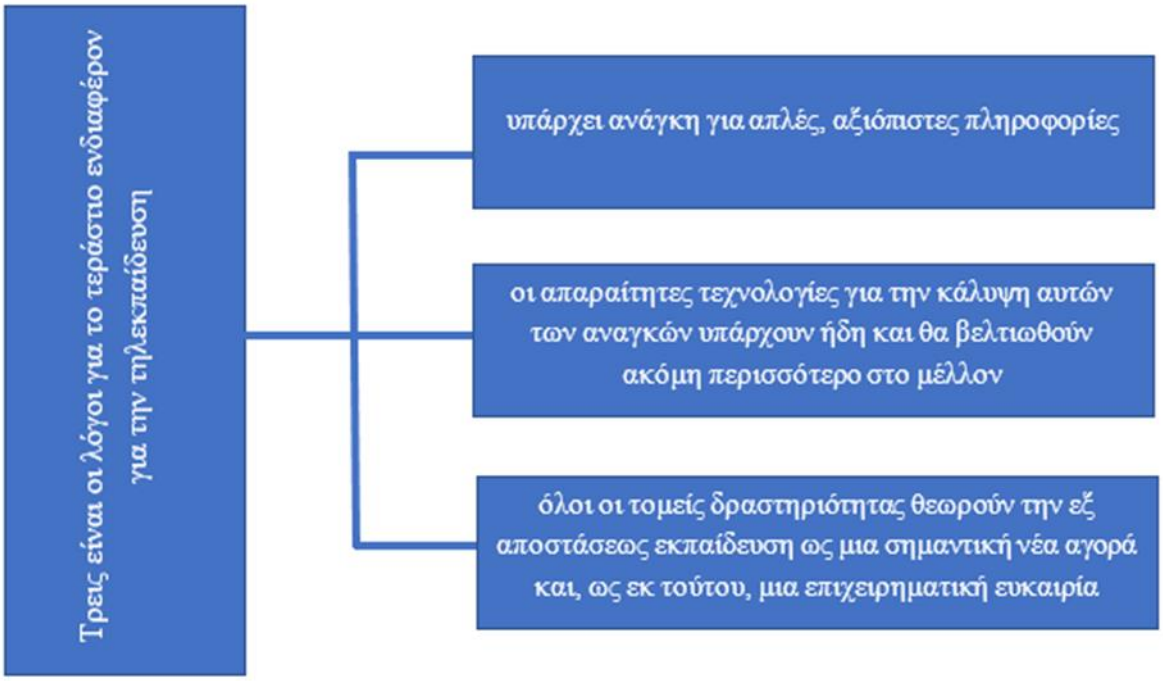
2

Συστήματα τηλεκπαίδευσης

2.1 Τηλεκπαίδευση

Ο όρος «τηλεκπαίδευση» (tele-education) ή «εκπαίδευση από απόσταση» (distance education) συχνά ταυτίζεται με τον όρο «μάθηση από απόσταση» (distance learning). Γενικότερα, όλες αυτές οι έννοιες συνήθως οριοθετούνται στα πλαίσια του όρου «ηλεκτρονική μάθηση» (e-learning) [11]. Σε μια πιο ελεύθερη απόδοση του ορισμού η τηλεκπαίδευση είναι ένας τρόπος μάθησης με τη βοήθεια σύγχρονων τεχνολογικών μέσων. Η επικοινωνία του εκπαιδευτή και των εκπαιδευομένων επιτυγχάνεται μέσω αμφίδρομης ασύγχρονης ή σύγχρονης επικοινωνίας. Αρκετές φορές ειδικοί σε θέματα παιδαγωγικής έρευνας αναφέρονται με τον διεθνή όρο Open & Distance Learning (ODL) ερμηνεύοντας τον στα ελληνικά ως «εξ Αποστάσεως Εκπαίδευση» (εξΑΕ) ή «Ανοικτή εξ Αποστάσεως Εκπαίδευση» (ΑεξΑΕ). Η τηλεκπαίδευση ή «distance education», «distance learning», «e-learning» (κάνοντας χρήση του ξένου όρου) αποτελεί τη μεγαλύτερη ίσως εξέλιξη στην εκπαιδευτική διαδικασία των τελευταίων δεκαετιών.

Τρεις είναι οι λόγοι για το τεράστιο ενδιαφέρον για την τηλεκπαίδευση (Εικόνα 1)



Εικόνα 1: Τρεις είναι οι λόγοι για το τεράστιο ενδιαφέρον για την τηλεκπαίδευση [12]

Ο πρώτος λόγος είναι ότι υπάρχει ανάγκη για απλές, αξιόπιστες πληροφορίες.

Ο δεύτερος είναι ότι οι απαραίτητες τεχνολογίες για την κάλυψη αυτών των αναγκών υπάρχουν ήδη και θα βελτιωθούν ακόμη περισσότερο στο μέλλον.

Και ο τρίτος λόγος είναι ότι όλοι οι τομείς δραστηριότητας θεωρούν την εξ αποστάσεως εκπαίδευση ως μια σημαντική νέα αγορά και, ως εκ τούτου, μια επιχειρηματική ευκαιρία [12].

Πρώτα τα Ανοικτά Πανεπιστήμια εκμεταλλευόμενα την άνθιση του διαδικτύου και των νέων τεχνολογιών, καθιέρωσαν την τηλεκπαίδευση ως μοντέλο λειτουργίας για τη διανομή του διδακτικού υλικού, και έδειξαν τον τρόπο για την εφαρμογή του συγκεκριμένου μοντέλου στα άλλα εκπαιδευτικά ιδρύματα και φορείς. Σήμερα σχεδόν όλα τα εκπαιδευτικά ιδρύματα όλων των εκπαιδευτικών επιπέδων επωφελούνται από τα συστήματα τηλεκπαίδευσης μέσω των οποίων οι εκπαιδευόμενοι μπορούν να παρακολουθηθούν μαθήματα εξ αποστάσεως εκπαίδευσης και να αποκτηθούν οι ανάλογοι τίτλοι, βεβαιώσεις και πτυχία.

Ανάλογα με το πως πραγματοποιείται η επικοινωνία και πως γίνεται η παράδοση του διδακτικού υλικού στους εκπαιδευόμενους, η τηλεκπαίδευση μπορεί να χωριστεί σε δύο κατηγορίες, στη σύγχρονη και στην ασύγχρονη. Η Ασύγχρονη Τηλεκπαίδευση δεν απαιτεί την ταυτόχρονη συμμετοχή των εκπαιδευτών και των εκπαιδευόμενων. Οι μαθητές και ο εκπαιδευτικός δεν είναι υποχρεωτικό να βρίσκονται συγκεντρωμένοι μαζί την ίδια χρονική στιγμή στον ίδιο χώρο, για παράδειγμα σε μια αίθουσα ή τάξη. Η ασύγχρονη Τηλεκπαίδευση

επιτρέπει στους εκπαιδευόμενος να προσαρμόζουν τον ρυθμό και τον χρόνο σύμφωνα με τις δικές τους ανάγκες.

Η Σύγχρονη Τηλεκπαίδευση σε αντίθεση με την Ασύγχρονη είναι η εκπαίδευση η οποία πραγματοποιείται σε πραγματικό χρόνο. Έτσι, μπορεί να προσφέρει στην εκπαιδευτική διαδικασία, την αμεσότητα της επαφής των μαθητών με τους εκπαιδευτικούς. Η Σύγχρονη τηλεκπαίδευση δίνει μια εντελώς διαφορετική διάσταση στη διαδικασία της διδασκαλίας και της μάθησης. Παρόλο που οι μαθητές με τους εκπαιδευτικούς δεν βρίσκονται στον ίδιο τόπο και χώρο, υπάρχει οπτικοακουστική επικοινωνία που επιτυγχάνεται από την σύνδεση των μαθητών με τους εκπαιδευτικούς σε δίκτυο το οποίο επιτρέπει τηλεδιάσκεψη με βίντεο και ήχο. Υπάρχουν και πολλές επιπλέον δυνατότητες όπως η ανταλλαγή αρχείων, μηνυμάτων ακόμα και ηλεκτρονικού μαυροπίνακα. Τα συστήματα σύγχρονης τηλεδιάσκεψης διευκολύνουν τους εκπαιδευτικούς να παρέχουν μαθήματα, διαλέξεις και σεμινάρια, στα οποία οι μαθητές έχουν πρόσβαση σε πραγματικό χρόνο από οποιοδήποτε μέρος του κόσμου αρκεί να έχουν οποιαδήποτε συσκευή εξοπλισμένη με Διαδίκτυο

Πρέπει να επισημανθεί σε αυτό το σημείο ότι η Σύγχρονη και η Ασύγχρονη Τηλεκπαίδευση δεν αποτελούν έννοιες ανταγωνιστικές. Αντίθετα συμπληρώνουν η μία την άλλη. Στην Ασύγχρονη Τηλεκπαίδευση χρησιμοποιούνται τα LMS (Learning Management Systems - LMS), ενώ τα εργαλεία τηλεδιάσκεψης χρησιμοποιούνται για σύγχρονη Τηλεκπαίδευση.

2.2 Συστήματα Ασύγχρονης τηλεκπαίδευσης

Η Ασύγχρονη Τηλεκπαίδευση προσφέρει νέες δυνατότητες στην εκπαιδευτική διαδικασία, προσφέροντας ένα δυναμικό περιβάλλον αλληλεπίδρασης συνεχούς επικοινωνίας μεταξύ εκπαιδευτή και εκπαιδευόμενου, επιτρέποντας την οργάνωση του εκπαιδευτικού υλικού, την αποθήκευση και παρουσίασή του ανεξάρτητα από τις χωροχρονικές δεσμεύσεις της κλασσικής διδασκαλίας. Στόχος είναι η ενίσχυση όλων των εμπλεκόμενων στην εκπαιδευτική διαδικασία μέσα από τις παροχές της τηλεκπαίδευσης. Ταυτόχρονα δίνεται η δυνατότητα στον εκπαιδευτικό να οργανώσει το υλικό και την πορεία της διδασκαλίας του μέσα από ένα δυναμικό περιβάλλον διάχυσης της γνώσης. Ο εκπαιδευόμενος, τέλος, έχει στη διάθεση του ένα εναλλακτικό κανάλι εξατομικευμένης μάθησης χωρίς τους περιορισμούς του χρόνου και του χώρου και στο εκπαιδευτικό ίδρυμα, αποτελεσματικότητα, οικονομία κλίμακας και εποικοδομητική χρήση της υπάρχουσας δικτυακής υποδομής.

Τα Συστήματα Ασύγχρονης Τηλεκπαίδευσης ή αλλιώς Συστήματα Διαχείρισης της Μάθησης (Learning Management Systems - LMS) είναι πακέτα λογισμικού που στηρίζονται στις τεχνολογίες Διαδικτύου και χρησιμοποιούνται για τον σχεδιασμό, την υλοποίηση και τη

λειτουργία εκπαιδευτικών διαδικασιών. Πρόκειται για διαδικτυακές πλατφόρμες μάθησης στις οποίες συμμετέχουν μαθητές, καθηγητές και διαχειριστές. Οι δυνατότητες ενός τέτοιου πακέτου δεν περιορίζονται στην αποθήκευση εκπαιδευτικού περιεχομένου για μαθητές που είναι χρήσιμα για το μάθημα, αλλά επεκτείνονται σε μια δομή που περιέχει διαδικτυακές αξιολογήσεις και βιβλία τάξης, εργαλεία επικοινωνίας, όπως ιστολόγιο και φόρουμ, εργαλεία πολυμέσων, όπως podcast, μαθήματα βίντεο MOOC, λογαριασμούς πρόσβασης, ομάδες εργασίας κ.λπ. [13].

Ο διαχειριστής του LMS έχει τη δυνατότητα να επέμβει σε κάθε διαδικασία του συστήματος είτε διαχειριστική ή ακόμη και εκπαιδευτική. Μερικές ενδεικτικές δυνατότητες ενός LMS για τους εκπαιδευτικούς και τους μαθητές που εμπλέκονται στην εκπαιδευτική διαδικασία είναι οι ακόλουθες:

Εκπαιδευτικός:

- Ανάρτηση εκπαιδευτικού υλικού και ανακοινώσεων που αφορούν τους μαθητές του.
- Οργάνωση της δομής κάθε ενότητας για το εκάστοτε μάθημα.
- Ανάθεση ασκήσεων και εργασιών στους μαθητές του.
- Επικοινωνία με τους μαθητές του τμήματός του.
- Παρακολούθηση της συμμετοχής των μαθητών στις εκπαιδευτικές δραστηριότητες.
- Διαχείριση των μελών της τάξης, ή του μαθήματός του

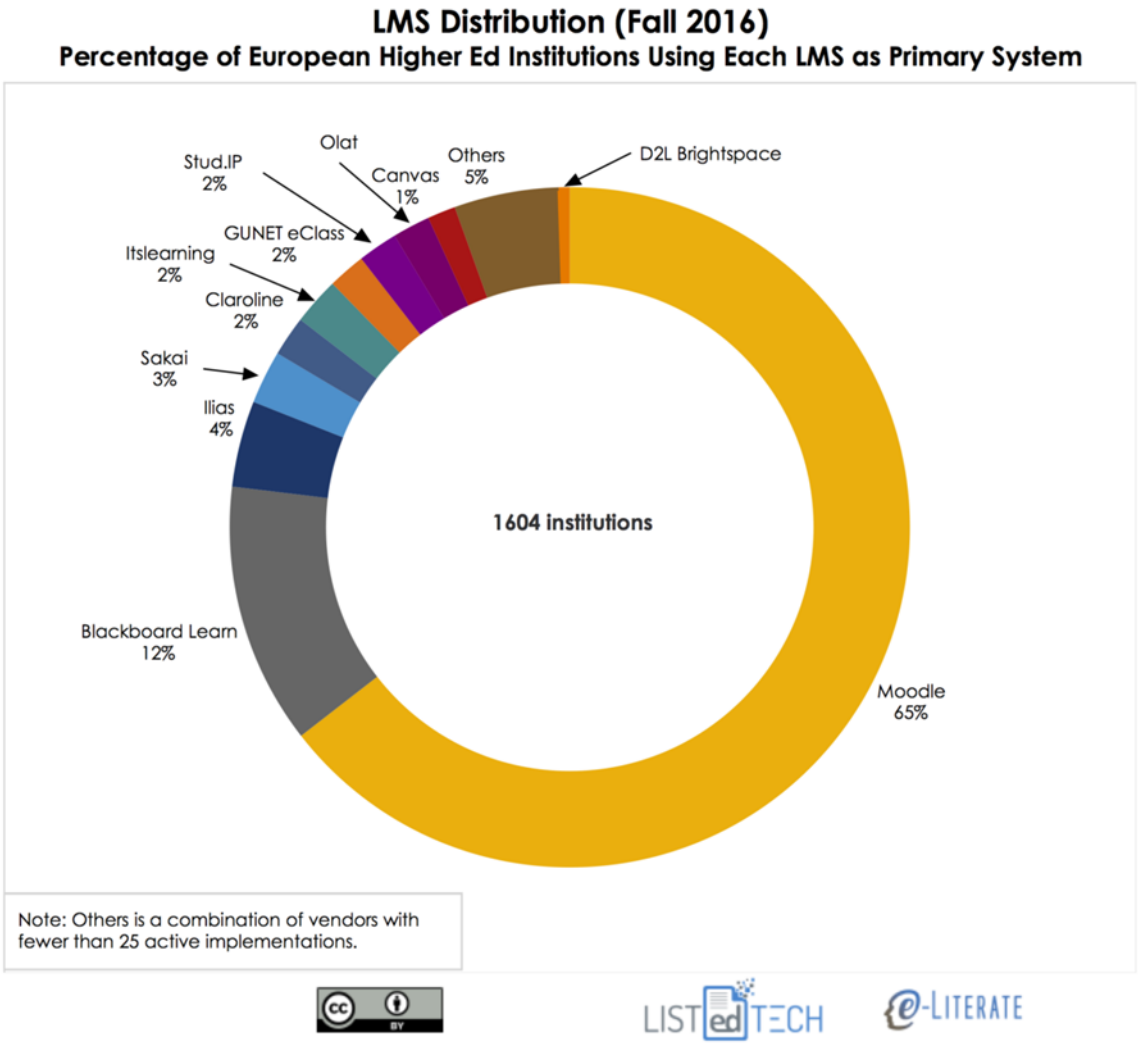
Μαθητής:

- Πρόσβαση στο ψηφιακό εκπαιδευτικό υλικό που αναρτούν οι εκπαιδευτικοί.
- Ενημέρωση για τις ανακοινώσεις του εκπαιδευτικού ιδρύματος.
- Υποβολή ασκήσεων και εργασιών.
- Οργάνωση της ύλης και ενημέρωση για τα τρέχοντα εκπαιδευτικά καθήκοντα.
- Αξιολόγηση του μαθητή με κλειστού τύπου ερωτήσεις, διαδικτυακά κουίζ κ.α.
- Φόρουμ συζήτησης, συνομιλίες (chat) με τους συμμαθητές αλλά και τους εκπαιδευτικούς, για διατύπωση ερωτήσεων και απαντήσεων αλλά και για ανταλλαγή απόψεων.

Το Σύστημα Διαχείρισης Μάθησης αποτελεί ζωτικό συστατικό της εκπαιδευτικής υποδομής του εκάστοτε εκπαιδευτικού ιδρύματος. Τα σύγχρονα LMS κατασκευάζονται συχνά χρησιμοποιώντας συγκριτικά νέες αρχιτεκτονικές λύσεις γνωστές ως Asynchronous Java και XML (AJAX). Τα LMS αποτελούν έναν δυναμικά εξελισσόμενο τομέα, όπου αναφύονται νέοι κατασκευαστές με νέα προϊόντα και δυνατότητες σε τακτική βάση. Υπάρχει μεγάλη προσφορά αλλά και δυνατότητα επιλογής ανάλογα με τις ανάγκες του κάθε οργανισμού αλλά και άλλους παράγοντες, όπως το κόστος αγοράς και συντήρησης. Επειδή για τα εκπαιδευτικά ιδρύματα το

κόστος είναι ένας βασικός παράγοντας, συχνά επιλέγονται LMS ανοικτού κώδικα που συνήθως συντηρούν και επεκτείνουν μόνα τους συμβάλλοντας στη μείωση του λειτουργικού κόστους. Ένα άλλο κέρδος του ανοικτού κώδικα είναι η τεχνογνωσία που αποκτούν τα εκπαιδευτικά ιδρύματα μέσα από διάφορες αναπτυξιακές και ερευνητικές δραστηριότητες αλλά και η μη εξάρτησή τους από εταιρείες που αναπτύσσουν κλειστό λογισμικό.

Βέβαια, τα LMS υπήρχαν και πριν την πανδημία, όμως κατά τη διάρκεια αυτής της περιόδου, αξιοποιήθηκαν πλήρως. Οι εκπαιδευτικοί δημιούργησαν σύνθετα μαθήματα που είχαν διάφορες δραστηριότητες, όπως τεστ και διαγωνίσματα για την αξιολόγηση, γλωσσάρια, εργασίες κ.α.. Σύμφωνα με την έκθεση LMS Market [14], στα ευρωπαϊκά AEI, οι ηγέτες των LMS είναι: Moodle (65%), Blackboard (12%) (Εικόνα 2)



Εικόνα 2 : Ποσοστό κατανομής LMS των ευρωπαϊκών AEI [14]

Δύο είναι οι βασικοί λόγοι που καθιστούν το LMS συχνό στόχο για επιθέσεις ασφαλείας. Το LMS είναι ένα τεράστιο αποθετήριο δεδομένων, αρκετά από τα οποία είναι ευαίσθητα και η λειτουργικότητα του συστήματος είναι εξαιρετικά σημαντική για κάθε εκπαιδευτικό ίδρυμα. Ως εκ τούτου, το LMS πρέπει να παρέχεται με ένα σχετικό επίπεδο ασφάλειας [15]. Ακολουθεί περιγραφή τριών από τα πιο διαδεδομένα LMS.

2.2.1 Moodle

Το Moodle (Modular Object-Oriented Dynamic Learning) είναι μια πλατφόρμα ανοιχτού κώδικα, που δημιουργήθηκε και αναπτύχθηκε στην Αυστραλία από τον προγραμματιστή Martin Dougiamas, το 1999 ως τμήμα του διδακτορικού του. Σκοπός της ανάπτυξής του ήταν να βοηθήσει τους εκπαιδευτές να δημιουργήσουν δικτυακά μαθήματα δίνοντας έμφαση στην συνεργατική κατασκευή του περιεχομένου, την αλληλεπίδραση καθώς και τη συνεχόμενη ανάπτυξή του. Το Moodle είναι μια διαδικτυακή εφαρμογή ανοιχτού κώδικα, ο πηγαίος κώδικας είναι γραμμένος σε PHP και οι βάσεις δεδομένων που υποστηρίζει είναι η MySQL και η PostgreeSQL [13].

Το Moodle είναι ένα Σύστημα Διαχείρισης Μάθησης (LMS) που χρησιμοποιείται ως εργαλείο για τη δημιουργία διαδικτυακών δυναμικών ιστοσελίδων για διδασκαλία. Το LMS είναι μια διαδικτυακή πλατφόρμα μάθησης στην οποία συμμετέχουν μαθητές, καθηγητές και διαχειριστές. Έχει τη δυνατότητα να παρέχει πολλά εργαλεία για τη διαχείριση και την προώθηση της μάθησης γι' αυτό και είναι πολύ δημοφιλές μεταξύ των εκπαιδευτικών. Η εγκατάστασή του πρέπει να γίνει είτε σε web server είτε σε έναν τοπικό υπολογιστή ή ακόμα και σε μια εταιρεία φιλοξενίας Ιστού. Το Moodle διαθέτει διάφορες εκδόσεις και η εγκατάστασή του μπορεί να γίνει ανάλογα με τον αριθμό των μαθητών που πρόκειται να υποστηρίξει. Μπορεί να χρησιμοποιηθεί εξίσου αποτελεσματικά από ένα δημοτικό σχολείο με λίγες εκατοντάδες μαθητές ή από εκπαιδευτικά ιδρύματα με χιλιάδες φοιτητές που το χρησιμοποιούν ως την κύρια πλατφόρμα για τη διεξαγωγή διαδικτυακών μαθημάτων [16]. Οι χρήστες του υπολογίζονται σε 60 εκατομμύρια σε 220 χώρες. Στην πραγματικότητα, είναι το προϊόν που έχει κερδίσει το μεγαλύτερο μερίδιο αγοράς τα τελευταία χρόνια.

Παράλληλα διαθέτει πολλά πλεονεκτήματα σε σύγκριση με άλλες παρόμοιες εκπαιδευτικές πλατφόρμες, καθώς είναι άμεσα παραμετροποιήσιμο, ανάλογα με τις ανάγκες των μαθημάτων και των χρηστών. Μπορεί εύκολα να εγκατασταθεί και υπάρχει υποστήριξη από μια μεγάλη κοινότητα χρηστών και προγραμματιστών. Χρησιμοποιεί γνώριμες, ώριμες και ισχυρές τεχνολογίες και προσφέρει μια οικονομική λύση η οποία σε αρκετές περιπτώσεις είναι πιο ευέλικτη από ό,τι τα εμπορικά LMS. Το Moodle διαθέτει μια ισχυρή λειτουργία διαχείρισης

μαθημάτων που καλύπτει τη δημιουργία μαθημάτων, εργασιών, κουίζ, εγγράφων και άλλα. Υπάρχουν, ακόμη, ποικίλες ενότητες που βοηθούν τους μαθητές και τους εκπαιδευτικούς να αλληλεπιδρούν μεταξύ τους, όπως συνομιλία, φόρουμ κ.α. .

Μερικά χαρακτηριστικά του Moodle περιγράφονται στην εικόνα που ακολουθεί.

Εικόνα 3: Χαρακτηριστικά του Moodle [17]

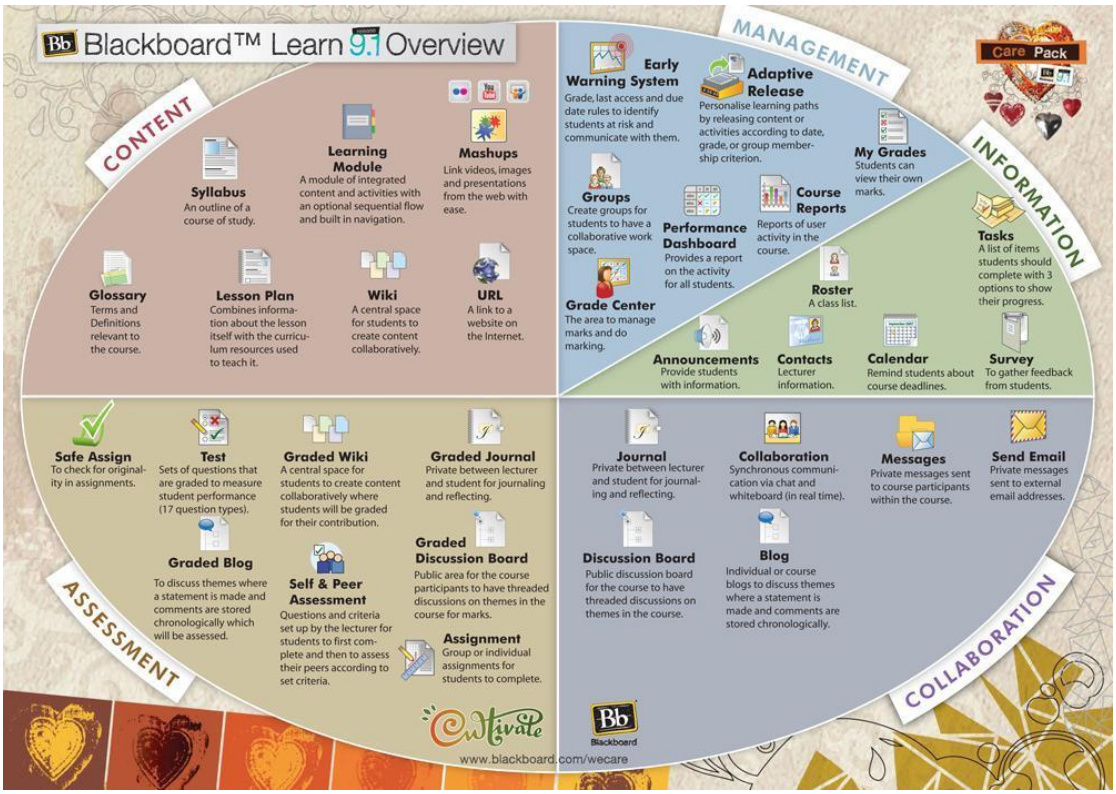
2.2.2 Blackboard

Το Blackboard είναι ένας ολοκληρωμένος ψηφιακός χώρος μάθησης. Πρόκειται για μία διαδεδομένη εμπορική πλατφόρμα που χρησιμοποιείται πάνω από δύο δεκαετίες από μεγάλες επιχειρήσεις, δημόσιες υπηρεσίες αλλά και εκπαιδευτικούς φορείς, όπως πολλά κολέγια και πανεπιστήμια. Από πολλούς θεωρείται μια εκπαιδευτική πλατφόρμα που είναι εύκολα προσβάσιμη αλλά και αρκετά ευέλικτη, καθώς οι χρήστες μπορούν να έχουν πρόσβαση μέσω του διαδικτύου από οπουδήποτε. Επιτρέπει στους συμμετέχοντες γρήγορη πρόσβαση σε περιεχόμενο, ανακοινώσεις, συζητήσεις, τεστ, εργασίες, εικονικές τάξεις. Σημαντικά χαρακτηριστικά του Blackboard είναι η χρηστικότητα, η τυποποίηση, η ασφάλεια, η διαχείριση τάξης και η αλληλεπίδραση δασκάλου - μαθητή. Το 2015 η εταιρεία ανακοίνωσε μια ενημέρωση, που ονομάζεται Blackboard Collaborate Ultra που επιτρέπει την αλληλεπίδραση πρόσωπο με

πρόσωπο στην τάξη, η οποία δημιουργεί μια αίσθηση φυσικής παρουσίας με τους δασκάλους να παραδίδουν ζωντανά μαθήματα σε τάξεις με πάνω από 250 μαθητές. Προσφέρει πολλά εργαλεία (Εικόνα 4) για την υποστήριξη μαθησιακών και διδακτικών δραστηριοτήτων, όπως Blackboard Analytics, Grade center, Blackboard Collaborate και πολλά άλλα.

Οι δυνατότητες για αξιολόγηση των μαθητών μέσα από τα τεστ, κουίζ και διαδικτυακών εξετάσεων (ιδιαίτερα χρήσιμα στην περίοδο της πανδημίας) που μπορούν να σχεδιαστούν εύκολα και γρήγορα είναι ένα σημαντικό χαρακτηριστικό του Blackboard. Οι μαθητές μπορούν να λάβουν άμεση ανατροφοδότηση μετά την υποβολή των τεστ με ή χωρίς διαβαθμισμένο υλικό.

Ωστόσο, το Blackboard έχει ορισμένους περιορισμούς. Ένα βασικός περιορισμός είναι το κόστος, με τα ακαδημαϊκά ιδρύματα να πρέπει να πληρώσουν ένα τεράστιο ποσό για να χρησιμοποιήσουν τις υπηρεσίες του. Ως εμπορικό προϊόν κοστολογείται ανάλογα με τις παροχές (τάξεις, αριθμός μαθητών) που θέλει ο αγοραστής και το κοστολόγιο κυμαίνεται από 300 έως 900 δολάρια. Επίσης η πολύπλοκη διεπαφή του και ορισμένα εγγενή τεχνικά ζητήματα μπορούν να απογοητεύσουν τους εκπαιδευτικούς. Τέλος, είναι επίσης ευάλωτο σε πολλά ζητήματα ασφάλειας, όπως και οι άλλες πλατφόρμες [18].



Εικόνα 4 : Χαρακτηριστικά του Blackboard [19]

2.2.3 Open eclass

Η πλατφόρμα Open eClass είναι ένα ολοκληρωμένο σύστημα διαχείρισης ηλεκτρονικών μαθημάτων που προσφέρεται από το Ακαδημαϊκό Διαδίκτυο GUNET για την υποστήριξη υπηρεσιών ασύγχρονης εξ αποστάσεως εκπαίδευσης. Ακολουθώντας τη φιλοσοφία του ανοικτού κώδικα, υποστηρίζεται ενεργά από το GUNET και διανέμεται ελεύθερα χωρίς περιορισμούς ή υποχρεώσεις. Η πλατφόρμα είναι διαθέσιμη στην ηλεκτρονική διεύθυνση https://www.openeclass.org. Η υπηρεσία δεν απαιτεί ειδικές τεχνικές γνώσεις και είναι προσβάσιμη μέσω ενός απλού προγράμματος περιήγησης στο διαδίκτυο. Βασική επιδίωξη της πλατφόρμας είναι η ενσωμάτωση νέων τεχνολογιών κατά την εκπαιδευτική διαδικασία και η εποικοδομητική χρήση του διαδικτύου.

Η πρώτη έκδοση του Open eClass κυκλοφόρησε τον Μάρτιο του 2003. Αυτή η αρχική έκδοση βασίστηκε στην πλατφόρμα ανοικτού κώδικα Claroline. Έκτοτε, έχουν σχεδιαστεί και αναπτυχθεί αρκετές νέες εκδόσεις, οι οποίες αποτελούν πλέον ανεξάρτητες πλατφόρμες που δεν έχουν καμία ομοιότητα με την αρχική πλατφόρμα. Η τρέχουσα έκδοση της πλατφόρμας είναι η 3.13 η οποία δεν θυμίζει σε τίποτα την αρχική. Διαθέτει μοντέρνα και προσαρμοστική διεπαφή που βασίζεται σε σύστημα Bootstrap 3x που του δίνει τη δυνατότητα να προσαρμόζεται σε οποιοδήποτε συσκευή (υπολογιστές, smart phones και tablets) ανεξάρτητα από το μέγεθος της οθόνης. Είναι διαθέσιμο στο App Store και στο Play Store.

Κεντρικός πυρήνας της πλατφόρμας Open eClass είναι το ηλεκτρονικό μάθημα που αποτελεί μια αυτόνομη οντότητα στην πλατφόρμα που προσφέρει πλήθος υποσυστημάτων. Ο υπεύθυνος καθηγητής οργανώνει το υλικό του αναλόγως με το ποιο μοντέλο μάθησης θέλει να υλοποιήσει, δηλαδή από ένα απλό ενημερωτικό site έως ένα ολοκληρωμένο περιβάλλον εκπαίδευσης. Οι κατηγορίες μαθημάτων που υποστηρίζει η πλατφόρμα είναι τρεις. Τα ανοικτά μαθήματα, στα οποία έχουν όλοι πρόσβαση, τα ανοικτά με εγγραφή στην πλατφόρμα που έχουν πρόσβαση μόνο όσοι έχουν λογαριασμό στην πλατφόρμα, και τα κλειστά μαθήματα, στα οποία είναι υποχρεωτική η εγγραφή στην πλατφόρμα, καθώς και η εγγραφή τους στο μάθημα από τον ίδιο τον υπεύθυνο καθηγητή του μαθήματος.

Μερικά από τα βασικά στοιχεία που συνθέτουν ένα ψηφιακό μάθημα και εισάγονται από τον καθηγητή στην πλατφόρμα eClass είναι τα εξής: Η περιγραφή του μαθήματος κατά την οποία παρέχονται πληροφορίες για τους στόχους και τη δομή του μαθήματος. Η Ατζέντα που αναφέρεται στα γεγονότα σταθμούς του μαθήματος, όπως διαλέξεις, συναντήσεις, αξιολογήσεις κλπ. Τα Έγγραφα που διαθέτουν το ψηφιακό υλικό, δηλαδή εικόνες, κείμενα, παρουσιάσεις κτλ. Οι Εργασίες είναι ένας χώρος που οι μαθητές αναρτούν τις εργασίες τους. Ασκήσεις αυτοαξιολόγησης που ο καθηγητής αναρτά για τους μαθητές του. Φόρουμ

συζητήσεων για θέματα που αφορούν στο μάθημα. Οι ανακοινώσεις για τους εκπαιδευόμενους από τον καθηγητή τους. Τέλος οι χρήσιμοι σύνδεσμοι από το διαδίκτυο που αφορούν στο μάθημα και σε πολλά άλλα. Τα στοιχεία αυτά μπορούν να ενεργοποιούνται ή να απενεργοποιούνται από τον καθηγητή ανάλογα με την πορεία του μαθήματος, έτσι ώστε να απλοποιείται το περιβάλλον εργασίας εμφανίζοντας μόνο τις απαραίτητες ενότητες για κάθε χρονική στιγμή.

Η πλατφόρμα Open eClass χρησιμοποιείται από το σύνολο σχεδόν των Ακαδημαϊκών Ιδρυμάτων της χώρας υποστηρίζοντας ένα μεγάλο πλήθος ηλεκτρονικών μαθημάτων με χιλιάδες χρήστες να συμμετέχουν σε αυτά. Παράλληλα χρησιμοποιείται με μεγάλη επιτυχία στη δευτεροβάθμια ακόμη και στην Πρωτοβάθμια εκπαίδευση υποστηρίζοντας την υπηρεσία ηλεκτρονικής τάξης (η-Τάξη) σε όλα τα σχολεία της Ελλάδος. Στη συνέχεια παρατίθεται ένας κατάλογος (Εικόνα 5) με τις ενεργές εγκαταστάσεις της πλατφόρμας Open eClass που έχουν δηλωθεί από τους διαχειριστές τους στην ομάδα Ασύγχρονης Τηλεκπαίδευσης του GUnet.

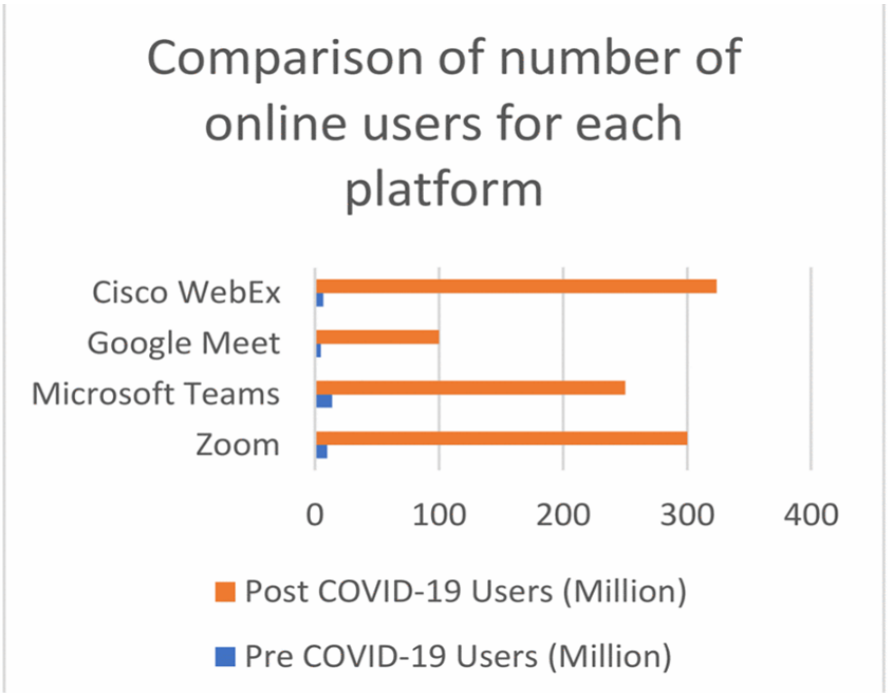
Η πλατφόρμα Open eClass βρίσκεται σε μια φάση λειτουργικής και σχεδιαστικής ωριμότητας. Ο βασικός προσανατολισμός της παραμένει η ενίσχυση και η υποστήριξη της εκπαιδευτικής δραστηριότητας μέσα από ένα εύχρηστο περιβάλλον τεχνολογικής αιχμής. Ειδικότερα επιχειρείται η ανάπτυξη υποδομών εκπαίδευσης και κατάρτισης ανεξάρτητα από τους περιοριστικούς παράγοντες του χώρου και του χρόνου της συμβατικής διδασκαλίας με την εισαγωγή των νέων τεχνολογιών της πληροφορίας και της επικοινωνίας (ΤΠΕ). Παράλληλα, σημαντικοί σχεδιαστικοί άξονες της πλατφόρμας αποτελούν η προσαρμοστικότητα στις απαιτήσεις, η ευελιξία, η ευκολία στη χρήση, η δυνατότητα αναβάθμισης και επέκτασης, η ελεύθερη διάθεση χωρίς την απαίτηση αδειών χρήσης και συντήρησης, οι μικρές λειτουργικές απαιτήσεις, η ανεξαρτησία από το υποκείμενο Λειτουργικό Σύστημα, η χρήση ανοικτών προτύπων, η δυνατότητα ολοκλήρωσης της πλατφόρμας με άλλες δικτυακές υπηρεσίες, οι ξεκάθαρες λειτουργικές δομές (εγγραφή, πρόσβαση, δημιουργία μαθήματος, διαχείριση κλπ), η διαλειτουργικότητα και η ασφάλεια, καθώς και η συνεχής υποστήριξη από το Ακαδημαϊκό Διαδίκτυο (GUnet) [20].

Εικόνα 5 : Κατάλογος με τις ενεργές εγκαταστάσεις της πλατφόρμας Open eClass [20]

2.3 Συστήματα Σύγχρονης τηλεκπαίδευσης

Η τηλεδιάσκεψη μπορεί να χρησιμοποιηθεί ως αποτελεσματικό εργαλείο διδασκαλίας και επικοινωνίας στη σύγχρονη εξ αποστάσεως εκπαίδευση, επειδή τα συστήματα τηλεκπαίδευσης που παρέχουν αλληλεπίδραση σε πραγματικό χρόνο, σύμφωνα με σχετικές έρευνες για την εκπαίδευση από απόσταση, αυξάνουν τη δέσμευση των μαθητών, παρέχουν δυνατότητα άμεσης ανατροφοδότησης δίνουν δυνατότητες συνεργασίας στην εξ αποστάσεως εκπαίδευση. Τα συστήματα τηλεκπαίδευσης δίνουν τη δυνατότητα σε μαθητές και εκπαιδευτικούς να εκφραστούν με τη χρήση οπτικής, λεκτικής και ακουστικής επικοινωνίας με τους άλλους συμμετέχοντες, λόγω των δυνατοτήτων πολυμέσων της τεχνολογίας τηλεδιάσκεψης που βασίζεται στο διαδίκτυο. Ταυτόχρονα το περιβάλλον που δημιουργούν για την υποστήριξη της μάθησης προσομοιώνει σε πολύ μεγάλο βαθμό το περιβάλλον της φυσικής τάξης [21]. Αυτό έχει ως αποτέλεσμα να μεγαλώνει η ψυχολογική δέσμευση για εργασίες και μελέτη και αντίθετα να μειώνεται η ασάφεια που αρκετές φορές συμβαίνει από την επικοινωνία μόνο με κείμενο.

Με τα χρόνια, υπήρξαν πολλές δημοφιλείς εφαρμογές σύγχρονης τηλεκπαίδευσης, συμπεριλαμβανομένων των Zoom, Microsoft Teams, Google Meet (Hangouts), Skype, Adobe Connect, CiscoWebex και Freeconferencecall. Με βάση το [22] το Zoom, το MS Teams, το CiscoWebex και το Google Meet ήταν οι πιο συχνά χρησιμοποιούμενες εφαρμογές τηλεκπαίδευσης στην ηλεκτρονική μάθηση. Στην περίοδο του lockdown λόγω του COVID-19 σχεδόν όλα τα εκπαιδευτικά ιδρύματα σε όλα τα μέρη του κόσμου χρησιμοποίησαν της παραπάνω πλατφόρμες τηλεκπαίδευσης μαζί με ήδη εφαρμοσμένα συστήματα ασύγχρονης τηλεκπαιδευσης. Στην Εικόνα 6 βλέπουμε τη δεκαπλάσια αύξηση των χρηστών ανά ημέρα σε σύγκριση για τους χρήστες πριν την πανδημία.



Εικόνα 6 : Αύξηση αριθμού χρηστών ανά ημέρα [3]

2.3.1 Zoom

Το Zoom είναι η πιο δημοφιλής πλατφόρμα τηλεδιάσκεψης στον κόσμο και αναπτύχθηκε από την Zoom Video Communications. Παρέχει υπηρεσίες διαδικτυακής συνομιλίας μέσω μιας εφαρμογής ζωντανών κλήσεων που βασίζεται στο cloud και χρησιμοποιείται για εικονικές συσκέψεις, εξ αποστάσεως εκπαίδευση. Το Zoom έχει γίνει η πιο δημοφιλής εφαρμογή για τον τομέα της εκπαίδευσης και στην περίοδο της πανδημίας, αφού περισσότεροι από 300 εκατομμύρια χρήστες το χρησιμοποιούσαν καθημερινά. Οι δυνατότητες του Zoom είναι πολλές, όπως ατομικές συναντήσεις, ομαδικές βιντεοδιασκέψεις, κοινή χρήση οθόνης, συμβατότητα. Οι προσκεκλημένοι μπορούν να παρακολουθήσουν τη σύσκεψη χωρίς να χρειάζεται να κατεβάσουν καμία εφαρμογή και χωρίς να δημιουργήσουν λογαριασμούς στην

εφαρμογή. Αρκεί μόνο να κάνουν κλικ στον σύνδεσμο που τους έχει δοθεί χρησιμοποιώντας ένα από τα προγράμματα περιήγησης Chrome και Firefox. Επιπλέον, η δωρεάν έκδοση του Zoom είναι για 40 λεπτά δωρεάν και 100 συμμετέχοντες το πολύ [23]. Το Zoom έχει γίνει η πιο διαδεδομένη πλατφόρμα τηλεδιάσκεψης καθώς όλο και περισσότεροι άνθρωποι το χρησιμοποιούν Ωστόσο αντιμετωπίζει τεράστιες αντιδράσεις για το απόρρητο και την ασφάλεια, καθώς οι ειδικοί προειδοποιούν ότι οι προεπιλεγμένες ρυθμίσεις δεν είναι αρκετά ασφαλείς [24]. Ο Έρικ Γιουάν, ο ιδρυτής και διευθύνων σύμβουλος που δημιούργησε το Zoom το 2011, ζήτησε συγγνώμη στο ιστολόγιό του που η πλατφόρμα δεν υπήρξε, όσο έπρεπε ασφαλής. Αν και η εφαρμογή δεν σχεδιάστηκε κυρίως για ηλεκτρονική μάθηση το Zoom με τακτικές αναβαθμίσεις εστίασε και εστιάζει σε ζητήματα απορρήτου και διαφάνειας. Με τις νέες εκδόσεις, από τον Απρίλιο του 2020 που κυκλοφόρησε η έκδοση 5.0 του Zoom επιλύθηκαν επιτυχώς πολλά ζητήματα ασφάλειας, βελτιωμένη κρυπτογράφηση, ζητήματα απορρήτου και κωδικών πρόσβασης [22].

2.3.2 Teams

Το Teams είναι μια εφαρμογή της Microsoft και κυκλοφόρησε τον Μάρτιο του 2017 στη Νέα Υόρκη. Μια δωρεάν έκδοση του Microsoft Teams παρουσιάστηκε στις 12 Ιουλίου του 2018, που περιορίζει τον αριθμό των χρηστών και τη χωρητικότητα αποθήκευσης αρχείων αλλά προσφέρει δυνατότητες επικοινωνίας για τις περισσότερες πλατφόρμες δωρεάν [22]. Το Microsoft Teams είναι ενσωματωμένο στη σουίτα λογισμικού γραφείου του Office 365 και περιλαμβάνει πρόσθετα που επιτρέπουν σε προϊόντα που δεν ανήκουν στη Microsoft να συνδέονται σωστά. Στοχεύει σε τάξεις ή ομάδες για συνεργασία, κοινή χρήση και συνομιλία. Εκτός από τη συνομιλία κειμένου, υποστηρίζονται επίσης βιντεοκλήσεις και κοινή χρήση οθόνης. Συνδυάζει περιεχόμενο, συνομιλίες και εφαρμογές σε ένα μέρος, επιτρέποντας στους εκπαιδευτικούς να δημιουργούν εξατομικευμένα και συνεργατικά μαθησιακά περιβάλλοντα. Η εφαρμογή Teams υποστηρίζει τη συνεργασία και την επικοινωνία με μαθητές και εκπαιδευτικούς. Επίσης οι εκπαιδευτικοί μπορούν να διανέμουν εργασίες, να δίνουν σχόλια να κάνουν κουίζ για μαθητές και να ταξινομούν το υλικό των μαθητών στην καρτέλα εργασιών που προσφέρεται στους συνδρομητές του Office 365 Education [25]. Μερικά γνωστά προβλήματα στο Teams σχετίζονται με τη δομή των αρχείων, καθώς μπερδεύει τους χρήστες. Μερικές φορές, το Teams ενδέχεται να έχει κολλήσει κατά την φόρτωση, ή να μη λειτουργεί η κάμερα και το μικρόφωνο. Επίσης να μην λειτουργεί σωστά λόγω κάποιου απροσδόκητου σφάλματος. Το Teams μετρά πλέον περίπου 250 εκατομμύρια μηνιαίους ενεργούς χρήστες.

2.3.3 Google Meet

Το Google Meet (πρώην Hangouts) είναι μια υπηρεσία επικοινωνίας βίντεο που αναπτύχθηκε από την Google. Κατά τη διάρκεια της πανδημίας COVID-19 η χρήση του Meet αυξήθηκε κατακόρυφα, φτάνοντας τους 100 εκατομμύρια χρήστες την ημέρα την τελευταία εβδομάδα του Απριλίου 2020 [22]. Σε αντίθεση με άλλες εφαρμογές τηλεπικοινωνιών, το Google Meet έχει μια πλήρη, δωρεάν έκδοση και εξαιρετικά απλοποιημένη λειτουργία. Οποιοσδήποτε διαθέτει έναν λογαριασμό Google, μπορεί να δημιουργήσει μια σύσκεψη στο διαδίκτυο με έως και 100 συμμετέχοντες και διάρκεια έως και 60 λεπτά ανά σύσκεψη. Η Google εγγυάται την ταυτόχρονη επικοινωνία με πολλές επαφές και με την καλύτερη ποιότητα ήχου και εικόνας για κάθε συνάντηση. Δεν απαιτείται η λήψη και εγκατάσταση της εφαρμογής για την συμμετοχή σε μια σύσκεψη μιας και μπορεί να χρησιμοποιηθεί οποιοδήποτε πρόγραμμα περιήγησης ιστού. Πολλά πλεονεκτήματα που προσφέρει το Google Meet, όπως καταγραφή συνεδρίας, ιδιωτικές συνομιλίες και πραγματοποίηση ζωντανών μεταδόσεων μπορούν να χρησιμοποιηθούν μόνο από λογαριασμούς συνδρομής Google. Επίσης ο αριθμός των συμμετεχόντων είναι περιορισμένος ακόμη και με συνδρομή επί πληρωμή.

2.3.4 Cisco Webex

Η Cisco Webex είναι Αμερικανική εταιρεία που αναπτύσσει και παρέχει συστήματα διαδικτυακών διασκέψεων. Ιδρύθηκε ως WebEx το 1995 και εξαγοράστηκε από τη Cisco Systems το 2007. Το Cisco Webex είναι ένα λογισμικό τηλεδιάσκεψης και διαδικτυακής διάσκεψης που επιτρέπει στον χρήστη τη δυνατότητα δημιουργίας ασφαλών εικονικών χώρων [26]. Διαθέτει εφαρμογές για επιτραπέζιους υπολογιστές και για κινητά καθώς και μια εφαρμογή Ιστού που δίνει τον έλεγχο της διάσκεψης από το πρόγραμμα περιήγησή. Η δωρεάν υπηρεσία δεν περιορίζει τη διάρκεια της σύσκεψης και επιτρέπει 100 συμμετέχοντες τη φορά. Επίσης οι προσκεκλημένοι έχουν τη δυνατότητα να συμμετέχουν στη σύσκεψη χρησιμοποιώντας έναν αριθμό κλήσης όπου δεν μπορούν να δουν τους άλλους συμμετέχοντες, αλλά μπορούν να μοιραστούν τις σκέψεις τους [24]. Ένα βασικό πλεονεκτήματα που έχει το Webex είναι η δυνατότητα ενσωμάτωσης υπηρεσιών του με LMS (π.χ. Moodle) για τη διευκόλυνση της διαδικτυακής μάθησης και της χρήσης εικονικών αιθουσών διδασκαλίας με τη διαχείριση δραστηριοτήτων και άλλων δραστηριοτήτων, όπως η προετοιμασία, η εφαρμογή και η αξιολόγηση [27]. Παράλληλα η δωρεάν έκδοση διαθέτει επιλογές κοινής χρήσης επιφάνειας εργασίας, κοινής χρήσης εφαρμογών, κοινής χρήσης αρχείων και κοινής χρήσης πίνακα. βίντεο υψηλής ευκρίνειας (HD), προσωπικά δωμάτια, δυνατότητες ψηφοφορίας κ.α. Με το Cisco WebEx να προσελκύει 324 εκατομμύρια χρήστες μόνο τον Μάρτιο του 2020 και 50+ εκατομμύρια λήψεις της εφαρμογής στο Google Play Store, αποτελεί μια από τις κορυφαίες εφαρμογές τηλεδιάσκεψης [28].

2.4 Το Cloud Computing στα συστήματα τηλεκπαίδευσης

Το cloud computing αναφέρεται στην παροχή υπολογιστικών υπηρεσιών — συμπεριλαμβανομένων διακομιστών, αποθήκευσης, βάσεων δεδομένων, δικτύωσης, λογισμικού, αναλυτικών στοιχείων και νοημοσύνης— μέσω του Διαδικτύου («cloud») για να προσφέρει ταχύτερη καινοτομία, ευέλικτους πόρους και οικονομίες κλίμακας. Με το cloud computing, οι χρήστες μπορούν να έχουν πρόσβαση σε αυτές τις υπηρεσίες κατόπιν ζήτησης, χωρίς να χρειάζεται να επενδύσουν και να διατηρήσουν την υποκείμενη υποδομή. Υπάρχουν πολλοί διαφορετικοί τύποι υπολογιστικού νέφους, όπως:

Υποδομή ως υπηρεσία (IaaS): Αυτός είναι ο πιο βασικός τύπος υπολογιστικού νέφους και παρέχει στους χρήστες εικονικούς υπολογιστικούς πόρους, όπως διακομιστές, χώρο αποθήκευσης και δικτύωση.

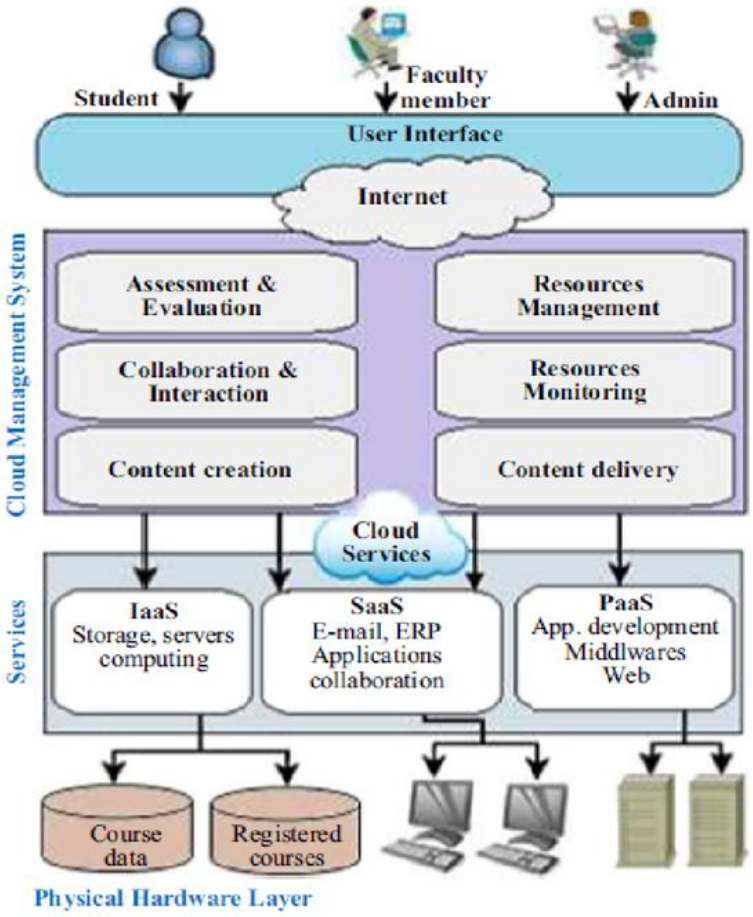
Πλατφόρμα ως υπηρεσία (PaaS): Αυτός ο τύπος υπολογιστικού νέφους παρέχει στους χρήστες μια πλατφόρμα για την ανάπτυξη, την εκτέλεση και τη διαχείριση εφαρμογών, χωρίς να χρειάζεται να ανησυχούν για τη διαχείριση της υποκείμενης υποδομής.

Software as a Service (SaaS): Αυτός είναι ο πιο προηγμένος τύπος υπολογιστικού νέφους και παρέχει εφαρμογές λογισμικού μέσω του Διαδικτύου, με συνδρομή.

Το cloud computing έχει πολλά πλεονεκτήματα με πρώτο την εξοικονόμηση κόστους για τα εκπαιδευτικά ιδρύματα, καθώς δεν χρειάζεται να επενδύουν και να συντηρούν ακριβές υποδομές εσωτερικού χώρου. Επίσης επιτρέπει την επεκτασιμότητα με την εύκολη κλιμάκωση των πόρων προς τα πάνω ή προς τα κάτω, με βάση τις μεταβαλλόμενες ανάγκες. Ένα άλλο πλεονέκτημα για τους χρήστες είναι ότι μπορούν να έχουν πρόσβαση σε πόρους του cloud computing από οπουδήποτε με σύνδεση στο Διαδίκτυο. Επίσης, η αξιοπιστία είναι μεγάλη μιας και οι πάροχοι Cloud έχουν γενικά πολλά κέντρα δεδομένων και χρησιμοποιούν προηγμένες τεχνικές για να εξασφαλίσουν υψηλή διαθεσιμότητα. Τέλος οι εφαρμογές στο cloud computing είναι καινοτόμες, επειδή οι πάροχοι Cloud ενημερώνουν και βελτιώνουν συνεχώς τις υπηρεσίες τους, ώστε οι χρήστες να μπορούν να επωφελούνται από τις νέες τεχνολογίες και δυνατότητες. Το αποτέλεσμα είναι ότι η ζήτηση για cloud computing αυξάνεται σταθερά και τα προγράμματά του χρησιμοποιούνται ευρέως [29].

Το cloud computing και τα συστήματα τηλεκπαίδευσης έχουν μια φυσική συνέργεια, καθώς οι υπηρεσίες που βασίζονται στο cloud μπορούν να προσφέρουν μια σειρά από οφέλη που μπορούν να βελτιώσουν την παράδοση και τη διαχείριση της διαδικτυακής εκπαίδευσης. Στην Εικόνα 7 βλέπουμε την κοινή αρχιτεκτονική των συστημάτων τηλεκπαίδευσης που βασίζονται στο cloud. Υπάρχουν πολλοί τρόποι με τους οποίους το cloud computing μπορεί να

χρησιμοποιηθεί στην τηλεκπαίδευση. Καταρχάς πολλοί πάροχοι LMS προσφέρουν λύσεις που βασίζονται σε σύννεφο που είναι προσβάσιμες από οπουδήποτε με σύνδεση στο Διαδίκτυο. Αυτό μπορεί να προσφέρει μεγαλύτερη ευελιξία και ευκολία σε μαθητές και καθηγητές, καθώς μπορούν να έχουν πρόσβαση σε υλικό μαθημάτων και να συμμετέχουν σε εικονικά μαθήματα από οπουδήποτε. Επίσης, η παράδοση περιεχομένου είναι ευκολότερη για τα συστήματα που βασίζονται στο cloud, γιατί μπορούν να χρησιμοποιηθούν για την παράδοση μεγάλων αρχείων πολυμέσων, όπως βίντεο και εικόνων, στους μαθητές γρήγορα και αποτελεσματικά, ανεξάρτητα από την τοποθεσία τους. Τα συστήματα τηλεδιάσκεψης, όπως είναι το Zoom και το Webex, για τη σύγχρονη μάθηση βασίζονται στο cloud για τη δημιουργία εικονικών αιθουσών διδασκαλίας. Τα εργαλεία ανάλυσης και διαχείρισης δεδομένων που βασίζονται στο cloud μπορούν να χρησιμοποιηθούν για την παρακολούθηση της προόδου των μαθητών, την παροχή εξατομικευμένων μαθησιακών εμπειριών και τη βελτίωση της συνολικής αποτελεσματικότητας της διαδικτυακής εκπαίδευσης. Τέλος οι υπηρεσίες αποθήκευσης που βασίζονται στο cloud, όπως το Google Drive, μπορούν να χρησιμοποιηθούν για την αποθήκευση και κοινή χρήση μεγάλων ποσοτήτων δεδομένων και αρχείων, στα οποία μπορούν να έχουν πρόσβαση μαθητές και καθηγητές από οπουδήποτε [30].



Εικόνα 7 : Κοινή αρχιτεκτονική των συστημάτων τηλεκπαίδευσης που βασίζονται σε cloud [29]

3

Χαρακτηριστικά ζητήματα ασφαλείας και απορρήτου

Η ασφάλεια των πληροφοριών κέρδισε την προσοχή σε όλους σχεδόν του τομείς της επιστήμης της πληροφορικής σε παγκόσμιο επίπεδο. Στην επιστημονική έρευνα, υπάρχουν διάφορες προσεγγίσεις για τον ορισμό της ασφάλειας πληροφοριών. Η Ασφάλεια Πληροφοριών μπορεί να οριστεί ως η προστασία των δεδομένων που μεταδίδονται μεταξύ των χρηστών στο Διαδίκτυο από οτιδήποτε μπορεί να το βλάψει, να το αλλάξει ή να το εκθέσει σε προβολή από άτομα χωρίς τα απαραίτητα δικαιώματα για αυτό [12]. Ο κάθε οργανισμός που έχει συστήματα πληροφορικής πρέπει να κατανοήσει τη σημασία των περιουσιακών του στοιχείων και να λαμβάνει όλα τα απαραίτητα μέτρα για την προστασία τους έστω και αν το κόστος, τουλάχιστον στην αρχή, είναι αυξημένο, γιατί σε θέματα ασφάλειας δεν πρέπει να υπάρχει κανένας συμβιβασμός. Εάν και όταν παρουσιαστεί κάποιο ζήτημα ασφαλείας, τότε αυτό θα πρέπει να ερευνηθεί διεξοδικά και να παρακολουθείται έστω και αν η πρώτη διάγνωση έδειξε ότι δεν υπάρχει πρόβλημα, διότι δεν είναι λίγες οι φορές που στην αρχή έχουμε ψευδώς αρνητική διάγνωση. Οι πληροφορίες που διακινούνται στον παγκόσμιο ιστό αρκετά συχνά είναι απροστάτευτες και εκτεθειμένες σε διάφορες απειλές και ζητήματα ασφάλειας. Ειδικά οι πληροφορίες που σχετίζονται με συστήματα τηλεκπαίδευσης, οι οποίες μπορεί να είναι ευαίσθητες, εμπιστευτικές και ιδιωτικές θα πρέπει να προφυλάσσονται από επιθέσεις και απειλές [31].

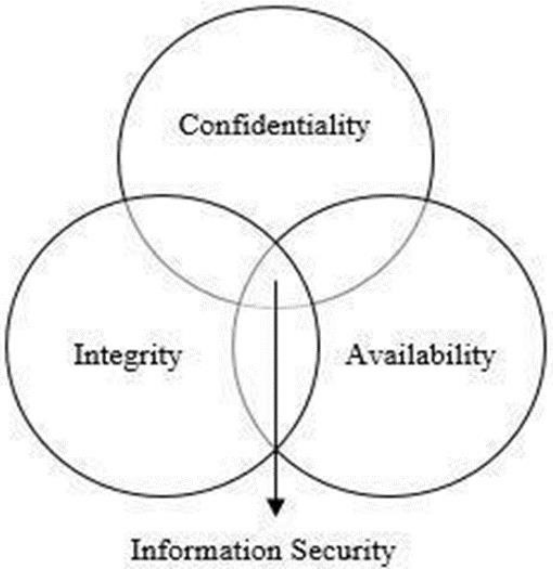
Η εξέλιξη της ηλεκτρονικής μάθησης ακολουθεί την εξέλιξη του Ιστού, η οποία εξηγείται από το γεγονός ότι έχουμε e-learning 1.0 (Web 1.0), e-learning 2.0 (Web 2.0) και e-learning 3.0 (Web 3.0). Αυτή είναι η κύρια αιτία που σχεδόν όλα τα συστήματα τηλεκπαίδευσης είναι εφαρμογές που βασίζονται στο διαδίκτυο. Έτσι τα συστήματα τηλεκπαίδευσης κληρονομούν εφαρμογές που βασίζονται στο διαδίκτυο, εργαλεία τηλεδιάσκεψης και μαζί με αυτά

κληρονομούν και τις ευπάθειες λογισμικού που αυτά έχουν όσον αφορά την ασφάλεια [7]. Πληθώρα δραστηριοτήτων και μια μεγάλη ποικιλία δημιουργικών εργασιών, καθώς και διαδραστικές μορφές επικοινωνίας μεταξύ εκπαιδευτών και εκπαιδευομένων, συμβάλλουν στην αποτελεσματικότητα της μαθησιακής διαδικασίας. Το πρόβλημα της διασφάλισης της ασφάλειας των πληροφοριών κατά τη διαδικασία της εξ αποστάσεως εκπαίδευσης είναι ιδιαίτερα επίκαιρο σήμερα. Αναζητώντας στη βιβλιογραφία αναφορές σχετικές με την τηλεκπαίδευση διαπιστώνουμε ότι θέματα σχετικά με τις δυνατότητες, τη χρήση και την αποτελεσματικότητα έχουν αναλυθεί και συζητηθεί αρκετά. Αντίθετα όμως για θέματα που αφορούν στην ασφάλεια της τηλεκπαίδευσης δεν υπάρχουν αρκετά άρθρα ιδιαίτερα πριν την εμφάνιση του COVID-19. Τα πιο κρίσιμα ελαττώματα ασφαλείας, όπως συζητούνται στη βιβλιογραφία, ταξινομούνται στις εξής ομάδες: έλεγχο ταυτότητας, διαθεσιμότητα, εμπιστευτικότητα και επιθέσεις ακεραιότητας [7].

3.1 Χαρακτηριστικά ασφαλείας

Σε αντίθεση με το περιβάλλον της τάξης, όπου ο εκπαιδευόμενος παραδίδει τις εργασίες του στον εκπαιδευτικό του απευθείας σε έντυπη μορφή, στο περιβάλλον ηλεκτρονικής τάξης που υλοποιούν τα συστήματα τηλεκπαίδευσης ο μαθητής πρέπει να υποβάλει την εργασία του σε ηλεκτρονική μορφή. Ο κίνδυνος παραβίασης αυτών των πληροφοριών είναι πολύ υψηλός γι' αυτό πρέπει να διασφαλίσουμε την επικοινωνία από τους πιθανούς κινδύνους. Υπάρχει επείγουσα ανάγκη, λοιπόν, να ξεπεράσουμε αυτούς τους κινδύνους, χρησιμοποιώντας απαιτήσεις ασφαλείας, όπως όνομα χρήστη και κωδικός πρόσβασης, βιομετρικά στοιχεία, κ.α.. Αν και οι απειλές για την ασφάλεια των πληροφοριών των συστημάτων τηλεκπαίδευσης δεν είναι απαραίτητα συγκεκριμένες, αυτό όμως δεν σημαίνει ότι ο κίνδυνος δεν ισχύει και για το σύστημα [5].

Πριν αναλύσουμε τις απειλές των συστημάτων τηλεκπαίδευσης, είναι απαραίτητο να περιγράψουμε τις βασικές αρχές για τη διασφάλιση της ποιότητας των διαδικτυακών μαθημάτων. Οι τρείς βασικοί πυλώνες (Εικόνα 8) της ασφάλειας των πληροφοριών (Information Security) είναι η εμπιστευτικότητα (Confidentiality), η ακεραιότητα (Integrity) και η διαθεσιμότητα (Availability). Δεν πρέπει να υπάρχει καμία ανοχή και κανένας συμβιβασμός γιατί σε περίπτωση που κάποιος από τους τρείς πυλώνες δεν μπορέσει να αμυνθεί σε μια επίθεση τότε ολόκληρο το περιβάλλον καταρρέει.



Εικόνα 8 : Πυλώνες Ασφάλειας Πληροφοριών[31]

Δύο ακόμη πυλώνες στους οποίους πρέπει να δίνεται ιδιαίτερη προσοχή στα συστήματα τηλεκπαίδευσης είναι η αυθεντικότητα και η μη αποποίηση.

3.1.1 Εμπιστευτικότητα - Confidentiality

Η εμπιστευτικότητα αναφέρεται στην προστασία ευαίσθητων πληροφοριών από την πρόσβαση μη εξουσιοδοτημένων ατόμων και την απουσία μη εξουσιοδοτημένης αποκάλυψης πληροφοριών. Όταν μόνο οι νόμιμοι συμμετέχοντες στη τηλεκπαίδευση μπορούν να δουν τις πληροφορίες του συστήματος τηλεκπαίδευσης, τότε η εμπιστευτικότητα διασφαλίζεται και οι πληροφορίες παραμένουν μυστικές από όλους εκτός από αυτούς που έχουν δικαίωμα πρόσβασης. Η εμπιστευτικότητα διασφαλίζει ότι οι πληροφορίες προστατεύονται και δεν μπορούν να έχουν πρόσβαση παράνομα πρόσωπα, συχνά όμως στις μέρες μας αυτού του είδους οι πληροφορίες δέχονται επίθεση. Σε ένα σύστημα τηλεκπαίδευσης συνήθως υπάρχει μεγάλος αριθμός χρηστών με διαφορετικούς ρόλους ο καθένας (μαθητής, εκπαιδευτικός, διαχειριστής κ.α.) γι' αυτό και απαιτούνται τόσο ένα σύστημα σύνδεσης όσο και μια ισχυρή σήμανση οριοθέτησης για κάθε διαφορετική ομάδα χρηστών διασφαλίζοντας ότι κάθε χρήστης θα έχει πρόσβαση μόνο στις πληροφορίες που τον αφορούν. Για παράδειγμα κατά τη λήψη ενός διαδικτυακού τεστ ή τη διενέργεια εξετάσεων η αρχή της εμπιστευτικότητας είναι πολύ σημαντική, καθώς πρέπει να διασφαλίζεται ότι το περιεχόμενό τους δεν θα είναι διαθέσιμο μέχρι την προγραμματισμένη ώρα και ότι το τεστ του μαθητή δεν θα είναι προσβάσιμο στους συμμαθητές του. Προκειμένου να προστατευθούν όλες αυτές οι πληροφορίες συνήθως εφαρμόζονται δικλείδες ασφαλείας, όπως η κρυπτογράφηση και ο έλεγχος ταυτότητας [4].

Η επίθεση εμπιστευτικότητας περιορίζει την πρόσβαση και τις δραστηριότητες διανομής δεδομένων χωρίς να εστιάζει στην αλλαγή του περιεχομένου δεδομένων. Τρεις είναι οι μεγάλες κατηγορίες που μπορούμε να διακρίνουμε σε μια τέτοια περίπτωση επίθεσης: ανασφαλής κρυπτογραφική αποθήκευση, μη ασφαλής άμεση αναφορά αντικειμένων, διαρροή πληροφοριών και ακατάλληλη διαχείριση σφαλμάτων [18].

- Μη ασφαλής κρυπτογραφική αποθήκευση: για την προστασία των δεδομένων στα συστήματα τηλεκπαίδευσης σπάνια χρησιμοποιούν κρυπτογραφικούς μηχανισμούς. Αυτό έχει ως αποτέλεσμα τα ευαίσθητα δεδομένα να αποθηκεύονται σε μια βάση δεδομένων χωρίς κρυπτογράφηση και έτσι να είναι πιο εύκολο να αποκαλυφθούν.
- Μη ασφαλής άμεση αναφορά αντικειμένου: πρόκειται για την έλλειψη μεθόδων εξουσιοδότησης από το ηλεκτρονικό σύστημα στις διεπαφές ιστού που χρησιμοποιεί για αναφορές αντικειμένων (κύρια κλειδιά, εγγραφές δεδομένων και αρχεία)
- Διαρροή πληροφοριών και ακατάλληλος χειρισμός σφαλμάτων: πραγματοποιείται όταν μέσω μηνυμάτων σφαλμάτων δύναται να αποκαλυφθούν ευαίσθητες πληροφορίες ή δεδομένα [18].

3.1.2 Διαθεσιμότητα - Availability

Διαθεσιμότητα είναι η διαβεβαίωση ότι τα δεδομένα του συστήματος τηλεκπαίδευσης είναι προσβάσιμα στον χρήστη οποιαδήποτε στιγμή, όποτε χρειάζεται και σε οποιαδήποτε τοποθεσία. Με άλλα λόγια διαθεσιμότητα είναι η ετοιμότητα για τη σωστή εξυπηρέτηση του χρήστη. Υποδηλώνει ότι ένα σύστημα τηλεκπαίδευσης μπορεί να είναι προσβάσιμο από εξουσιοδοτημένους χρήστες, όποτε χρειάζεται και διασφαλίζει ότι «οι πόροι πληροφοριών και επικοινωνίας είναι άμεσα προσβάσιμοι και αξιόπιστοι έγκαιρα από εξουσιοδοτημένα άτομα». Η διαθεσιμότητα του εκάστοτε συστήματος τηλεκπαίδευσης εξαρτάται πλήρως από τη διαθεσιμότητα της υπηρεσίας Διαδικτύου, το διαθέσιμο εύρος ζώνης, τον τύπο σύνδεσης στο Διαδίκτυο. Επίσης η ταχύτητα είναι πολύ σημαντική. Βασική αιτία για την παραβίαση της διαθεσιμότητας είναι κυρίως η άρνηση της υπηρεσίας ή/και η απώλεια των δυνατοτήτων επεξεργασίας δεδομένων [4].

Παρατηρείται συχνά, όταν σκεφτόμαστε την ασφάλεια, η διαθεσιμότητα να είναι μια απαίτηση που συχνά παραμελείται, παρόλο που έχει παρατηρηθεί ότι, εάν οι εφαρμογές βασίζονται στο διαδίκτυο ή είναι πολύ αργές λόγω επιθέσεων άρνησης υπηρεσίας, μειώνεται δραματικά οι παραγωγικότητα των χρηστών. Η διαθεσιμότητα υλικού και πληροφοριών προς πρόσβαση ανά πάσα στιγμή και σε οποιαδήποτε τοποθεσία είναι ζωτικής σημασίας για τους χρήστες των συστημάτων τηλεκπαίδευσης, γιατί, εάν μια πλατφόρμα τηλεκπαίδευσης είναι αργή, οι χρήστες όχι μόνο απογοητεύονται, αλλά χρειάζονται και περισσότερο χρόνο για να κάνουν τη δουλειά τους. Το γεγονός αυτό αυξάνει την αρνητική επίδραση στην παραγωγικότητα. Για την πρόληψη

της διαθεσιμότητας, που είναι το αντίθετο της άρνησης υπηρεσίας δεν υπάρχουν αποτελεσματικοί μηχανισμοί, ωστόσο μπορεί να ανιχνεύσει αυτόματα κανείς πότε συμβαίνει παρακολουθώντας τις εφαρμογές και τις συνδέσεις δικτύου για μια επίθεση άρνησης υπηρεσίας. Μόλις ένα περιστατικό συμβεί τότε με τα κατάλληλα αντιμέτρα μπορούν να περιοριστούν οι επιπτώσεις της επίθεσης [32].

3.1.3 Ακεραιότητα - Integrity

Ένα κρίσιμο στοιχείο ασφάλειας είναι η ακεραιότητα που αναφέρεται στην προστασία των δεδομένων από σκόπιμες ή τυχαίες μη εξουσιοδοτημένες αλλαγές. Ακεραιότητα σημαίνει ότι μόνο εξουσιοδοτημένα υποκείμενα (δηλαδή χρήστες ή προγράμματα υπολογιστών) επιτρέπεται να τροποποιούν δεδομένα (ή εκτελέσιμα προγράμματα). Διαβεβαιώνει ότι οι πληροφορίες και τα δεδομένα δεν παραποιούνται ή τροποποιούνται κατά λάθος ή κακόβουλα από μη εξουσιοδοτημένα άτομα και είναι ακριβώς στην αρχική τους μορφή. Έτσι, η ακεραιότητα διασφαλίζει ότι οι πληροφορίες είναι αναλλοίωτες και αξιόπιστες [4].

Η ακεραιότητα των προγραμμάτων και των δεδομένων είναι ένα πολύ σημαντικό θέμα παρόλο που συχνά στην καθημερινή ζωή συχνά παραμελείται. Η διασφάλιση της διαθεσιμότητας και της ακεραιότητας των πληροφοριών είναι ο κύριος στόχος σε σχέση με την ασφάλεια των συστημάτων τηλεκπαίδευσης. την Η ακεραιότητα των λειτουργικών συστημάτων και των προγραμμάτων είναι στενά συνδεδεμένη με το απόρρητο των δεδομένων και εάν παραβιαστεί η ακεραιότητα του λειτουργικού συστήματος, τότε η οθόνη αναφοράς (ένας μηχανισμός που διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση σε δεδομένα και να εκτελούν λειτουργίες) ενδέχεται να μην λειτουργεί πλέον σωστά. Εάν ο μηχανισμός που περιορίζει και ελέγχει την πρόσβαση στα δεδομένα δεν λειτουργεί, τότε είναι προφανές ότι το απόρρητο των πληροφοριών δεν μπορεί να διασφαλιστεί. Οπότε είναι πολύ σημαντικό να προστατεύεται η ακεραιότητα των λειτουργικών συστημάτων ώστε και το απόρρητο των ίδιων των δεδομένων να προστατεύεται [32].

Ο πρωταρχικός παράγοντας ακεραιότητας είναι ο έλεγχος πρόσβασης που είναι το κλειδί για τη διατήρηση της ακεραιότητας στα συστήματα τηλεκπαίδευσης. Δεν επιτρέπεται καμία παράνομη προσπάθεια τροποποίησης του περιεχομένου και μόνο εξουσιοδοτημένοι χρήστες μπορούν να ενημερώνουν και να έχουν πρόσβαση στα περιεχόμενα των δεδομένων. Ο κύριος στόχος στην ασφάλεια των συστημάτων τηλεκπαίδευσης είναι η συμμόρφωση με τη διαθεσιμότητα και την ακεραιότητα των δεδομένων [5].

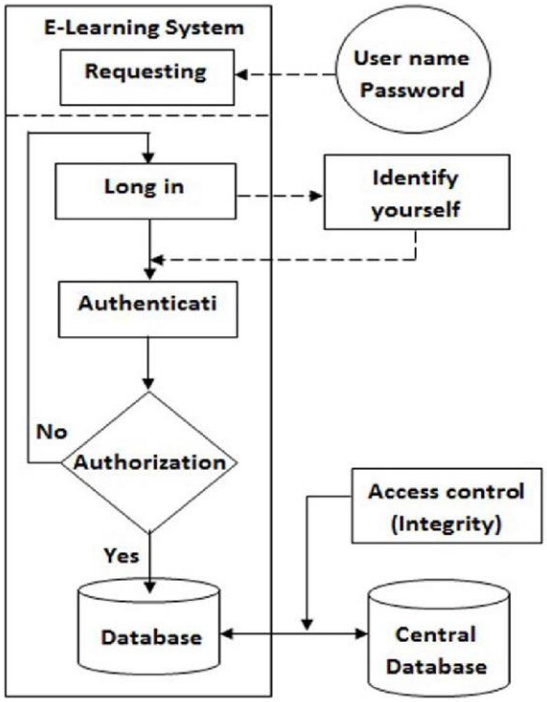
3.1.4 Αυθεντικοποίηση - Authentication

Ο έλεγχος ταυτότητας παρέχει έναν τρόπο αναγνώρισης ενός χρήστη και αναφέρεται στην επικύρωση της ταυτότητάς του πριν εκχωρηθεί η πρόσβαση και είναι μια ζωτική διαδικασία

για το εκάστοτε σύστημα τηλεκπαίδευσης. Για να διασφαλιστεί ότι όλες οι κοινοποιημένες πληροφορίες κατά τη διάρκεια της περιόδου λειτουργίας του συστήματος τηλεκπαίδευσης προστατεύονται, πριν παραχωρηθεί πρόσβαση στο σύστημα από τους χρήστες, ζητείται να εισαγάγουν ένα όνομα χρήστη και έναν κωδικό πρόσβασης [33].

Κάθε χρήστης έχει μοναδική ταυτότητα που θα πρέπει να ελέγχεται και να προστατεύεται πριν από την πρόσβαση και τη μετάδοση δεδομένων. Ο έλεγχος ταυτότητας είναι υποχρεωτικός για να διασφαλιστεί ότι ο νόμιμος μαθητής ή εκπαιδευτικός έχει πρόσβαση στο σύστημα. Η προστασία της ταυτότητας των μαθητών και των εκπαιδευτικών είναι πρωταρχικής σημασίας στον κυβερνοχώρο. Με την ανάπτυξη της τεχνολογίας όμως οι χάκερ έχουν νέα εργαλεία και μεθόδους για να υποκλέψουν την ταυτότητα των χρηστών. Ως εκ τούτου, για ένα σύστημα τηλεκπαίδευσης η αξιόπιστη ταυτοποίηση του χρήστη είναι ένας βασικός παράγοντας καθώς αποτελεί τη βάση για τον έλεγχο πρόσβασης. Μόλις αναγνωριστεί ο χρήστης, τότε απαιτείται να επαληθευτεί ότι είναι ο ίδιος με το άτομο που ισχυρίζεται ότι είναι [34].

Ο τρόπος επαλήθευσης της ταυτότητας ενός χρήστη είναι ο έλεγχος ταυτότητας με τη λήψη κάποιου είδους πιστοποιητικών και τη χρήση αυτών των πιστοποιητικών για την επαλήθευση της ταυτότητας του. Η διαδικασία ελέγχου ταυτότητας οδηγεί πάντα στη διαδικασία εξουσιοδότησης μόνο εάν τα πιστοποιητικά είναι έγκυρα. Η εικόνα 9 περιγράφει πώς γίνεται ο έλεγχος ταυτότητας και η εξουσιοδότηση σε έναν βασικό κύκλο ζωής μιας διαδικασίας ονόματος χρήστη/κωδικού πρόσβασης κατά τη διάρκεια της σύνδεσης στο σύστημα ηλεκτρονικής μάθησης, κάθε εκπαιδευόμενος έχει ένα μοναδικό όνομα χρήστη και κωδικό πρόσβασης για να επιτρέψει την ιεραρχική πρόσβαση στα διαδικτυακά δεδομένα. Επίσης κάθε φορά που ένας μαθητής προσπαθεί να αποκτήσει πρόσβαση στο διαδικτυακό υλικό χρειάζεται ξανά η διαδικασία επαλήθευσης ταυτότητας. Αν όμως ένας νόμιμος χρήστης με κακόβουλη πρόθεση θέλει να προκαλέσουν ζημιά στο περιεχόμενο τότε δεν μπορεί κανείς να τον εμποδίσει [5]. Επιθέσεις ελέγχου ταυτότητας συμβαίνουν, όταν οι χάκερ αποκτούν παράνομα τους κωδικούς πρόσβασης των χρηστών και προσπαθούν να έχουν ελεύθερη πρόσβαση στο υλικό των συστημάτων τηλεκπαίδευσης. Επιπλέον, όταν συμβαίνει αυτή η επίθεση, είναι εύκολο για τους χάκερ να έχουν την ευκαιρία να εκτελέσουν άλλους τύπους επιθέσεων, για παράδειγμα, επιθέσεις διαθεσιμότητας, εμπιστευτικότητας και ακεραιότητας [18].



Εικόνα 9 : Διαδικασία ελέγχου ταυτότητας [5]

3.1.5 Μη άρνηση - Non Repudiation

Το τελευταίο βήμα προς την επιβολή της ασφάλειας των πληροφοριών είναι η μη άρνηση ή αλλιώς μη απόρριψη ή μη αποκήρυξη. Η μη άρνηση επιβάλλει στους νόμιμους χρήστες να μην αρνούνται την ολοκληρωμένη λειτουργία που έχουν κάνει. Για παράδειγμα, εάν ένας εκπαιδευόμενος υποβάλει την εργασία του/της δεν πρέπει να αρνηθεί την υποβολή του υλικού του. Οι μαθητές μπορεί να αρνηθούν την αποδοχή πληροφοριών ή να διαφωνήσουν να συμμετάσχουν σε οποιαδήποτε συναλλαγή εγγράφων γι' αυτό και απαιτείται ένας συστηματικός και επίσημος μηχανισμός προκειμένου να εξαναγκαστούν οι εγγεγραμμένοι χρήστες να μη μπορούν να αρνηθούν την εργασία ή τις τροποποιήσεις που έχουν πραγματοποιήσει στο σύστημα [34].

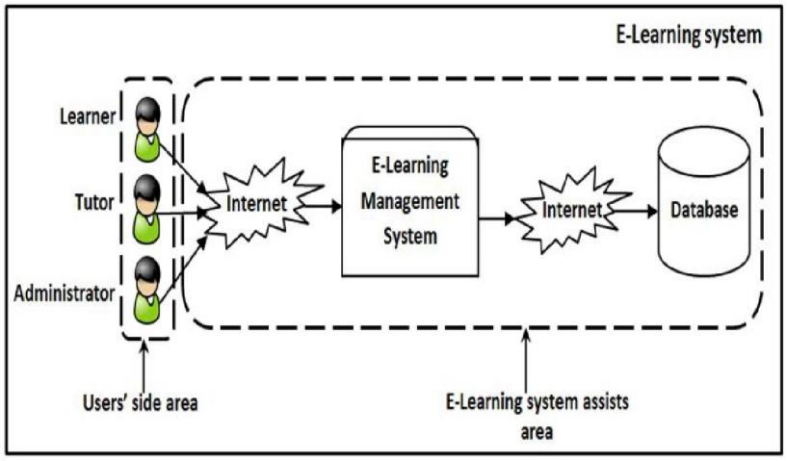
Η μη άρνηση σημαίνει ότι οι χρήστες δεν είναι σε θέση να αρνηθούν ότι έχουν πραγματοποιήσει συναλλαγές. Οι σημαντικές πληροφορίες, όπως οι ερωτήσεις των εξετάσεων, οι σωστές απαντήσεις και οι απαντήσεις που επιλέγει ο μαθητής πρέπει να αποθηκεύονται έτσι ώστε να μην είναι δυνατή καμία τροποποίηση. Ορισμένες δραστηριότητες στα συστήματα τηλεκπαίδευσης απαιτούν την εφαρμογή μη άρνησης, ειδικά για δραστηριότητες που επηρεάζουν τη βαθμολόγηση, όπως η λήψη ενός κουίζ ή η υποβολή μιας εργασίας [33]. Ως εκ τούτου, απαιτούνται μηχανισμοί καταγραφής που καταγράφουν όλες τις δραστηριότητες των χρηστών. Ένα άλλο αντίμετρο για τη μη άρνηση είναι η ψηφιακή υπογραφή [32].

Αυτός ο όρος χρησιμοποιείται, όταν οποιοσδήποτε χρήστης δεν μπορεί να αρνηθεί ότι έχει στείλει μηνύματα. Εξασφαλίζει την ιδιοκτησία των ενεργειών του χρήστη μέσω ψηφιακών υπογραφών, ώστε ο χρήστης να μην μπορεί να αρνηθεί ενέργειες όπως η πρόσβαση στο σύστημα ή ανταλλαγή μηνυμάτων κ.α. Οι μαθητές και οι εκπαιδευτικοί λόγω της εξ αποστάσεως εκπαίδευσης, ενδέχεται να μην συμπεριφέρονται αναμενόμενα παραδείγματος χάρη οι μαθητές μπορεί να μην ολοκληρώσουν την εργασία που τους έχει ανατεθεί με ειλικρίνεια ή μπορεί να καθυστερήσουν ή να αρνηθούν πλήρως την εργασία που τους έχει ανατεθεί. Η καλύτερη λύση για να αποφευχθεί η άρνηση είναι το βιομετρικό σύστημα μαζί με ψηφιακές υπογραφές και ασύμμετρη κρυπτογράφηση, όπου το ιδιωτικό κλειδί χρησιμοποιείται για την υπογραφή και το δημόσιο κλειδί χρησιμοποιείται για τη διαδικασία επαλήθευσης [35].

3.2 Τύποι επιθέσεων στο σύστημα ηλεκτρονικής μάθησης

Η κατανόηση των θεμάτων ασφάλειας σε συστήματα τηλεκπαίδευσης βοηθά τους χρήστες προστατεύσουν τα περιουσιακά στοιχεία και να αποφύγουν απειλές για την ασφάλεια καθώς και να βελτιώσουν την προστασία τόσο των συστημάτων αλλά και των χρηστών. Συνηθισμένοι στόχοι των περιουσιακών στοιχείων σε συστήματα τηλεκπαίδευσης είναι το περιεχόμενο των συστημάτων τηλεκπαίδευσης, τα προσωπικά δεδομένα των χρηστών, το εύρος ζώνης και τα μηνύματα που διακινούνται μεταξύ των χρηστών.

Μπορούμε να χωρίσουμε τις επιθέσεις σε στοιχεία ηλεκτρονικής μάθησης με βάση την περιοχή που πραγματοποιείται η επίθεση χωρίζοντάς τες σε δύο περιοχές, όπως παρουσιάζεται στην Εικόνα 10, κάθε περιοχή που περικλείεται με διακεκομμένη γραμμή. Η πρώτη περιοχή αφορά τις επιθέσεις που συμβαίνουν στην πλευρά των χρηστών, όπως οι επιθέσεις ελέγχου ταυτότητας. Η δεύτερη περιοχή αφορά επιθέσεις, οι οποίες συμβαίνουν στην πλευρά του συστήματος διαχείρισης ηλεκτρονικής μάθησης, όπως επιθέσεις ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας. Σε αυτή την ενότητα, θα αναλυθούν οι επιθέσεις σε συστήματα τηλεκπαίδευσης.



Εικόνα 10 : Τύποι επιθέσεων και περιοχή που συμβαίνουν [5]

Δεδομένου ότι η τηλεκπαίδευση πραγματοποιείται μέσω του Διαδικτύου, κάθε στοιχείο μπορεί να αποτελέσει πιθανό στόχο εισβολής ή άλλων κακόβουλων επιθέσεων. Αυτό μπορεί να έχει ως συνέπεια την μη εξουσιοδοτημένη τροποποίηση ή/και καταστροφή εκπαιδευτικών περιουσιακών στοιχείων. Τα συστήματα τηλεκπαίδευσης έχουν προσελκύσει την προσοχή των εγκληματιών του διαδικτύου που έχουν ιδιαίτερες ικανότητες στο να παραβιάζουν τέτοια συστήματα. Ως εκ τούτου, καθώς τα χαρακτηριστικά των διαδικτυακών συστημάτων μάθησης γίνονται πιο περίπλοκα, εκτίθενται ολοένα και περισσότερο σε απειλές για την ασφάλεια [36]. Μερικές από τις πιο κοινές επιθέσεις στο διαδίκτυο για συστήματα τηλεκπαίδευσης [31] είναι οι εξής:

3.2.1 Κακόβουλες επιθέσεις και απειλές για την ασφάλεια στο περιβάλλον συστημάτων τηλεκπαίδευσης

Οι κυριότερες απειλές για την ασφάλεια που ενδέχεται να συμβούν σε ένα σύστημα τηλεκπαίδευσης είναι:

Ιός (Virus): Ο ιός είναι ένα κακόβουλο πρόγραμμα, που συνήθως εγκαθίσταται σε έναν υπολογιστή εν αγνοία του χρήστη και ενεργοποιείται σε προκαθορισμένο χρόνο ή μετά από μια συγκεκριμένη ενέργεια για να προκαλέσει ζημιά στο σύστημα. Οι ιοί ενσωματώνονται σε μηνύματα ηλεκτρονικού ταχυδρομείου ή προγράμματα και το άνοιγμα ή η εκτέλεση ενός προγράμματος ενεργοποιεί ακούσια τον ιό. Οι ιοί δημιουργούν αντίγραφα του εαυτού τους και εξαπλώνονται σε ολόκληρο το σύστημα. Ο γραπτός κακόβουλος κώδικας ή τα σενάρια που περιέχει ο ιός ενδέχεται να επηρεάσουν σοβαρά το σύστημα. Συγκεκριμένα, μπορεί να έχει ως αποτέλεσμα τη κατάληψη μεγάλου χώρου στον σκληρό δίσκο, την καταστροφή αρχείων και φακέλων, την αργή εκκίνηση του υπολογιστή ή άλλες βλάβες [31].

Σκουλήκι (Worm): Ένα worm είναι ένα κακόβουλο πρόγραμμα που αναπαράγει τον εαυτού του και εξαπλώνεται στο δίκτυο των υπολογιστών που είναι διασυνδεδεμένοι σε αυτό. Το δίκτυο θεωρείται ως το μέσο για την εξάπλωση του σκουληκιού. Η επίδραση του τύπου worm είναι να εκμεταλλεύεται ευπάθειες στο λογισμικό ασφαλείας για να κλέψει ευαίσθητες πληροφορίες, να εγκαταστήσει κερκόπορτες που μπορούν να χρησιμοποιηθούν για πρόσβαση στο σύστημα, για καταστροφή αρχείων και για άλλου είδους βλάβη. Τα σκουλήκια καταναλώνουν μεγάλους όγκους μνήμης, καθώς και εύρος ζώνης. Αυτό έχει ως αποτέλεσμα οι διακομιστές, τα μεμονωμένα συστήματα και τα δίκτυα να υπερφορτώνονται και να δυσλειτουργούν

Δούρειος ίππος (Trojan horse): Ο Δούρειος ίππος είναι ένας τύπος κακόβουλου λογισμικού που «μεταμφιέζεται» ως έγκυρο και επίσημο. Σε αντίθεση με άλλους τύπους ιών, οι δούρειοι ίπποι δεν πολλαπλασιάζονται. Με την εγκατάσταση αυτού του λογισμικού στη συσκευή ενός χρήστη, οι εγκληματίες του κυβερνοχώρου προσπαθούν να αποκτήσουν πρόσβαση στα ευαίσθητα αρχεία και τα προσωπικά δεδομένα του χρήστη. Μετά τη φόρτωση του δούρειου ίππου στον υπολογιστή κυβερνοεγκληματίες, μπορούν να πραγματοποιήσουν ορισμένες ενέργειες, χωρίς τη συναίνεση του χρήστη όπως η απομακρυσμένη ακρόαση, η παράνομη πρόσβαση στο σύστημα, η διαταραχή της απόδοσης του υπολογιστή του χρήστη, η κλοπή δεδομένων κ.α.

Κακόβουλο λογισμικό (Malware): Η λέξη malware αποτελεί έναν συνδυασμό των λέξεων "malicius" (κακόβουλο) και "software" (λογισμικό). Ο συγκεκριμένος όρος, επομένως, περιγράφει οποιαδήποτε μορφή κακόβουλου κώδικα, ανεξάρτητα από το πώς συμπεριφέρεται, πώς προσβάλλει τα θύματα ή τι ζημιά προκαλεί. Το κακόβουλο λογισμικό είναι ένα κακόβουλο πρόγραμμα που προκαλεί επιβλαβείς επιπτώσεις ή ανεπιθύμητες δραστηριότητες που εκτελούνται στον υπολογιστή.

Adware: Το Adware (ή λογισμικό διαφήμισης) χρησιμοποιείται για να περιγράψει διάφορες αναδυόμενες διαφημίσεις που εμφανίζονται στον υπολογιστή ή την κινητή συσκευή σας. Το adware είναι κακόβουλο λογισμικό που μπορεί να βλάψει τη συσκευή σας επιβραδύνοντας την, παρεμβαίνοντας στο πρόγραμμα περιήγησής σας ή εγκαθιστώντας ιούς ή spyware. Ακόμη μπορεί να οδηγήσει σε κλοπή ταυτότητας με την αρπαγή διαπιστευτηρίων από τους χρήστες ή μπορεί να πραγματοποιήσει λήψη άλλου κακόβουλου λογισμικού.

Λογισμικό κατασκοπίας (Spyware): Λογισμικό κατασκοπίας που διεισδύει στον υπολογιστή με κύρια πρόθεση να συλλέξει στοιχεία για το μεμονωμένο άτομο ή ίδρυμα, τα στοιχεία που παρακολουθούνται θα ανακατευθυνθούν στον εισβολέα ή στο σύστημα που είναι συνδεδεμένο. Το spyware δεν είναι τόσο καταστροφικό για τις συσκευές των χρηστών, αλλά συχνά χρησιμοποιείται παράνομα για τη συλλογή δεδομένων, όπως αριθμούς πιστωτικών καρτών ή

πληροφορίες τραπεζικών λογαριασμών, χωρίς τη συγκατάθεση του χρήστη. Ο αντίκτυπος του spyware μπορεί να οδηγήσει σε παρακολούθηση του συστήματος.

Rootkit: Το Rootkit είναι ένα κακόβουλο λογισμικό που εκτελείται τη στιγμή της εκκίνησης και παρέχουν σε εισβολείς απεριόριστη πρόσβαση σε ένα σύστημα, ενώ αποκρύπτουν την παρουσία τους. Είναι πολύ δύσκολο να αναγνωριστούν αφού ξεκινούν νωρίτερα από την εκκίνηση του λειτουργικού συστήματος για αυτόν το λόγο, είναι σχεδόν αδύνατη η ανίχνευσή τους χρησιμοποιώντας συνηθισμένες τεχνικές ελέγχου. Περιλαμβάνουν εγκατάσταση μη εμφανισμένων αρχείων, κακόβουλων λογαριασμών χρηστών [31].

3.2.2 Επιθέσεις στην πλευρά του χρήστη σε σύστημα τηλεκπαίδευσης

Cross-site Scripting ή XSS: Το XSS είναι ένας συχνός τρόπος μόλυνσης μιας ιστοσελίδας, με τον οποίον εισάγεται κακόβουλος κώδικας, σε μια ευάλωτη γραμμή κώδικα της ιστοσελίδας. Οι εισβολείς που εκμεταλλεύονται επιθέσεις XSS μπορούν να πάρουν τον έλεγχο του λογαριασμού του χρήστη και να κλέψουν προσωπικές πληροφορίες και να ενεργοποιήσουν προγράμματα Trojan. Επίσης, μπορούν να τροποποιήσουν το περιεχόμενο της μολυσμένης σελίδας, και να παραπλανήσουν τον χρήστη ώστε να παραδώσει οικειοθελώς τα προσωπικά του username/password ή να ανακατευθύνουν τον χρήστη σε κακόβουλους ιστότοπους [37].

Ψάρεμα (Phishing): Το ηλεκτρονικό ψάρεμα είναι μια προσπάθεια απόκτησης των ιδιωτικών διαπιστευτηρίων του χρήστη. Πρόκειται για μια μορφή επίθεσης κοινωνικής μηχανικής, στην οποία ο επιτιθέμενος μιμείται μια αξιόπιστη οντότητα, ζητώντας από το θύμα να αποκαλύψει ευαίσθητες πληροφορίες. Αμέσως μετά την εμφάνιση του COVID-19 και τη μαζική μετάβαση στην εξ' αποστάσεως εκπαίδευση μια σειρά από ιστοτόπους ηλεκτρονικού ψαρέματος (phishing) για δημοφιλή συστήματα τηλεκπαίδευσης, όπως το Zoom και το Moodle, άρχισαν να εμφανίζονται. Εκτός όμως από ψεύτικες ιστοσελίδες μεγάλος ήταν και αριθμός των ηλεκτρονικών μηνυμάτων (email) ηλεκτρονικού ψαρέματος. Οι χρήστες κινδύνευαν να μολυνθούν από διάφορες απειλές, αν άνοιγαν τα email και έκαναν κλικ σε οποιονδήποτε σύνδεσμο [8].

Παραπλάνηση περιεχομένου (Content Spoofing): Η πλαστογράφηση περιεχομένου, γνωστή και ως έγχυση περιεχομένου, είναι ένας τύπος επίθεσης στον κυβερνοχώρο κατά την οποία ένας εισβολέας τροποποιεί ή εισάγει περιεχόμενο σε έναν ιστότοπο χωρίς τη γνώση ή τη συγκατάθεση του κατόχου ή του διαχειριστή του ιστότοπου. Αυτό μπορεί να γίνει με την εκμετάλλευση ευπαθειών στον κώδικα του ιστότοπου ή με τη χρήση τεχνικών phishing ή κοινωνικής μηχανικής για να εξαπατήσει έναν διαχειριστή, ώστε να δώσει στον εισβολέα πρόσβαση στον ιστότοπο. Μόλις ο εισβολέας έχει πρόσβαση, μπορεί στη συνέχεια να τροποποιήσει το περιεχόμενο του ιστότοπου για να διαδώσει κακόβουλο λογισμικό, να κλέψει προσωπικές πληροφορίες ή να ανακατευθύνει τους χρήστες σε κακόβουλους ιστότοπους. Η

πλαστογράφηση περιεχομένου μπορεί επίσης να χρησιμοποιηθεί για την πλαστοπροσωπία ενός νόμιμου ιστότοπου, προκειμένου να εξαπατήσει τους χρήστες να παρέχουν ευαίσθητες πληροφορίες ή να κάνουν κλικ σε κακόβουλους συνδέσμους.

Η διαφορά μεταξύ της πλαστογράφησης περιεχομένου με την Cross-Site Scripting (XSS) είναι ότι η δεύτερη χρησιμοποιεί JavaScript κώδικα, οπότε, αν σε μια εφαρμογή χρησιμοποιούνται αντίμετρα για τη προστασία από XSS επιθέσεις, αυτό δεν επαρκεί για την προστασία της από επιθέσεις πλαστογράφησης περιεχομένου που βασίζονται σε απλό κείμενο. Για να αποφευχθεί η πλαστογράφηση περιεχομένου, οι ιδιοκτήτες ιστοτόπων θα πρέπει να διασφαλίζουν ότι ο ιστότοπός τους είναι σωστά ασφαλισμένος και ότι όλο το λογισμικό διατηρείται ενημερωμένο, καθώς και να εκπαιδεύουν τους χρήστες τους σχετικά με τους κινδύνους του phishing και της κοινωνικής μηχανικής.

Clickjacking: Clickjacking είναι μία τεχνική επίθεσης που παραπλανεί τους χρήστες να κάνουν κλικ σε ένα κουμπί ή σύνδεσμο σε μια ιστοσελίδα, όταν στην πραγματικότητα κάνουν κλικ σε κάτι άλλο. Αυτό μπορεί να πραγματοποιηθεί επικαλύπτοντας ένα κουμπί ή σύνδεσμο με ένα διαφανές στρώμα και παραπλανώντας τον χρήστη να κάνει κλικ σε αυτό. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει αυτό το κλικ για να εκτελέσει μία ενέργεια σε όνομα του χρήστη, όπως να κάνει μία αγορά ή να κλέψει προσωπικά δεδομένα. Αυτή η τεχνική έχει απεριόριστες χρήσεις, όταν πρόκειται για εκμετάλλευση των χρηστών. Για παράδειγμα, μια τέτοια επίθεση μπορεί να χρησιμοποιηθεί για να διανεμηθεί malware ή να ξεκινήσουν επιθέσεις phishing [31].

Επίθεση ωμής βίας (Brute force attack): Η επίθεση ωμής βίας χρησιμοποιεί τη διαδικασία δοκιμής και σφάλματος για να αποκτήσει τα διαπιστευτήρια χρήστη. Αυτή η επίθεση μαντεύει κωδικούς πρόσβασης και ονόματα χρήστη στέλνοντας πολλές απαιτήσεις στον διακομιστή ιστού με ένα κενό πεδίο cookie για να μηδενίσει τον αριθμό αποτυχιών σύνδεσης. Ο εισβολέας χρησιμοποιεί αυτοματοποιημένα εργαλεία για να δοκιμάσει μεγάλο αριθμό διαφορετικών εισόδων, όπως κωδικούς πρόσβασης ή κλειδιά, προκειμένου να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα ή δίκτυο. Η τεχνική «brute force» χρησιμοποιεί 92 χαρακτήρες που αποτελούνται από τα 26 γράμματα του αγγλικού αλφάβητου, πεζά και κεφαλαία (52 συνολικά), αριθμούς από το 0 έως το 9 και όλα τα σύμβολα και τα σημεία στίξης (32). Όταν ο εισβολέας γνωρίζει το μήκος του κωδικού πρόσβασης, μπορεί να το μαντέψει από έναν περιορισμένο αριθμό προσπαθειών, αλλά αν δεν γνωρίζει το μήκος του, ο αριθμός των προσπαθειών, αν και περιορισμένος, είναι εξαιρετικά μεγάλος. Ο εισβολέας χρησιμοποιεί ένα σενάριο ή πρόγραμμα για να προσπαθήσει επανειλημμένα να συνδεθεί, χρησιμοποιώντας διαφορετικούς συνδυασμούς εισόδων, μέχρι να βρει τον σωστό. Οι επιθέσεις ωμής βίας μπορούν να χρησιμοποιηθούν για την απόκτηση πρόσβασης σε ένα ευρύ φάσμα συστημάτων, συμπεριλαμβανομένων διακομιστών, ιστοτόπων και μεμονωμένων λογαριασμών χρηστών. Μπορούν επίσης να χρησιμοποιηθούν για να σπάσουν την κρυπτογράφηση, δοκιμάζοντας κάθε

δυνατό κλειδί μέχρι να βρεθεί το σωστό. Για να αποτραπούν επιθέσεις ωμής βίας, είναι σημαντικό να χρησιμοποιούνται ισχυροί κωδικοί πρόσβασης και να περιορίζεται ο αριθμός των προσπαθειών σύνδεσης που μπορούν να πραγματοποιηθούν, πριν κλειδωθεί ο λογαριασμός. Επιπλέον, μέτρα ασφαλείας όπως ο έλεγχος ταυτότητας δύο παραγόντων και ο αποκλεισμός IP μπορούν επίσης να βοηθήσουν στην αποτροπή επιθέσεων ωμής βίας [13].

Επίθεση πειρατείας συνεδρίας (session hijacking attack): Μια επίθεση πειρατείας συνεδρίας στην ηλεκτρονική μάθηση αναφέρεται σε έναν τύπο κυβερνοεπίθεσης, κατά τον οποίο ένας εισβολέας παρεμποδίζει και αναλαμβάνει μια ενεργή συνεδρία μεταξύ ενός χρήστη και μιας πλατφόρμας ηλεκτρονικής μάθησης. Αυτό μπορεί να γίνει με την εκμετάλλευση τρωτών σημείων στο δίκτυο ή την εφαρμογή Ιστού ή με τη χρήση εργαλείων για τη λήψη και την επανάληψη των cookies περιόδου λειτουργίας. Μόλις ο εισβολέας έχει παραβιάσει τη συνεδρία, μπορεί να έχει πρόσβαση στον λογαριασμό του χρήστη και να εκτελέσει ενέργειες για λογαριασμό του, όπως προβολή ή τροποποίηση υλικού μαθημάτων, υποβολή εργασιών ή προβολή προσωπικών πληροφοριών. Για να αποτραπούν επιθέσεις πειρατείας συνεδρίας, είναι σημαντικό να εφαρμόζονται ασφαλή πρωτόκολλα για τη δημιουργία και τη διατήρηση της κατάστασης περιόδου λειτουργίας, όπως η χρήση ασφαλών cookie και η κρυπτογράφηση δεδομένων συνεδρίας. Επιπλέον, η χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων μπορεί να βοηθήσει στην περαιτέρω ασφάλεια της συνεδρίας. Για παράδειγμα το Moodle χειρίζεται τη συνεδρία χρησιμοποιώντας δύο cookies: το MoodleSession και το MoodleSessionTest τα οποία όμως μπορούν να υποκλαπούν και να αποκωδικοποιηθούν, επειδή το Moodle χρησιμοποιεί μόνο SSL (Secure Socket Layer) κανάλια στην υπηρεσία σύνδεσης και τα αιτήματα HTTP γίνονται σε απλό κείμενο. Ένας εισβολέας μπορεί να χρησιμοποιήσει αυτά τα δεδομένα στο δικό του αίτημα HTTP αμέσως μόλις λάβει το cookie και έτσι να αναλάβει τον έλεγχο της περιόδου σύνδεσης χρήστη-στόχου. Ο μόνος τρόπος για να αποτραπεί αυτό είναι η χρησιμοποίηση του πρωτοκόλλου SSL [32].

Επίθεση ελέγχου ταυτότητας (Authentication attack): Μια επίθεση ελέγχου ταυτότητας στα συστήματα τηλεκπαίδευσης αναφέρεται σε έναν τύπο κυβερνοεπίθεσης στον οποίο ένας εισβολέας επιχειρεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε μια πλατφόρμα τηλεκπαίδευσης, επιχειρώντας να παρακάμψει τα πρωτόκολλα ελέγχου ταυτότητας του συστήματος. Αυτό μπορεί να γίνει, όταν ο εισβολέας επιχειρεί να μαντέψει ή σπάσει τους κωδικούς πρόσβασης, εκμεταλλευόμενος τρωτά σημεία στο σύστημα ή χρησιμοποιώντας τακτικές κοινωνικής μηχανικής για να εξαπατήσει τους χρήστες να δώσουν τα διαπιστευτήρια σύνδεσής τους. Ο στόχος μιας τέτοιας επίθεσης είναι συνήθως η κλοπή προσωπικών πληροφοριών ή η διακοπή της κανονικής λειτουργίας της πλατφόρμας. Για την αποτροπή τέτοιων επιθέσεων, είναι σημαντικό να εφαρμόζονται ισχυρά πρωτόκολλα ελέγχου ταυτότητας

και μέτρα ασφαλείας και να εκπαιδεύονται οι χρήστες σχετικά με τις βέλτιστες πρακτικές για την προστασία των προσωπικών τους πληροφοριών.

Zoombombing: Αυτή η επίθεση υποδηλώνει ανεπιθύμητους και ενοχλητικούς εισβολείς που συμμετέχουν και διακόπτουν μια συνάντηση με επιθετική ομιλία. Αυτό το κάνουν μαντεύοντας ή αποκτώντας τη μοναδική διεύθυνση URL ή το αναγνωριστικό της σύσκεψης και, στη συνέχεια, συμμετέχοντας στην κλήση με προσβλητικό ή ενοχλητικό περιεχόμενο. Αυτό μπορεί να περιλαμβάνει την κοινή χρήση πορνογραφικών εικόνων, τη δημιουργία ρατσιστικών σχολίων ή ρητορικής μίσους ή την αναπαραγωγή δυνατών ή ενοχλητικών ήχων. Αν και ο όρος προέρχεται από το όνομα της εφαρμογής Zoom, το φαινόμενο εμφανίζεται και στις άλλες εφαρμογές τηλεδιάσκεψης. Το Zoombombing αυξήθηκε κατακόρυφα κατά τη διάρκεια της πανδημίας COVID-19 καθώς περισσότεροι άνθρωποι χρησιμοποιούν το Zoom και άλλες πλατφόρμες τηλεδιάσκεψης για εργασία, σχολείο και προσωπική χρήση. Σε γενικές γραμμές, το zoombombing ως φαινόμενο μόλις και μετά βίας υπήρχε πριν από την καραντίνα. Η αύξησή του κατά την πανδημία συνάδει με το γεγονός ότι οι περισσότερες προσκλήσεις για zoombombing στοχεύουν εκπαιδευτικές τηλεδιασκέψεις. Για να αποτραπεί το Zoombombing, συνιστάται στους χρήστες να δημιουργούν ισχυρούς κωδικούς πρόσβασης, να χρησιμοποιούν τη λειτουργία της αίθουσας αναμονής, να κλειδώνουν τη σύσκεψη μόλις ξεκινήσει και να αναφέρουν οποιαδήποτε ύποπτη ενέργεια [38].

3.2.3 Επιθέσεις στο περιβάλλον του συστήματος τηλεκπαίδευσης

Sniffing: Το sniffing στην απλούστερη μορφή του, είναι η πράξη παρακολούθησης και υποκλοπής της κυκλοφορίας σε ένα δίκτυο με σκοπό την εξαγωγή ευαίσθητων πληροφοριών, όπως διαπιστευτήρια σύνδεσης ή προσωπικές πληροφορίες. Αυτό μπορεί να γίνει με τη χρήση εξειδικευμένου λογισμικού για την παρακολούθηση και ανάλυση της κυκλοφορίας του δικτύου. Το sniffing μπορεί να αποτελεί σημαντικό πρόβλημα για την ασφάλεια σε περιβάλλοντα ηλεκτρονικής μάθησης, καθώς μπορεί να επιτρέψει μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες και να διαταράξει τη διαδικασία μάθησης. Για να αποτρέψουν το sniffing, οι οργανισμοί μπορούν να χρησιμοποιούν κρυπτογράφηση, τείχη προστασίας και ασφαλή πρωτόκολλα δικτύου για την προστασία των δικτύων τους και των δεδομένων των χρηστών. Επιπλέον, οι πλατφόρμες και οι εφαρμογές ηλεκτρονικής μάθησης θα πρέπει να σχεδιάζονται με γνώμονα την ασφάλεια και να ενημερώνονται τακτικά για την αντιμετώπιση γνωστών τρωτών σημείων [36].

Άρνηση υπηρεσίας (Denial-of-Service (DoS)): Οι επιθέσεις Denial-of-Service (DoS) στις πλατφόρμες τηλεκπαίδευσης αφορούν επιθέσεις στον κυβερνοχώρο που στοχεύουν να διακόψουν ή να αρνηθούν την πρόσβαση σε πλατφόρμες, διακομιστές ή υπηρεσίες ηλεκτρονικής μάθησης κατακλύζοντάς τις με κίνηση ή αιτήματα. Αυτό μπορεί να εμποδίσει

τους μαθητές να έχουν πρόσβαση στο εκπαιδευτικό υλικό και να διαταράξει τη μαθησιακή διαδικασία.

Μια επίθεση DoS σε μια πλατφόρμα ηλεκτρονικής μάθησης μπορεί να έχει πολλές συνέπειες, όπως:

• Διακοπή πρόσβασης σε υλικό μαθημάτων, εργασίες και αξιολογήσεις για μαθητές.

• Αποτροπή μαθητών από την υποβολή της εργασίας τους ή τη συμμετοχή σε διαδικτυακές εξετάσεις.

• Υπερφόρτωση διακομιστών και δικτύων, με αποτέλεσμα να διακοπούν ή να μην είναι διαθέσιμα.

• Διακοπή της επικοινωνίας και της συνεργασίας μεταξύ μαθητών και εκπαιδευτών.

Για την προστασία από επιθέσεις DoS σε περιβάλλοντα ηλεκτρονικής μάθησης, οι οργανισμοί μπορούν να χρησιμοποιήσουν τείχη προστασίας, συστήματα ανίχνευσης και πρόληψης εισβολών και διαμόρφωσης και φιλτραρίσματος κυκλοφορίας για να περιορίσουν τον αντίκτυπο μιας επίθεσης. Επιπλέον, οι πλατφόρμες ηλεκτρονικής μάθησης θα πρέπει να σχεδιάζονται με γνώμονα την ασφάλεια και να ενημερώνονται τακτικά για να αντιμετωπίζουν γνωστά τρωτά σημεία. Είναι επίσης σημαντικό να υπάρχουν σχέδια αντιμετώπισης περιστατικών για γρήγορη απόκριση και μετριασμό των επιπτώσεων μιας επίθεσης. Οι οργανισμοί και τα ιδρύματα θα πρέπει επίσης να εκπαιδεύουν τους μαθητές και το προσωπικό τους σχετικά με τον τρόπο αναγνώρισης και αναφοράς πιθανών επιθέσεων DoS και να διασφαλίζουν ότι τα συστήματα και το λογισμικό ενημερώνονται τακτικά για την αποφυγή τρωτών σημείων.

Κατανεμημένη επίθεση άρνησης υπηρεσίας (Distributed Denial-of-Service (DDoS)): Μια επίθεση κατανεμημένης άρνησης υπηρεσίας (DDoS) είναι ένας τύπος επίθεσης στον κυβερνοχώρο, κατά τον οποίον πολλαπλά συστήματα, που συχνά παραβιάζονται από κακόβουλο λογισμικό, πλημμυρίζουν έναν στοχευμένο ιστότοπο ή δίκτυο με επισκεψιμότητα, σε μια προσπάθεια να το καταστήσουν μη διαθέσιμο στους χρήστες. Αυτό επιτυγχάνεται συντρίβοντας τον διακομιστή του στόχου με μεγάλο όγκο επισκεψιμότητας, καθιστώντας δύσκολη ή αδύνατη την πρόσβαση των νόμιμων χρηστών στον ιστότοπο ή την υπηρεσία. Οι επιθέσεις Distributed Denial-of-Service (DDoS) μπορούν να έχουν σημαντικό αντίκτυπο στην τηλεκπαίδευση, καθώς μπορούν να διαταράξουν τα διαδικτυακά μαθήματα και να εμποδίσουν τους μαθητές και τους δασκάλους να έχουν πρόσβαση στο διαδικτυακό υλικό μαθημάτων, τις εργασίες και τα εργαλεία επικοινωνίας. Κατά τη διάρκεια μιας επίθεσης DDoS, η στοχευμένη πλατφόρμα τηλεκπαίδευσης μπορεί να μην είναι διαθέσιμη, προκαλώντας ακύρωση ή καθυστέρηση των μαθημάτων και εμποδίζοντας τους μαθητές να υποβάλουν εργασίες ή να δώσουν εξετάσεις. Επιπλέον, οι επιθέσεις DDoS μπορεί να προκαλέσουν κατάρρευση των διακομιστών, με αποτέλεσμα την απώλεια δεδομένων και την πιθανότητα περαιτέρω

παραβιάσεων. Για την αποτροπή επιθέσεων DDoS σε πλατφόρμες ηλεκτρονικής μάθησης, οι οργανισμοί θα πρέπει να εφαρμόζουν μέτρα ασφαλείας, όπως τείχη προστασίας, συστήματα ανίχνευσης εισβολών και υπηρεσίες προστασίας DDoS που βασίζονται σε σύννεφο. Θα πρέπει επίσης να διενεργούνται τακτικές ενημερώσεις ασφαλείας και αξιολογήσεις ευπάθειας για τον εντοπισμό και την επιδιόρθωση τυχόν ευπάθειας που θα μπορούσαν να εκμεταλλευτούν οι εισβολείς.

Οι επιθέσεις DoS ή DDoS δεν είναι νέοι τύποι απειλών. Ωστόσο, η ζημιά τους είναι πολύ πιο επικίνδυνη από τα προηγούμενα χρόνια. Ο όγκος των επιθέσεων DDoS και η περιπλοκή τους έχει αυξηθεί δραματικά λόγω της φθίνουσας τιμής της εκτόξευσης αυτού του τύπου επίθεσης. Ως εκ τούτου, είναι δύσκολο να εντοπιστούν και να προστατευτούν τα συστήματα από αυτά. Σύμφωνα με την έκθεση της Kaspersky, υπήρξε σημαντικός αριθμός επιθέσεων DoS σε συστήματα ηλεκτρονικής μάθησης από το 2019 και το 2020. Μάλιστα ο αριθμός αυξήθηκε κατά 550% το 2020 σε σύγκριση με το 2019 για την ίδια περίοδο (Ιανουάριος). Αξίζει να σημειωθεί ότι το Zoom είναι η πιο δημοφιλής πλατφόρμα που δέχεται επίθεση και το Moodle είναι η δεύτερη [18].

Spoofing: Οι απειλές πλαστογράφησης εμφανίζονται, όταν ένας εισβολέας μπορεί να συμμετέχει στο σύστημα, ενώ προσποιείται ότι είναι άλλος συμμετέχων, παραβιάζοντας πιθανώς τον έλεγχο ταυτότητας του συστήματος. Για παράδειγμα, ένας εισβολέας θα μπορούσε να ισχυριστεί ότι είναι νόμιμος συμμετέχων σε μια τηλεδιάσκεψη [39]. Η πλαστογράφηση (spoofing) στα συστήματα τηλεκπαίδευσης αναφέρεται στην πράξη της πλαστοπροσωπίας ενός μαθητή ή εκπαιδευτικού με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε εκπαιδευτικό υλικό ή αξιολογήσεις. Αυτό μπορεί να γίνει δημιουργώντας ψεύτικους λογαριασμούς, χρησιμοποιώντας κλεμμένα διαπιστευτήρια σύνδεσης ή χειραγωγώντας το σύστημα με κάποιον άλλο τρόπο. Ένα παράδειγμα πλαστογράφησης στα συστήματα τηλεκπαίδευσης είναι ένας μαθητής που χρησιμοποιεί μια ψεύτικη ταυτότητα για να δώσει ένα διαδικτυακό τεστ ή εξετάσεις για λογαριασμό άλλου μαθητή. Αυτό μπορεί να γίνει όταν ο μαθητής δημιουργεί έναν ψεύτικο λογαριασμό ή χρησιμοποιεί τα στοιχεία σύνδεσης κάποιου άλλου μαθητή.

Η πρόληψη της πλαστογραφίας στην ηλεκτρονική μάθηση μπορεί να είναι δύσκολη, αλλά ορισμένες στρατηγικές που μπορούν να χρησιμοποιήσουν τα ιδρύματα περιλαμβάνουν την εφαρμογή αυστηρών διαδικασιών ελέγχου ταυτότητας, την παρακολούθηση αρχείων καταγραφής συστημάτων για ύποπτη δραστηριότητα και τη χρήση εργαλείων, όπως το λογισμικό ανίχνευσης λογοκλοπής για τον εντοπισμό πιθανής εξαπάτησης. Επιπλέον, η εφαρμογή ελέγχου ταυτότητας δύο παραγόντων και η παροχή εκπαίδευσης σε μαθητές και εκπαιδευτικούς σχετικά με τον τρόπο αναγνώρισης και αναφοράς ύποπτης δραστηριότητας μπορεί επίσης να είναι χρήσιμη.

Επίθεση επανάληψης (Replay attack): Μια επίθεση επανάληψης είναι ένας άλλος τύπος επίθεσης δικτύου κατά την οποία ένας εισβολέας παρεμποδίζει και καταγράφει μια έγκυρη μετάδοση δεδομένων και στη συνέχεια αναμεταδίδει τα καταγεγραμμένα δεδομένα σε ύστερο χρόνο για να διακόψει ή να εξαπατήσει το σύστημα [40]. Στην ηλεκτρονική μάθηση, μια επίθεση επανάληψης μπορεί να αναφέρεται στην πράξη υποκλοπής και καταγραφής μιας έγκυρης διαδικτυακής αξιολόγησης ή δοκιμής και στη συνέχεια αναμετάδοσης των καταγεγραμμένων πληροφοριών σε μεταγενέστερο χρόνο προκειμένου να εξαπατηθεί ή να αποκτηθεί μη εξουσιοδοτημένη πρόσβαση σε εκπαιδευτικό υλικό.

Για παράδειγμα, ένας εισβολέας μπορεί να υποκλέψει και να καταγράψει τη συνεδρία ενός μαθητή κατά τη διάρκεια μιας διαδικτυακής εξέτασης και στη συνέχεια να χρησιμοποιήσει αυτήν την εγγραφή για να δώσει την ίδια εξέταση αργότερα και να επιτύχει υψηλότερη βαθμολογία. Για να αποτρέψουν επιθέσεις επανάληψης στην ηλεκτρονική μάθηση, τα ιδρύματα μπορούν να χρησιμοποιήσουν διάφορες μεθόδους, όπως λογισμικό παρακολούθησης και απομακρυσμένη παρακολούθηση, με τις οποίες μπορούν να εντοπίσουν και να αποτρέψουν την εξαπάτηση παρακολουθώντας τη δραστηριότητα του μαθητή κατά τη διαδικτυακή αξιολόγηση ή εξέταση.

3.2.4 Επιθέσεις στον διακομιστή της βάσης δεδομένων του συστήματος τηλεκπαίδευσης

Έγχυση SQL (SQL Injection): Η έγχυση SQL είναι ένας τύπος επίθεσης στον κυβερνοχώρο που χρησιμοποιείται για να αποκτηθεί μη εξουσιοδοτημένη πρόσβαση σε μια βάση δεδομένων εισάγοντας κακόβουλο κώδικα σε μια δήλωση SQL. Επιτρέπει σε έναν εισβολέα να έχει πρόσβαση, να τροποποιεί ή να διαγράφει ευαίσθητες πληροφορίες που είναι αποθηκευμένες στη βάση δεδομένων. Αυτό επιτυγχάνεται με την έγχυση κακόβουλων δηλώσεων SQL σε μια είσοδο φόρμας ιστού, μια παράμετρο συμβολοσειράς ερωτήματος ή άλλα δεδομένα που παρέχονται από τον χρήστη, τα οποία στη συνέχεια εκτελούνται από τον διακομιστή βάσης δεδομένων. Για παράδειγμα, ένας εισβολέας μπορεί να εισαγάγει κακόβουλο κώδικα SQL σε μια φόρμα σύνδεσης που έχει σχεδιαστεί για να παρακάμπτει τον έλεγχο ταυτότητας και να του παρέχει πρόσβαση στο σύστημα [16].

Οι επιθέσεις με έγχυση SQL μπορεί να είναι πολύ επικίνδυνες, καθώς μπορούν να επιτρέψουν σε έναν εισβολέα να έχει πρόσβαση σε ευαίσθητες πληροφορίες, να διακόψει ή να διαγράψει δεδομένα, ακόμη και να αναλάβει τον έλεγχο ολόκληρης της βάσης δεδομένων. Στα συστήματα τηλεκπαίδευσης, οι επιθέσεις SQL injection μπορούν να χρησιμοποιηθούν για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες, όπως αρχεία μαθητών, αποτελέσματα δοκιμών και άλλο εκπαιδευτικό υλικό. Για παράδειγμα, ένας εισβολέας μπορεί να χρησιμοποιήσει την ένεση SQL για να αποκτήσει πρόσβαση σε μια βάση δεδομένων που

περιέχει πληροφορίες μαθητών, όπως ονόματα, διευθύνσεις και αριθμούς κοινωνικής ασφάλισης, και στη συνέχεια να χρησιμοποιήσει αυτές τις πληροφορίες για κλοπή ταυτότητας ή άλλες δόλιες δραστηριότητες. Ένας εισβολέας μπορεί επίσης να χρησιμοποιήσει την ένεση SQL για να τροποποιήσει ή να διαγράψει αρχεία μαθητών, αποτελέσματα δοκιμών και άλλο εκπαιδευτικό υλικό. Αυτό μπορεί να έχει σοβαρές συνέπειες για το ίδρυμα και τους μαθητές, όπως ανακριβείς αναφορές βαθμών, ακαδημαϊκή ανεντιμότητα και απώλεια της ακεραιότητας των δεδομένων.

Για την αποτροπή επιθέσεων SQL injection στα συστήματα τηλεκπαίδευσης, είναι σημαντικό τα ιδρύματα να διαθέτουν ισχυρά μέτρα ασφαλείας για την προστασία των βάσεων δεδομένων που αποθηκεύουν πληροφορίες μαθητών και εκπαιδευτικό υλικό. Αυτό περιλαμβάνει την εφαρμογή ισχυρής επικύρωσης και απολύμανσης των εισροών χρήστη, τη χρήση προετοιμασμένων δηλώσεων με παραμετροποιημένα ερωτήματα και τον περιορισμό των προνομίων του χρήστη της βάσης δεδομένων στο ελάχιστο απαραίτητο για την εκτέλεση της εργασίας του. Επιπλέον, οι τακτικοί έλεγχοι ασφαλείας και οι σαρώσεις ευπάθειας μπορούν να βοηθήσουν στον εντοπισμό και τον μετριασμό πιθανών τρωτών σημείων στην εφαρμογή και την υποδομή [32].

Έγχυση στον LDAP (LDAP Injection): Η έγχυση LDAP είναι ένας τύπος επίθεσης στον κυβερνοχώρο που χρησιμοποιείται για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε έναν διακομιστή Lightweight Directory Access Protocol (LDAP) μέσω της εισαγωγής κακόβουλου κώδικα σε ένα ερώτημα LDAP. Επιτρέπει σε έναν εισβολέα να έχει πρόσβαση, να τροποποιεί ή να διαγράφει ευαίσθητες πληροφορίες που είναι αποθηκευμένες στον κατάλογο. Στα συστήματα τηλεκπαίδευσης, οι επιθέσεις ένεσης LDAP μπορούν να χρησιμοποιηθούν για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες, όπως αρχεία μαθητών, αποτελέσματα δοκιμών και άλλο εκπαιδευτικό υλικό που είναι αποθηκευμένο στον διακομιστή καταλόγου. Ένας εισβολέας θα μπορούσε να χρησιμοποιήσει αυτές τις πληροφορίες για κλοπή ταυτότητας ή άλλες δόλιες δραστηριότητες ή για να διακόψει ή να διαγράψει δεδομένα, ακόμη και να αναλάβει τον έλεγχο ολόκληρου του καταλόγου.

Αυτό επιτυγχάνεται με την εισαγωγή κακόβουλων δηλώσεων LDAP σε μια είσοδο φόρμας ιστού, μια παράμετρο συμβολοσειράς ερωτήματος ή άλλα δεδομένα που παρέχονται από τον χρήστη, τα οποία στη συνέχεια εκτελούνται από τον διακομιστή LDAP. Για παράδειγμα, ένας εισβολέας μπορεί να εισαγάγει κακόβουλο κώδικα LDAP σε μια φόρμα αναζήτησης που έχει σχεδιαστεί για να παρακάμπτει τον έλεγχο ταυτότητας και να του παρέχει πρόσβαση σε ευαίσθητες πληροφορίες που είναι αποθηκευμένες στον κατάλογο. Οι επιθέσεις έγχυσης LDAP μπορεί να είναι πολύ επικίνδυνες, καθώς μπορούν να επιτρέψουν σε έναν εισβολέα να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες, να διακόψει ή να διαγράψει δεδομένα, ακόμη και να αναλάβει τον έλεγχο ολόκληρου του καταλόγου. Για την αποτροπή επιθέσεων

έγχυσης LDAP στα συστήματα τηλεκπαίδευσης, είναι σημαντικό τα ιδρύματα να διαθέτουν ισχυρά μέτρα ασφαλείας για την προστασία των διακομιστών LDAP που αποθηκεύουν πληροφορίες μαθητών και εκπαιδευτικό υλικό [18].

Αδύναμος έλεγχος ταυτότητας (Weak Authentication): Ο ασθενής έλεγχος ταυτότητας αναφέρεται σε ένα σύστημα που δεν παρέχει επαρκή μέτρα ασφαλείας για την επαλήθευση της ταυτότητας ενός χρήστη. Αυτό μπορεί να περιλαμβάνει τη χρήση εύκολα μαντέψιμων κωδικών πρόσβασης, τη μη εφαρμογή ισχυρών μεθόδων ελέγχου ταυτότητας, όπως ο έλεγχος ταυτότητας δύο παραγόντων, ή την αποτυχία σωστής επικύρωσης της ταυτότητας ενός χρήστη. Στα συστήματα τηλεκπαίδευσης, ο αδύναμος έλεγχος ταυτότητας μπορεί να είναι μια σημαντική αδυναμία για την ασφάλεια, καθώς μπορεί να διευκολύνει τους μη εξουσιοδοτημένους χρήστες να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες, όπως τα αρχεία μαθητών και τα αποτελέσματα των εξετάσεων, και μπορεί επίσης να διευκολύνει τους μαθητές να εξαπατήσουν στις διαδικτυακές εξετάσεις [31].

Για παράδειγμα, ένα σύστημα που απαιτεί από έναν μαθητή να εισαγάγει μόνο ένα όνομα χρήστη και έναν κωδικό πρόσβασης χωρίς να υπάρχουν πρόσθετα μέτρα ασφαλείας, όπως έλεγχος ταυτότητας δύο παραγόντων, θεωρείται ότι έχει αδύναμο έλεγχο ταυτότητας. Ομοίως, ένα σύστημα που βασίζεται αποκλειστικά σε έναν στατικό κωδικό πρόσβασης ή σε έναν που είναι εύκολα μαντέψιμο, θεωρείται ότι έχει αδύναμο έλεγχο ταυτότητας. Για να αποφευχθεί ο αδύναμος έλεγχος ταυτότητας στην ηλεκτρονική μάθηση, τα ιδρύματα θα πρέπει να εφαρμόζουν ισχυρές μεθόδους ελέγχου ταυτότητας, όπως ο έλεγχος ταυτότητας δύο παραγόντων, χρησιμοποιώντας έναν συνδυασμό από κάτι που γνωρίζει ο χρήστης (όπως έναν κωδικό πρόσβασης), κάτι που έχει ο χρήστης (όπως τηλέφωνο ή διακριτικό ασφαλείας) και κάποιο προσωπικό δεδομένο του χρήστη (όπως δακτυλικό αποτύπωμα ή αναγνώριση προσώπου) για να επιβεβαιώσει την ταυτότητα του χρήστη.

3.3 Ζητήματα απορρήτου και προσωπικών δεδομένων

Το απόρρητο είναι ένα άλλο σημείο ανησυχίας επειδή οι πολιτικές απορρήτου των συστημάτων τηλεκπαίδευσης θα μπορούσαν να επιτρέψουν στις υπηρεσίες να συλλέγουν και να αποθηκεύουν πολλά δεδομένα από διάφορους πόρους (π.χ. αρχεία, βίντεο, έγγραφα, εγγραφές στο cloud κ.α.) και αυτές οι πληροφορίες θα μπορούσαν να αφορούν ευαίσθητα προσωπικά δεδομένα [41]. Η προστασία του απορρήτου των προσωπικών δεδομένων είναι σημαντική για τα συστήματα τηλεκπαίδευσης, καθώς περιλαμβάνουν πληροφορίες σχετικά με τους μαθητές και τους καθηγητές.

Το απόρρητο και η ασφάλεια είναι διαφορετικές έννοιες και κατά συνέπεια οι πληροφορίες μπορούν να είναι ασφαλείς σε ένα σύστημα, ενώ δεν διατηρείται το απόρρητό του. Έστω για παράδειγμα, ένα σχολείο που εφαρμόζει όλα τα προβλεπόμενα μέτρα ασφαλείας αλλά δεν ενημερώνει τους μαθητές για το τι επιτρέπεται και τι δεν επιτρέπεται να κάνουν με τις πληροφορίες στις οποίες έχουν πρόσβαση. Σε αυτή την περίπτωση οι πληροφορίες έχουν ασφάλεια, αλλά όχι εγγυήσεις εμπιστευτικότητας. Η διαχείριση του απορρήτου και της ασφάλειας απαιτεί διαφορετικές προσεγγίσεις, όσον αφορά το απόρρητο: «Οι άνθρωποι λένε ότι ενδιαφέρονται για το απόρρητο αλλά συμπεριφέρονται σαν να μην το κάνουν» γνωστό και ως «Το παράδοξο της ιδιωτικότητας» [6].

Η προστασία του απορρήτου των προσωπικών δεδομένων στα πληροφοριακά συστήματα είναι ζωτικής σημασίας στην εποχή μας, λόγω της ευρείας χρήσης εφαρμογών για κινητές συσκευές, και διαδικτυακές εφαρμογές που αποθηκεύουν και επεξεργάζονται προσωπικά δεδομένα ενός ολοένα και μεγαλύτερου αριθμού χρηστών, προκειμένου να παρέχουν προσωποποιημένες υπηρεσίες. Αυτή η ανάγκη αντικατοπτρίζεται στον νέο κανονισμό της ΕΕ, τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR), ο οποίος τέθηκε σε ισχύ στις 25 Μαΐου 2018, και υποχρεώνει τις οντότητες που συλλέγουν προσωπικά δεδομένα να περιγράφουν με διαφάνεια τις μεθόδους και τους σκοπούς συλλογής και επεξεργασίας. Ο GDPR ορίζει με πολλά άρθρα επακριβώς τι πρέπει να γίνει με την διαχείριση και αποθήκευση των δεδομένων όπως και με τη λειτουργικότητα του λογισμικού. Σήμερα κάθε νέο αλλά και είδη υπάρχον σύστημα πρέπει να συμμορφώνονται με τα άρθρα και τις διατάξεις του GDPR.

Οι πλατφόρμες τηλεκπαίδευσης αποθηκεύουν και επεξεργάζονται προσωπικές πληροφορίες εγγεγραμμένων χρηστών και επίσης παρέχουν τη δυνατότητα αυτές οι πληροφορίες να χρησιμοποιηθούν για να παρέχουν μια εξατομικευμένη εμπειρία χρήστη σύμφωνα με τις ανάγκες του. Όπως συμβαίνει με όλα τα άλλα συστήματα που ενσωματώνουν περιβάλλοντα διαχείρισης χρηστών, οι πλατφόρμες τηλεκπαίδευσης πρέπει να σχεδιάζονται και να αναπτύσσονται με τρόπο που να συμμορφώνεται με τους κανονισμούς προστασίας δεδομένων και τις αναδυόμενες ανάγκες απορρήτου [42].

Η ταχέως αυξανόμενη χρήση των συστημάτων τηλεκπαίδευσης λόγω της πανδημίας COVID-19 εκτός των άλλων έχει φέρει στο προσκήνιο και αυτά τα προϋπάρχοντα προβλήματα συλλογής και επεξεργασίας προσωπικών δεδομένων αλλά και τον τρόπο που μπορούν να αντιμετωπιστούν γρήγορα και αποτελεσματικά. Ιδιαίτερη προσοχή πρέπει να δοθεί στην συλλογή και επεξεργασία δεδομένων μαθητών της πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης μιας και πρόκειται για ανήλικους [1].

Όλες οι πλατφόρμες τηλεκπαίδευσης έχουν κατά βάση κοινά τυπικά χαρακτηριστικά που επηρεάζουν το GDPR. Οι πλατφόρμες πρέπει να ενημερώνουν τους χρήστες για το σκοπό για τον οποίο συλλέγονται τα δεδομένα και για τις δυνατότητες και τα οφέλη που προκύπτουν,

όπως η δυνατότητα συμμετοχής σε ιδιωτικές βιντεοδιασκέψεις. Η μη ενημέρωση του χρήστη σχετικά με τα δεδομένα που συλλέγονται για αυτόν θέτει την πλατφόρμα σε σύγκρουση με το «Δικαίωμα στην ενημέρωση» του GDPR. Επίσης πολλές πλατφόρμες αποθηκεύουν συνεδρίες τηλεδιάσκεψης, ώστε να μπορούν να τις ξαναδούν μαθητές και καθηγητές. Οι εκπαιδευτικοί μπορούν να επιλέξουν να χρησιμοποιήσουν αυτή τη λειτουργία ώστε η πλατφόρμα να λαμβάνει αυτόματα τη συγκατάθεση, χωρίς να υπάρχει η συγκατάθεση του μαθητή. Όμως κάθε μαθητής θα πρέπει να γνωρίζει αυτή τη λειτουργία και να συμφωνεί με αυτήν, αν θέλει να τη χρησιμοποιήσει. Ωστόσο κάποιοι αμφισβητούν την αναγκαιότητα αυτού του μέτρου, επειδή αυτός που συνήθως συμμετέχει περισσότερο στις τηλεδιασκέψεις είναι ο εκπαιδευτικός. Αλλά όμως και οι μαθητές σε μικρότερο βαθμό μπορεί να εμπλέκονται σε ερωτήσεις ή απαντήσεις που δεν θέλουν να διατηρήσουν ως δεδομένα οι πλατφόρμες τηλεκπαίδευσης. Κάθε πλατφόρμα πρέπει να ζητά τη συγκατάθεση τόσο από τον καθηγητή όσο και από τον μαθητή για την εγγραφή προκειμένου να μην έρχεται σε αντίθεση με τον GDPR σχετικά με τη συγκατάθεση των χρηστών. Επίσης οι μαθητές πρέπει να έχουν δικαίωμα πρόσβασης στα αποθηκευμένα δεδομένα «Δικαίωμα πρόσβασης» που τους αφορούν.

Οι χρήστες των συστημάτων τηλεκπαίδευσης πρέπει να έχουν το δικαίωμα να διαγράψουν τον λογαριασμό τους χρησιμοποιώντας το «Δικαίωμα στη λήθη» του GDPR, όμως οι αποθηκευμένες τηλεδιασκέψεις στις οποίες συμμετείχαν συνεχίζουν να είναι διαθέσιμες. Οπότε ρίχνοντας μια πιο προσεκτική ματιά αντιλαμβανόμαστε ότι υπάρχει σύγκρουση με το «Δικαίωμα στη λήθη», όπως ακριβώς συμβαίνει και με τα κοινόχρηστα αρχεία που περιέχουν προσωπικά δεδομένα των χρηστών όπως απαντήσεις σε τεστ και εργασίες που έχει αναθέσει ο εκπαιδευτικός και συνεχίζουν να είναι διαθέσιμα στους υπόλοιπους χρήστες και μετά τη διαγραφή του λογαριασμούς ενός χρήστη. Τέλος, γνωρίζουμε ότι σε μια φυσική τάξη ό,τι συμβαίνει περιορίζεται στους μαθητές και τον εκπαιδευτικό που είναι παρόντες, ενώ σε μια εικονική τάξη μπορούν να είναι και άλλοι παρόντες στο χώρο που είναι ο μαθητής και να παρακολουθούν το μάθημα. Επίσης, υπάρχουν ζητήματα που σχετίζονται με τη χρήση καμερών, μικροφώνων και την κοινή χρήση της οθόνης των χρηστών. Αυτό αποτελεί ένα ακόμη στοιχείο του αντίκτυπου του συστήματος στο «Δικαίωμα εναντίωσης» στην επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με το GDPR [1].

3.4 BYOD (Bring Your Own Device)

Το BYOD, που εισήχθη για πρώτη φορά από την Intel το 2009, σημαίνει ότι οι φοιτητές και οι εργαζόμενοι μπορούν να φέρουν τις δικές τους προσωπικές συσκευές και να τις χρησιμοποιούν για να έχουν πρόσβαση στο ιδιωτικό δίκτυο του οργανισμού τους. Ο στόχος του BYOD είναι να αυξήσει την παραγωγικότητα και την ευελιξία για τους μαθητές και τους εργαζομένους, και

αντίστοιχα να μειώσει το κόστος για τον οργανισμό. Τα τελευταία χρόνια, η χρήση του BYOD σε οργανισμούς και εκπαιδευτικά ιδρύματα έχει γίνει κοινή πρακτική, με πολλά οφέλη. Το BYOD στα συστήματα τηλεκπαίδευσης αναφέρεται σε ένα σενάριο στο οποίο οι μαθητές ενθαρρύνονται ή απαιτείται να χρησιμοποιούν τις δικές τους προσωπικές συσκευές, όπως smartphone, φορητούς υπολογιστές και tablet, για εκπαιδευτικούς σκοπούς [43]. Αυτό μπορεί να περιλαμβάνει πρόσβαση σε διαδικτυακό υλικό μαθημάτων, συμμετοχή σε εικονικά μαθήματα, υποβολή εργασιών και εξέταση. Μερικά από τα οφέλη του BYOD είναι η δυνατότητα των μαθητών να χρησιμοποιούν προσωπικές συσκευές με τις οποίες είναι ήδη εξοικειωμένοι με τη χρήση τους, κάτι που μπορεί να βελτιώσει τη συμμετοχή και τα κίνητρά τους στη μαθησιακή διαδικασία. Προσφέρει περισσότερη ευελιξία και ευκολία στους μαθητές, οι οποίοι μπορούν να έχουν πρόσβαση στο υλικό μαθημάτων και να συμμετέχουν σε εικονικά μαθήματα από οπουδήποτε. Παράλληλα εξασφαλίζει πιθανή μείωση του κόστους για σχολεία και εκπαιδευτικά ιδρύματα, καθώς δεν χρειάζεται να παρέχουν συσκευές για μαθητές. Ωστόσο, υπάρχουν επίσης πιθανές προκλήσεις και κίνδυνοι που σχετίζονται με το BYOD στα συστήματα τηλεκπαίδευσης. Μερικά κοινά ζητήματα ασφάλειας περιλαμβάνουν [44]:

Παραβιάσεις δεδομένων: Οι προσωπικές συσκευές ενδέχεται να μην έχουν το ίδιο επίπεδο ασφάλειας και μπορεί να είναι ευάλωτες σε πειρατεία, κακόβουλο λογισμικό και άλλες κυβερνοεπιθέσεις.

Απώλεια ή κλοπή συσκευών: Οι προσωπικές συσκευές είναι πιο πιθανό να χαθούν ή να κλαπούν και εάν δεν είναι σωστά ασφαλισμένες, αυτό μπορεί να θέσει σε κίνδυνο ευαίσθητα δεδομένα των μαθητών.

Έλλειψη συμμόρφωσης συσκευής: Οι προσωπικές συσκευές ενδέχεται να μην πληρούν τα ίδια πρότυπα ασφαλείας με τις συσκευές του εκπαιδευτικού ιδρύματος, γεγονός που μπορεί να δημιουργήσει τρωτά σημεία και να θέσει ευαίσθητα δεδομένα σε κίνδυνο.

Έλλειψη ασφάλειας δικτύου: Οι προσωπικές συσκευές ενδέχεται να μην έχουν ρυθμιστεί σωστά για σύνδεση στο δίκτυο του σχολείου, γεγονός που μπορεί να δημιουργήσει τρωτά σημεία και να θέσει ευαίσθητα δεδομένα σε κίνδυνο.

Phishing και κοινωνική μηχανική: Οι προσωπικές συσκευές μπορεί να είναι ευάλωτες σε επιθέσεις ηλεκτρονικού ψαρέματος και κοινωνικής μηχανικής, οι οποίες μπορούν να εξαπατήσουν τους χρήστες να παρέχουν ευαίσθητες πληροφορίες ή να εγκαταστήσουν κακόβουλο λογισμικό.

4

Ευπάθειες & επιθέσεις που έχουν καταγραφεί

Η ασφάλεια των εφαρμογών Ιστού, όπου ανήκουν και τα συστήματα τηλεδιάσκεψης, είναι ένα δύσκολο πρόβλημα, αφού αυτού του είδους οι εφαρμογές εξ ορισμού εκτίθενται σε κακόβουλους χρήστες. Τα χαρακτηριστικά ζητήματα ασφαλείας και απορρήτου που μπορούν να θέσουν σε κίνδυνο τα συστήματα τηλεκπαίδευσης έχουν παρουσιαστεί. Σε αυτή την ενότητα θα εξεταστούν οι πιο δημοφιλείς ή πιο χρησιμοποιούμενες ευπάθειες λογισμικού σύγχρονης και ασύγχρονης τηλεκπαίδευσης. Σκοπός του κεφαλαίου αυτού είναι ο εντοπισμός και η σύγκριση των συστημάτων τηλεκπαίδευσης όσον αφορά τις επιθέσεις, τις ευπάθειες και τα κοινά τρωτά σημεία τους.

Για τον εντοπισμό των ευπαθειών των συστημάτων τηλεκπαίδευσης χρησιμοποιήθηκαν οι πιο ευρέως χρησιμοποιούμενες ταξινομίες ασφαλείας προκειμένου να ταξινομηθούν οι αδυναμίες που εντοπίστηκαν στα λογισμικά που εξετάστηκαν. Οι ταξινομίες ασφαλείας είναι το OWASP (Open Web Application Security Project) και το CWE (Common Weakness Enumeration), δύο πρότυπα βιομηχανικά πλαίσια που χρησιμοποιούνται για τον εντοπισμό και την ιεράρχηση των κινδύνων ασφάλειας λογισμικού.

Το OWASP είναι ένας μη κερδοσκοπικός οργανισμός που εστιάζει στη βελτίωση της ασφάλειας του λογισμικού. Ένα από τα πιο γνωστά έργα του είναι το OWASP Top 10, το οποίο είναι μια λίστα με τους κορυφαίους 10 πιο κρίσιμους κινδύνους για την ασφάλεια των εφαρμογών Ιστού. Το OWASP Top 10 ενημερώνεται κάθε τρία χρόνια για να αντικατοπτρίζει νέες και αναδυόμενες απειλές [14].

Το CWE, από την άλλη πλευρά, είναι ένα έργο της MITER Corporation που παρέχει μια κοινή γλώσσα για την περιγραφή των τρωτών σημείων ασφαλείας του λογισμικού. Είναι ένας τυποποιημένος τρόπος εντοπισμού και περιγραφής αδυναμιών λογισμικού, ώστε να είναι εύκολα κατανοητές και να αντιμετωπιστούν. Το CWE παρέχει μια ολοκληρωμένη λίστα αδυναμιών λογισμικού, μαζί με ορισμούς, παραδείγματα και στρατηγικές μετριασμού. Οι κορυφαίες 25 πιο επικίνδυνες αδυναμίες λογισμικού του CWE είναι μια λίστα με τις πιο

κρίσιμες ευπάθειες ασφαλείας λογισμικού, όπως προσδιορίζονται από το έργο CWE, και ενημερώνεται ετησίως [37].

Και τα δύο πλαίσια χρησιμοποιούνται ευρέως από οργανισμούς και επαγγελματίες ασφαλείας για τον εντοπισμό και την ιεράρχηση των κινδύνων ασφάλειας λογισμικού. Το OWASP Top 10 εστιάζει στην ασφάλεια εφαρμογών ιστού, ενώ το CWE έχει ευρύτερο πεδίο εφαρμογής, καλύπτοντας ένα ευρύ φάσμα ευπαθειών ασφαλείας λογισμικού. Είναι συμπληρωματικά και μπορούν να χρησιμοποιηθούν μαζί για τη βελτίωση της συνολικής ασφάλειας των συστημάτων λογισμικού.

4.1 CWE Top 25

Οι κορυφαίες 25 πιο επικίνδυνες αδυναμίες λογισμικού CWE είναι μια λίστα που αντικατοπτρίζει τις νέες και αναδυόμενες απειλές και έχει σκοπό να βοηθήσει τους οργανισμούς να εντοπίσουν και να ιεραρχήσουν τους πιο κρίσιμους κινδύνους για τα συστήματα λογισμικού τους. Η πιο πρόσφατη έκδοση του CWE Top 25, όπως φαίνεται στον πίνακα 1, περιλαμβάνει τις πιο κοινές και επικίνδυνες αδυναμίες λογισμικού συμπεριλαμβανομένης της συνολικής βαθμολογίας του καθενός. Οι αδυναμίες συχνά είναι εύκολο να βρεθούν από τους επιτιθέμενους και να τις εκμεταλλευτούν έτσι ώστε να καταλάβουν πλήρως ένα σύστημα, να κλέψουν δεδομένα ή να αποτρέψουν τη λειτουργία των εφαρμογών.

Η ομάδα του CWE χρησιμοποίησε εκθέσεις του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST), κοινά δεδομένα ευπαθειών, την Εθνική Βάση Δεδομένων Ευπαθειών (NVD) και τις βαθμολογίες του Συστήματος Βαθμολόγησης Κοινών Ευπαθειών (CVSS) που σχετίζονται με κάθε εγγραφή CVE για την κατάρτιση του καταλόγου Infrastructure Security Administration) KEV (Known Exploited Vulnerabilities List), συμπεριλαμβανομένης της εστίασης στα αρχεία CVE. Στα δεδομένα εφαρμόστηκε ένας τύπος για τη βαθμολόγηση κάθε ευπάθειας με βάση την επικράτηση και τη σοβαρότητα [45].

Η χρήση της λίστας CWE Top 25 παρέχει μια κοινή γλώσσα για την περιγραφή των τρωτών σημείων ασφαλείας του λογισμικού παρέχοντας έναν τυποποιημένο τρόπο εντοπισμού και περιγραφής αδυναμιών λογισμικού, έτσι ώστε να είναι εύκολα κατανοητές και να αντιμετωπιστούν. Βοηθά τους οργανισμούς να εντοπίζουν και να ιεραρχούν τους κινδύνους ασφαλείας λογισμικού. Αυξάνει την επίγνωση των κινδύνων ασφάλειας λογισμικού και συμβάλλει στην ευαισθητοποίηση σχετικά με τους πιο κρίσιμους κινδύνους ασφάλειας λογισμικού ενθαρρύνοντας τους οργανισμούς να αναλάβουν δράση για την αντιμετώπισή τους.

Τέλος παρέχει στρατηγικές μετριασμού για κάθε ευπάθεια, οι οποίες μπορούν να βοηθήσουν τους οργανισμούς να αναπτύξουν αποτελεσματικούς ελέγχους ασφαλείας.

Πίνακας 1 : CWE - Τα κορυφαία 25 πιο επικίνδυνα σφάλματα λογισμικού [45]

Rank	ID	Name	Score	KEV Count (CVEs)	Rank Change vs. 2021
1	CWE-787	Out-of-bounds Write	64.20	62	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.97	2	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22.11	7	+3 ▲
4	CWE-20	Improper Input Validation	20.63	20	0
5	CWE-125	Out-of-bounds Read	17.67	1	-2 ▼
6	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17.53	32	-1 ▼
7	CWE-416	Use After Free	15.50	28	0
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.08	19	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.53	1	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	9.56	6	0
11	CWE-476	NULL Pointer Dereference	7.15	0	+4 ▲
12	CWE-502	Deserialization of Untrusted Data	6.68	7	+1 ▲
13	CWE-190	Integer Overflow or Wraparound	6.53	2	-1 ▼
14	CWE-287	Improper Authentication	6.35	4	0
15	CWE-798	Use of Hard-coded Credentials	5.66	0	+1 ▲
16	CWE-862	Missing Authorization	5.53	1	+2 ▲
17	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	5.42	5	+8 ▲
18	CWE-306	Missing Authentication for Critical Function	5.15	6	-7 ▼
19	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.85	6	-2 ▼
20	CWE-276	Incorrect Default Permissions	4.84	0	-1 ▼
21	CWE-918	Server-Side Request Forgery (SSRF)	4.27	8	+3 ▲
22	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	3.57	6	+11 ▲
23	CWE-400	Uncontrolled Resource Consumption	3.56	2	+4 ▲
24	CWE-611	Improper Restriction of XML External Entity Reference	3.38	0	-1 ▼
25	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.32	4	+3 ▲

Ωστόσο, είναι σημαντικό να τονιστεί ότι το πεδίο εφαρμογής είναι περιορισμένο στις πιο κρίσιμες ευπάθειες ασφαλείας λογισμικού, χωρίς να είναι εξαντλητικό και μπορεί να υπάρχουν ακόμα άλλα τρωτά σημεία. Η κατάταξη των τρωτών σημείων μπορεί να διαφέρει ανάλογα με το συγκεκριμένο πλαίσιο ενός οργανισμού και των συστημάτων λογισμικού του. Το CWE Top 25 εστιάζει σε ευπάθειες ασφαλείας λογισμικού, αλλά δεν καλύπτει άλλους τύπους κινδύνων.

Το Common Vulnerability Scoring System (CVSS) είναι ένα πλαίσιο που αναπτύχθηκε από την MITER Corporation και παρέχει έναν τρόπο για τη συνεπή και ακριβή μέτρηση της

σοβαρότητας των τρωτών σημείων ασφαλείας. Η βαθμολογία CVSS είναι μια αριθμητική τιμή που κυμαίνεται από 0 έως 10, με το 10 να είναι η πιο σοβαρή και υπολογίζεται με βάση διάφορους παράγοντες, όπως:

Βασική βαθμολογία: Αυτή είναι η βάση της βαθμολογίας CVSS και αντικατοπτρίζει τα εγγενή χαρακτηριστικά μιας ευπάθειας, όπως η εκμεταλλευσιμότητα και ο αντίκτυπός της.

Χρονική βαθμολογία: Αυτό αντικατοπτρίζει την τρέχουσα κατάσταση της ευπάθειας, όπως τη διαθεσιμότητα ενημερώσεων κώδικα ή λύσεις.

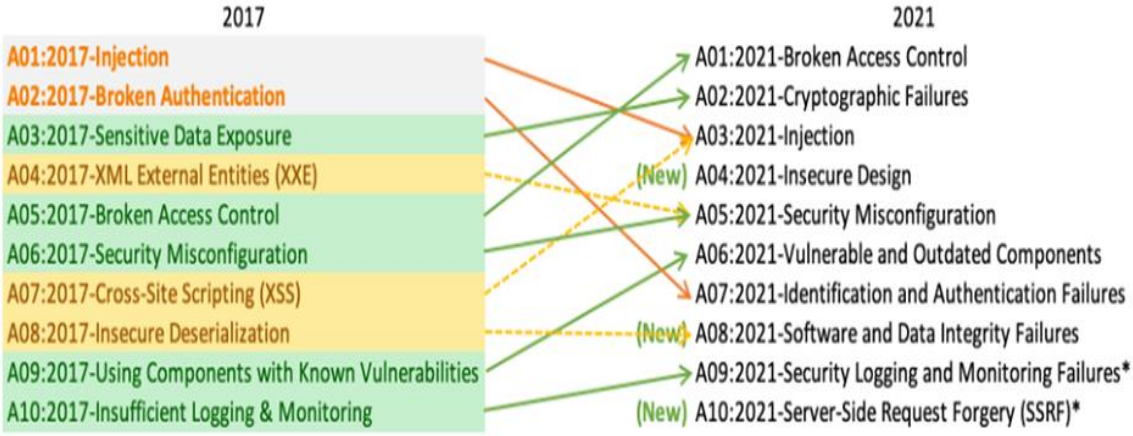
Περιβαλλοντική βαθμολογία: Αντικατοπτρίζει τον αντίκτυπο της ευπάθειας σε ένα συγκεκριμένο περιβάλλον, όπως ο αριθμός των επηρεαζόμενων συστημάτων ή η πιθανή απώλεια ευαίσθητων δεδομένων.

Σε καθέναν από αυτούς τους παράγοντες εκχωρείται μια τιμή με βάση ένα σύνολο προκαθορισμένων μετρήσεων και τύπων. Στη συνέχεια, η τελική βαθμολογία CVSS υπολογίζεται συνδυάζοντας αυτές τις τιμές. Η βαθμολογία CVSS είναι ένα χρήσιμο εργαλείο για τους επαγγελματίες ασφάλειας για να ιεραρχήσουν και να διαχειριστούν τα τρωτά σημεία με βάση τη σοβαρότητά τους. Βοηθά επίσης να κοινοποιηθεί ο κίνδυνος μιας ευπάθειας σε ενδιαφερόμενα μέρη, όπως η διοίκηση ή οι πελάτες. Εδώ περιγράφουμε θέματα μοντελοποίησης των εννοιών που χρησιμοποιεί η διπλωματική.

4.2 OWASP Top 10 – 2021

Ο OWASP ιδρύθηκε το 2001 και είναι μια ανοιχτή κοινότητα ειδικών, επαγγελματιών και ενθουσιωδών από όλο τον κόσμο που συνεργάζονται για τη βελτίωση της ασφάλειας των εφαρμογών Ιστού. Η λίστα OWASP Top 10 (πίνακας 2) βασίζεται σε έναν συνδυασμό ανάλυσης δεδομένων που παρέχονται από τους χρήστες και έρευνας από ειδικούς του κλάδου. Η ομάδα OWASP καθόρισε τις οκτώ κορυφαίες ευπάθειες της λίστας με βάση τη συμβολή της κοινότητας και τις πιο κοινές ευπάθειες στον κώδικα παραγωγής σήμερα. Οι υπόλοιπες δύο ευπάθειες προκύπτουν από την έρευνα επαγγελματιών του κλάδου που έχει στόχο να αντικατοπτρίσει τις πιο πρόσφατες και αναδυόμενες τάσεις στα τρωτά σημεία, όπου η έλλειψη δεδομένων ή η αδυναμία ελέγχου για μια ευπάθεια θα μπορούσε να την υποτιμήσει από μια διαδικασία που θα βασιζόταν αποκλειστικά σε τρωτά σημεία που ανακαλύφθηκαν κατά τη διάρκεια της δοκιμής.

Πίνακας 2 : Οι δέκα κορυφαίες ευπάθειες του OWASP 2021 [46]



Το OWASP Top 10 αναγνωρίζεται ευρέως ως χρήσιμο εργαλείο για τον εντοπισμό και την ιεράρχηση των κινδύνων ασφαλείας των εφαρμογών Ιστού. Είναι ευρέως αποδεκτό και χρησιμοποιείται ευρέως και αναγνωρίζεται ως ένας περιεκτικός και πρακτικός οδηγός για τους κινδύνους ασφαλείας των εφαρμογών Ιστού. Επίσης βοηθά τους οργανισμούς να δώσουν προτεραιότητα στις προσπάθειές τους για ασφαλή συστήματα εντοπίζοντας τους πιο κρίσιμους κινδύνους που πρέπει να αντιμετωπίσουν πρώτα. Ακόμη εστιάζει στους πιο συνηθισμένους κινδύνους ασφαλείας εφαρμογών ιστού, γεγονός που διευκολύνει τους οργανισμούς να τους κατανοήσουν και να εφαρμόσουν τα κατάλληλα μέτρα ασφαλείας. Τέλος ενημερώνεται τακτικά για να αντικατοπτρίζει τις αλλαγές στην τεχνολογία και το τοπίο απειλών, το οποίο βοηθά τους οργανισμούς να παραμένουν ενημερωμένοι σχετικά με τους πιο πρόσφατους κινδύνους που πρέπει να αντιμετωπίσουν.

Ωστόσο το περιορισμένο πεδίο εφαρμογής καλύπτει μόνο κινδύνους ασφάλειας εφαρμογών ιστού, επομένως οι οργανισμοί μπορεί να χρειαστεί να συμβουλευτούν άλλους πόρους για την αντιμετώπιση άλλων τύπων κινδύνων. Μπορεί να μην είναι ολοκληρωμένο για όλους τους οργανισμούς καθώς δεν είναι εξαντλητικό και ενδέχεται να μην καλύπτει όλους τους κινδύνους που μπορεί να αντιμετωπίσει ένας οργανισμός, ανάλογα με τις ιδιαιτερότητες του περιβάλλοντός του.

Εδώ ορίζουμε το πρόβλημα αυστηρά, δίνοντας τους κατάλληλους ορισμούς και πιθανά κάποια θεωρήματα, προτάσεις, κ.λ.π.

4.3 Ευπάθειες συστημάτων τηλεκπαίδευσης

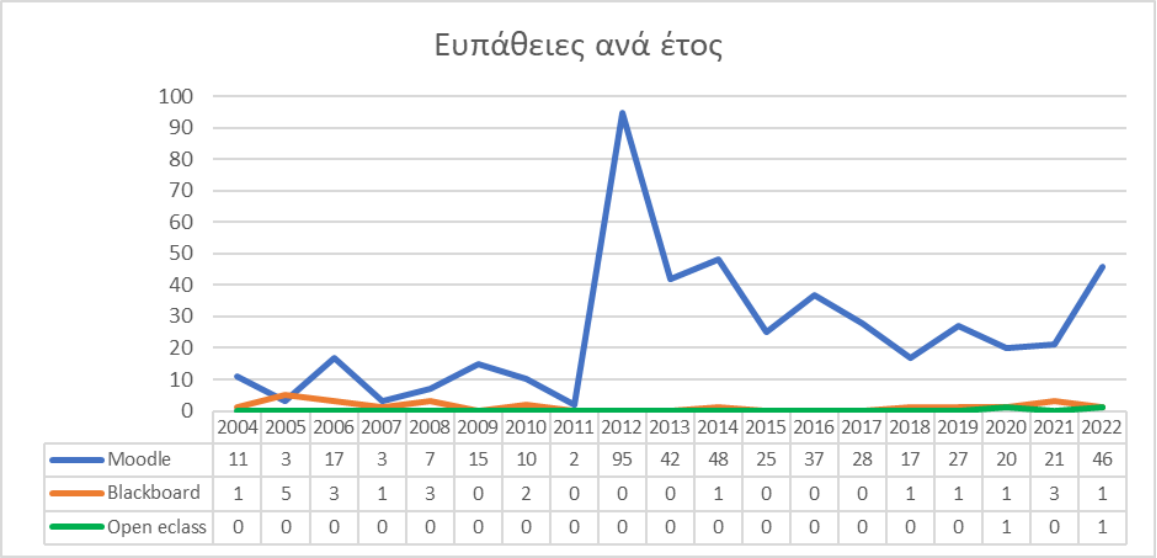
Για να προσδιορίσουμε τα τρωτά σημεία των πλατφορμών τηλεδιάσκεψης, χρησιμοποιήσαμε την πλατφόρμα CVE Details. Το cvedetails.com είναι ένας ιστότοπος που παρέχει λεπτομερείς πληροφορίες σχετικά με ευπάθειες στον κυβερνοχώρο που αποκαλύπτονται δημόσια,

συμπεριλαμβανομένων των κοινών ευπαθειών και εκθέσεων. Ο ιστότοπος παρέχει μια βάση δεδομένων ευπαθειών με δυνατότητα αναζήτησης που μπορεί να φιλτραριστεί με διάφορα κριτήρια, όπως όνομα προϊόντος, προμηθευτή και βαθμολογία CVSS. Οι χρήστες μπορούν να έχουν πρόσβαση σε πληροφορίες σχετικά με μια συγκεκριμένη ευπάθεια, συμπεριλαμβανομένης της περιγραφής της, της βαθμολογίας CVSS και τυχόν διαθέσιμες ενημερώσεις κώδικα ή λύσεις. Επίσης ο ιστότοπος παρέχει στατιστικά στοιχεία για τα πιο κοινά τρωτά σημεία και προϊόντα που επηρεάζονται, καθώς και μια ενότητα ειδήσεων που καλύπτει πρόσφατα περιστατικά ασφάλειας στον κυβερνοχώρο [14].

Τα κοινά τρωτά σημεία και εκθέσεις (CVE) είναι ένα τυποποιημένο αναγνωριστικό για μια ευπάθεια ασφαλείας. Εκχωρείται από την MITER Corporation, η οποία διαχειρίζεται τη λίστα CVE. Σε κάθε CVE εκχωρείται ένα μοναδικό αναγνωριστικό (π.χ. CVE-2021-XXXXX) και περιλαμβάνει μια περιγραφή της ευπάθειας, πληροφορίες σχετικά με το λογισμικό και τις εκδόσεις που επηρεάζονται και αναφορές σε τυχόν διαθέσιμες ενημερώσεις κώδικα ή λύσεις. Ο στόχος του συστήματος CVE είναι να παρέχει έναν συνεπή και τυποποιημένο τρόπο για τους ερευνητές και τους οργανισμούς ασφάλειας να εντοπίζουν και να παρακολουθούν τα τρωτά σημεία με σκοπό τη βελτίωση της ασφάλειας του λογισμικού και των συστημάτων [47].

4.3.1 Συστήματα Ασύγχρονης τηλεκπαίδευσης - LMS

Με βάση τα δεδομένα από το CVE Details συγκρίνουμε τα συστήματα ασύγχρονης τηλεκπαίδευσης (LMS) που παρουσιάσαμε στο κεφάλαιο 2. Το Moodle, το Blackboard και το Open Eclass είναι όλα Συστήματα Διαχείρισης Μάθησης (LMS) και όσον αφορά την ασφάλεια, και τα τρία συστήματα διαθέτουν ενσωματωμένα χαρακτηριστικά ασφαλείας, όπως έλεγχο ταυτότητας χρήστη και έλεγχο πρόσβασης. Ωστόσο, τα συγκεκριμένα χαρακτηριστικά ασφαλείας και το επίπεδο ασφάλειας που παρέχεται μπορεί να διαφέρουν μεταξύ των τριών συστημάτων. Στην εικόνα 11 παρουσιάζεται ο αριθμός ευπαθειών ανά έτος για τα τρία LMS. Παρατηρώντας την εικόνα 11 διαπιστώνουμε ότι στο Open Eclass έχουν διαπιστωθεί ελάχιστες ευπάθειες προφανώς, επειδή δεν έχει τόσο μεγάλη αποδοχή εκτός Ελλάδας όσο τα άλλα δύο LMS. Το Moodle είναι το λογισμικό με τον μεγαλύτερο αριθμό ευπαθειών διαχρονικά με μεγάλη απόσταση από τα άλλα δύο LMS. Αυτό έχει να κάνει πιθανώς με την μεγάλη διάδοση που έχει μεταξύ των συστημάτων ασύγχρονης τηλεκπαίδευσης αλλά και με το γεγονός ότι πρόκειται για λογισμικό ανοικτού κώδικα. Τέλος το Blackboard είναι ένα ευρέως χρησιμοποιούμενο σύστημα διαχείρισης εκμάθησης (LMS) με τις λιγότερες ευπάθειες σε σχέση με το ποσοστό αγοράς που κατέχει.



	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Moodle	11	3	17	3	7	15	10	2	95	42	48	25	37	28	17	27	20	21	46
Blackboard	1	5	3	1	3	0	2	0	0	0	1	0	0	0	1	1	1	3	1
Open eclass	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1

Εικόνα 11 : Ευπάθειες ανά έτος

Στον πίνακα 3 παρουσιάζεται ο αριθμός των ευπαθειών ανά κατηγορία επικινδυνότητας. Το CVSS Score δίνει μια αριθμητική τιμή που κυμαίνεται από 0 έως 10 αλλά εδώ οι ευπάθειες οργανώθηκαν σε τρεις κατηγορίες. Χαμηλού ρίσκου με βαθμολογία από 0 έως 3, μεσαίου ρίσκου με βαθμολογία από 3.1 έως 7 και υψηλού ρίσκου με βαθμολογία από 7.1 έως 10. Παρατηρώντας τον πίνακα εύκολα διαπιστώνεται ότι η πλειοψηφία των ευπαθειών κατατάσσονται στην μεσαία κατηγορία. Αυτό ισχύει και για τα τρία συστήματα τηλεκπαίδευσης ως ποσοστό των ευπαθειών.

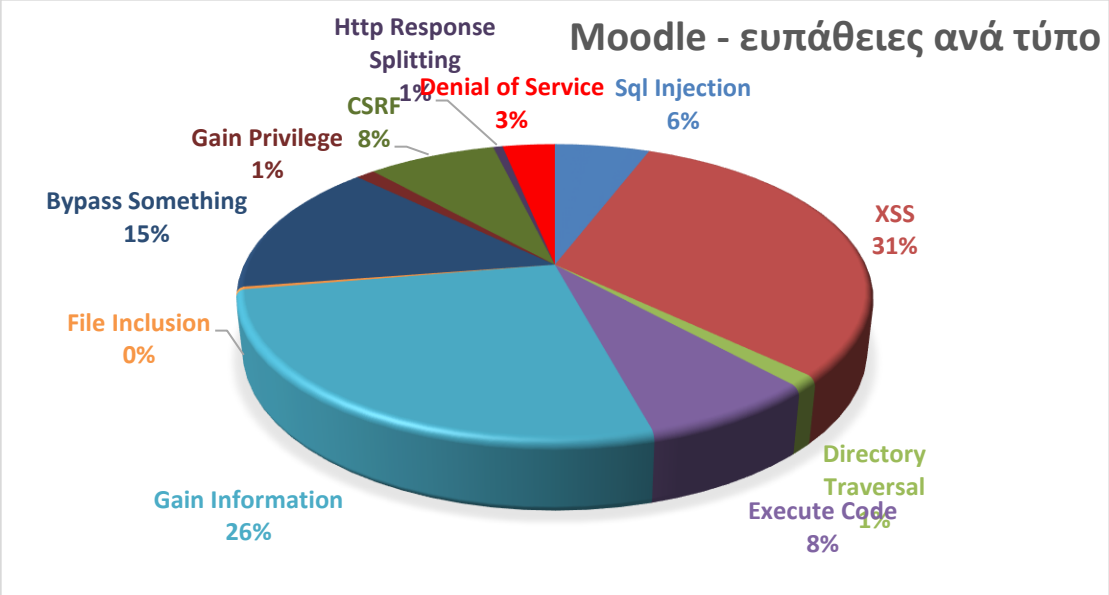
Πίνακας 3 : Σύγκριση επικινδυνότητας ευπαθειών

	CVSS Score	moodle	Blackboard	Openeclass
Επικινδυνότητα	0-3	34	2	0
	3-7	408	19	2
	7-10	32	2	0
Σύνολο		474	23	2

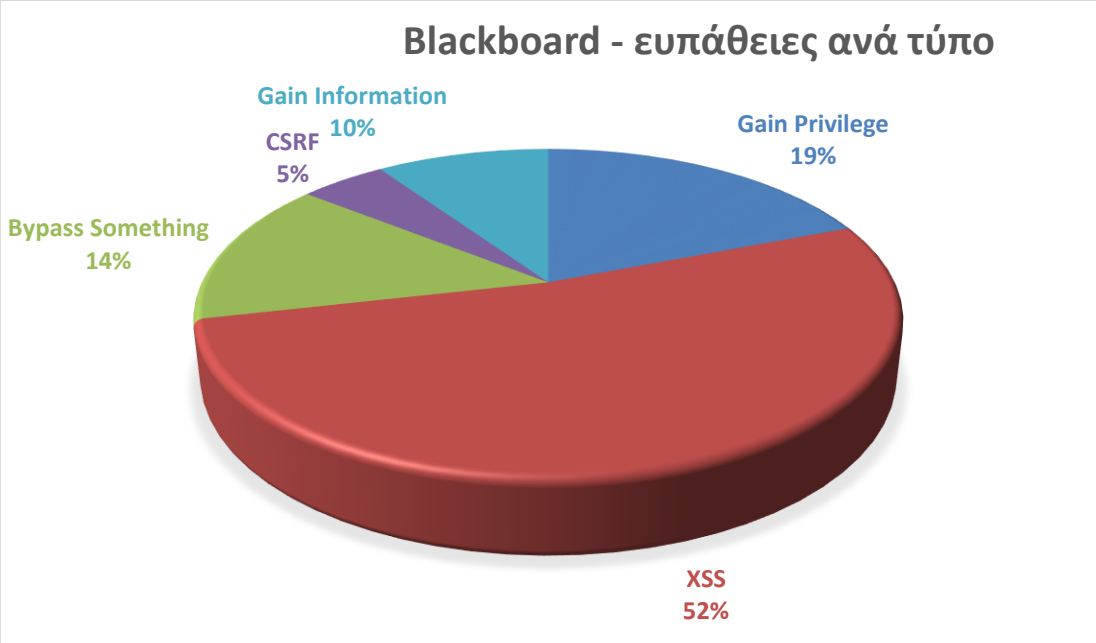
Αναλύοντας τις ευπάθειες και τα τρωτά σημεία των LMS που παρουσιάστηκαν στο κεφάλαιο 3 παρατηρούμε ότι για τα δεδομένα που δημοσιεύθηκαν στο CVE Details μεταξύ 2004 και 2022 το Moodle είναι ευάλωτο στους ακόλουθους 11 τύπους επιθέσεων, όπως φαίνεται και στην Εικόνα 12. Τη πιο σημαντική θέση στις επιθέσεις έχουν οι ευπάθειες XSS (31%), Gain Information (26%), Bypass Something (15%) και με το ίδιο ποσοστό (8%) οι Execute Code και CSRF. Έχουν παρατηρηθεί και άλλες σημαντικές ευπάθειες αλλά σε μικρότερο ποσοστό όπως είναι η SQL Ingection (6%) και Denial Of Service (3%).

Μεταξύ του 2004 και 2022, το Blackboard έχει παρουσιάσει 5 τύπους ευπάθειας, αυτές είναι οι XSS (52%), Gain Privilege (19%), Bypass Something (14%), Gain Information (10%), και τέλος η CSRF (5%) όπως μπορούμε να δούμε στην Εικόνα 13.

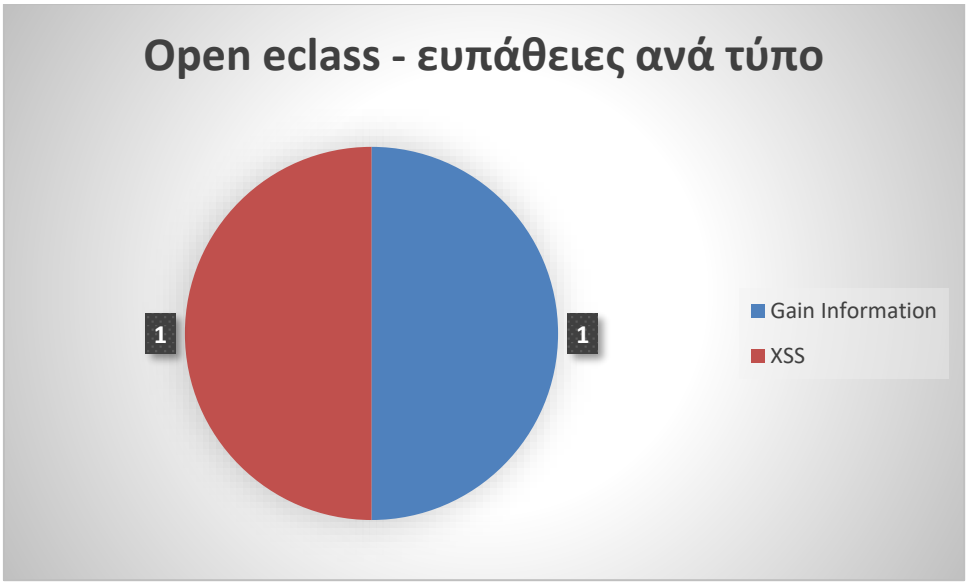
Στο open eclass έχουμε μόνο 2 καταγεγραμμένες ευπάθειες και αυτές είναι μία επίθεση Gain Information το 2020 και άλλη μία XSS το 2022 παρατηρώντας και την Εικόνα 14 που ακολουθεί.



Εικόνα 12 : Οι ευπάθειες του Moodle ανά τύπο



Εικόνα 13 : Ευπάθειες του Blackboard ανά τύπο



Εικόνα 14 : Ευπάθειες του Blackboard ανά τύπο

4.3.2 Συστήματα Σύγχρονης Τηλεκπαίδευσης

Τα συστήματα σύγχρονης τηλεκπαίδευσης εμφανίστηκαν αρκετά αργότερα από τα LMS και έχουν γίνει ιδιαίτερα δημοφιλή από την εμφάνιση του COVID-19 και μετά. Αυτός άλλωστε είναι και ο λόγος που τα στοιχεία σύγκρισης πριν το 2017 είναι ελάχιστα γι' αυτό και δεν αξιολογήθηκαν στην Εικόνα 15. Από τα συστήματα τηλεκπαίδευσης που παρουσιάστηκαν στο κεφάλαιο 2 δεν υπάρχουν καταγεγραμμένες ευπάθειες στο CVE Details για το Google meet. Για τις άλλες τρεις πλατφόρμες παρατηρείται ότι το Microsoft teams εμφάνισε την πρώτη ευπάθεια το 2019, δύο χρόνια μετά την πρώτη κυκλοφορία του και χρονιά έναρξης της πανδημίας. Παρά την αλματώδη αύξηση της χρήσης του τα περιστατικά ασφαλείας παρέμειναν σταθερά χαμηλά. Το Cisco Webex διατηρεί σε χαμηλό αριθμό τα περιστατικά επιθέσεων ασφαλείας με μόνη εξαίρεση την χρονιά του 2020 που υπήρξε η χρονιά με την μεγαλύτερη και απότομη αύξηση της χρήσης του μιας και αρκετά εκπαιδευτικά ιδρύματα πολλών χωρών (μεταξύ αυτών και η Ελλάδα) χρησιμοποίησαν την συγκεκριμένη πλατφόρμα για όλα τα δημόσια εκπαιδευτικά ιδρύματα και για διάρκεια αρετών μηνών λόγω της καραντίνας. Το 2022 όμως τα περιστατικά έπεσαν στους συνηθισμένους χαμηλούς αριθμούς. Τέλος το Zoom, η πλατφόρμα με την μεγαλύτερη απήχηση μεταξύ των χρηστών από το 2019 και μετά, παρουσιάζει κάθε χρόνο αύξηση των ευπαθειών. Μια αύξηση που συνεχίζεται και το 2023 που γράφεται αυτή η εργασία με 6 νέες ευπάθειες για τον μήνα Ιανουάριο.

Εικόνα 15 : Ευπάθειες ανά έτος

Ο πίνακας 4 περιέχει τη σύγκριση επικινδυνότητας των ευπαθειών των συστημάτων σύγχρονης τηλεκπαίδευσης. Η ανάλυση του πίνακα δείχνει ότι στο Webex έχουμε κυρίως ευπάθειες μέσου και υψηλού ρίσκου, ενώ στο Zoom οι ευπάθειες είναι μέσου και χαμηλού ρίσκου ως επι το πλείστον, χωρίς όμως να λείπουν οι ευπάθειες στην κατηγορία υψηλού ρίσκου που είναι περίπου στο μισό των άλλων κατηγοριών. Τέλος στο Teams εντοπίζονται αποκλειστικά και μόνο ευπάθειες μέσου ρίσκου.

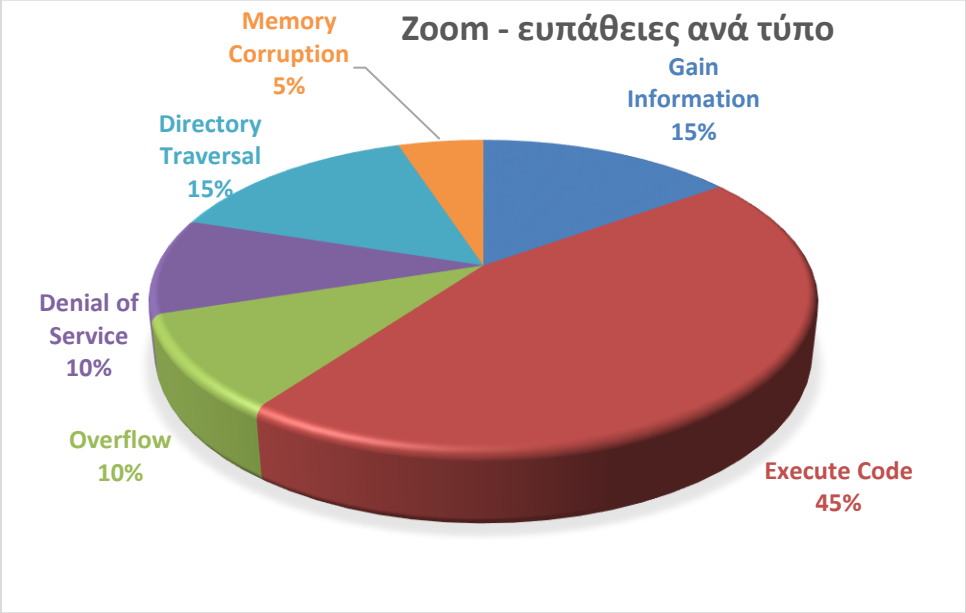
Πίνακας 4 : Σύγκριση επικινδυνότητας ευπαθειών

	CVSS Score	Webex	Zoom	Teams
Επικινδυνότητα	0-3	7	25	0
	3-7	30	27	5
	7-10	13	14	0
Σύνολο		50	66	5

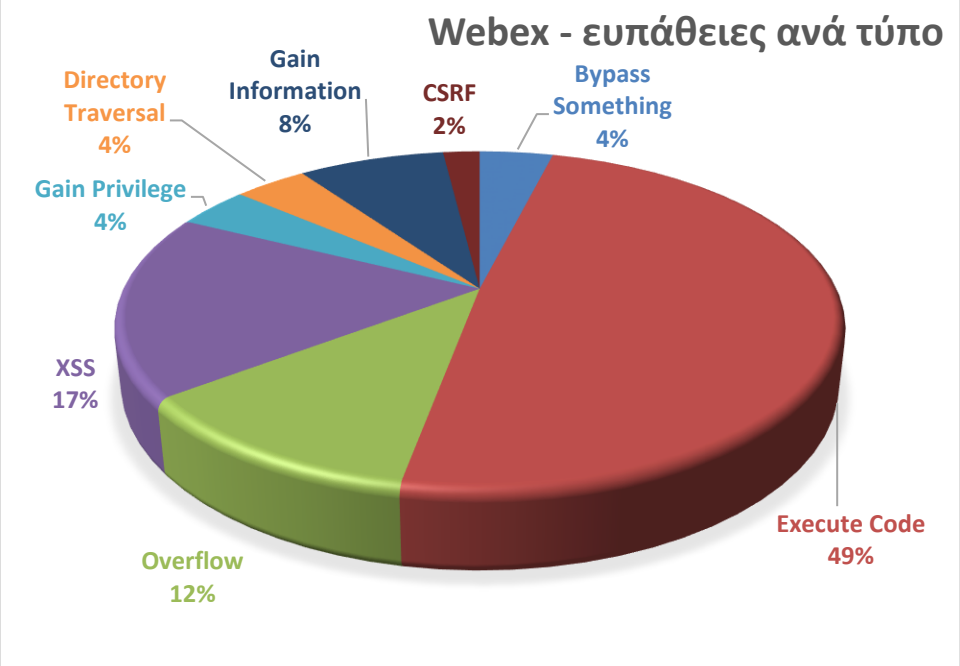
Η μελέτη ευπαθειών και τρωτών σημείων στα συστήματα σύγχρονης τηλεκπαίδευσης αποκάλυψε ότι για δεδομένα από το 2017 μέχρι σήμερα το Zoom είναι ευάλωτο σε 6 τύπους ευπάθειας που είναι Execute Code (45%), Gain Information (15%), Directory Traversal (15%), DoS και Overflow με 10% και Memory Corruption 5% (Εικόνα 16).

Για το Cisco Webex παρατηρούνται 8 τύποι ευπάθειας οι οποίοι είναι Execute Code (49%), XSS (17%), Overflow (12%), Gain Information (8%), Directory Traversal (4%), Gain Privilege (4%), ByPass Something (4%) και CSRF (2%) (Εικόνα 17).

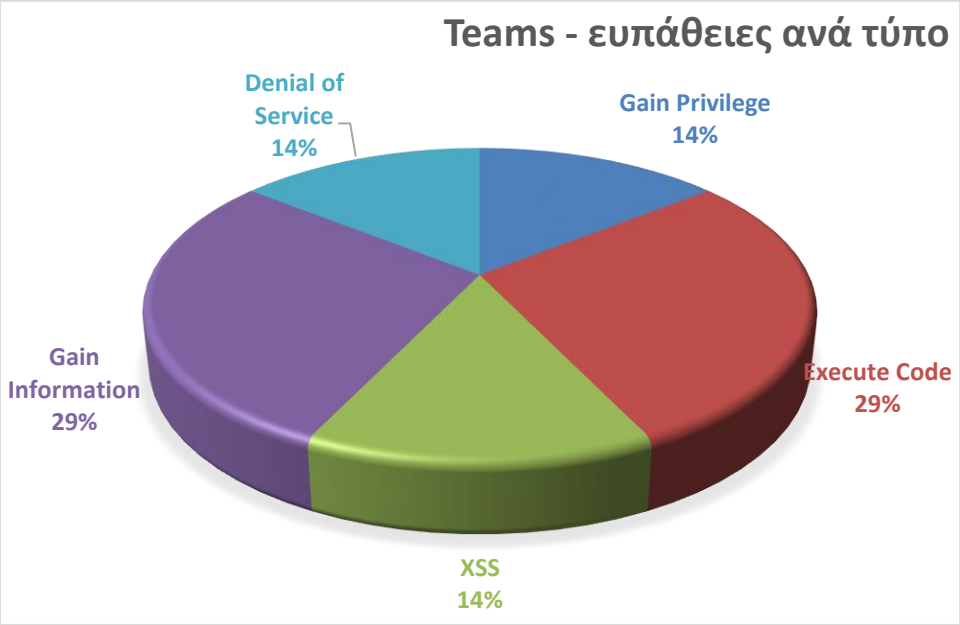
Τέλος για το Microsoft teams για δεδομένα από το 2019 και μετά εκδηλώθηκαν 5 τύποι ευπάθειας συμπεριλαμβανομένου του Execute Code (29%), Gain Information (29%), XSS (14%), Gain Privilege (14%) και Denial of Service (14%) (Εικόνα 18).



Εικόνα 16 : Zoom - ευπάθειες ανά τύπο



Εικόνα 17 : Webex - ευπάθειες ανά τύπο



Εικόνα 18 : Teams - ευπάθειες ανά τύπο

Το Google Meet, όπως και κάθε άλλο λογισμικό, ενδέχεται να έχει ευπάθειες που θα μπορούσαν να εκμεταλλευτούν οι εισβολείς. Ωστόσο, είναι πιθανό να μην έχουν αναφερθεί γνωστές ευπάθειες για το Google Meet στη βάση δεδομένων CVE. Αυτό μπορεί να οφείλεται στο ότι δεν έχουν ανακαλυφθεί ακόμη γνωστά τρωτά σημεία ή έχουν ανακαλυφθεί αλλά δεν έχουν αναφερθεί. Είναι γνωστό ότι η Google διαθέτει ένα πρόγραμμα επιβράβευσης σφαλμάτων που ανταμείβει τους ερευνητές για την εύρεση και την αναφορά τρωτών σημείων στα προϊόντα της και η εταιρεία διαθέτει μια ειδική ομάδα ασφαλείας που εργάζεται για να ανακαλύψει και να διορθώσει ευπάθειες προτού μπορέσουν να χρησιμοποιηθούν. Αυτό σημαίνει ότι τα τρωτά σημεία ανακαλύπτονται και επιδιορθώνονται προτού μπορέσουν να αναφερθούν στη βάση δεδομένων CVE.

Το Google Meet είναι μια εφαρμογή που εκτελείται εξ ολοκλήρου στο πρόγραμμα περιήγησης και, ως εκ τούτου, δεν απαιτεί συχνές ενημερώσεις κώδικα ασφαλείας. Αυτό σημαίνει ότι οι συμμετέχοντες σε συσκέψεις δεν χρειάζεται να εγκαταστήσουν κανένα λογισμικό, επέκταση ή πρόσθετο καθώς λειτουργεί με τις τελευταίες εκδόσεις των προγραμμάτων περιήγησης Chrome, Firefox, Edge ή Safari. Είναι σημαντικό να σημειωθεί ότι η απουσία τρωτών σημείων στη βάση δεδομένων CVE δεν σημαίνει απαραίτητα ότι ένα λογισμικό είναι εντελώς απαλλαγμένο από τρωτά σημεία, σημαίνει απλώς ότι δεν έχουν αναφερθεί γνωστά τρωτά σημεία.

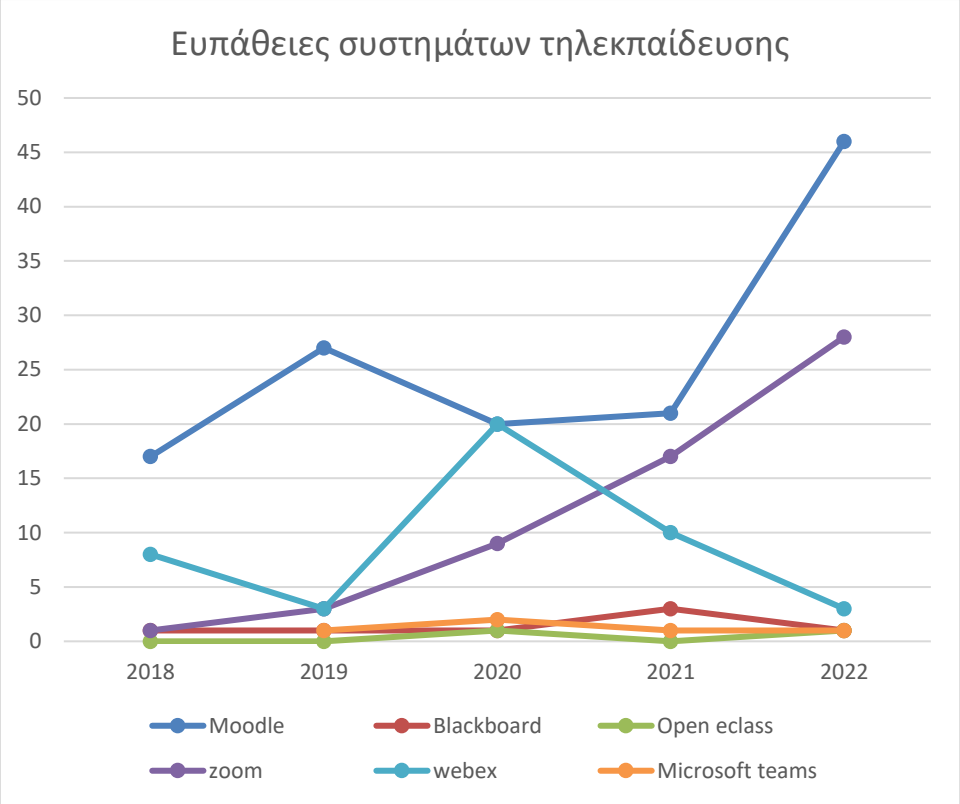
Συγκρίνοντας τα βασικά χαρακτηριστικά ασφάλειας των συστημάτων σύγχρονης τηλεκπαίδευσης παρατηρείται ότι όλα τα συστήματα εκτελούν κρυπτογράφηση δεδομένων

κατά τη μεταφορά των δεδομένων, εκτός από το Zoom. Μόνο το Zoom δεν έχει προεπιλεγμένη αυτή την δυνατότητα, αλλά αντίθετα πρέπει να ρυθμιστεί χειροκίνητα από τον χρήστη. Όλα τα συστήματα σύγχρονης τηλεκπαίδευσης κρυπτογραφούν τα δεδομένα που αποθηκεύονται στο νέφος αλλά μόνο το Webex δίνει τη δυνατότητα για κρυπτογράφηση από άκρο σε άκρο. Η κρυπτογράφηση από άκρο σε άκρο είναι αρκετά επιβαρυντική για ένα σύστημα καθώς απαιτεί επιπλέον επεξεργασία πριν τη αποστολή αλλά και μετά τη λήψη των δεδομένων, ωστόσο είναι από τα βασικότερα στοιχεία για την ολοκληρωμένη ασφάλεια ενός συστήματος [3]. Τέλος όλα τα συστήματα, εκτός από το Zoom, απαιτούν από τους χρήστες να συνδεθούν πριν τη χρήση του συστήματος τηλεκπαίδευσης. Το Zoom επιτρέπει ανώνυμες συνδέσεις σε συσκέψεις, γεγονός που μπορεί να οδηγήσει σε κάθε είδους προβλήματα εάν δεν υπάρχουν οι κατάλληλοι έλεγχοι ασφαλείας. Μια λεπτομερής σύγκριση των συστημάτων σύγχρονης τηλεκπαίδευσης παρουσιάζεται στον πίνακα 4.

Πίνακας 5 : Σύγκριση χαρακτηριστικών ασφαλείας σύγχρονων συστημάτων τηλεκπαίδευσης [3]

Security Feature	Zoom	Microsoft Teams	Cisco Webex	Google Meet
Encryption During Data Transfer	✓	✓	✓	✓
Encryption at Rest by Default	✗	✓	✓	✓
End-to-End Encryption	✗	✗	✓	✗
User Identity	✗	✓	✓	✓
Documented Security Design	✓	✓	✓	✓
Open Source	✗	✗	✗	✗

Ενώ η εξ αποστάσεως εκπαίδευση αποτελεί εδώ και καιρό μια επιλογή για πολλούς μαθητές, η πανδημία έχει αναγκάσει μια άνευ προηγουμένου στροφή προς την εξ αποστάσεως εκπαίδευση, καθώς τα σχολεία και τα πανεπιστήμια έκλεισαν τις πόρτες τους για προσωπική διδασκαλία. Η πανδημία Covid-19 είχε σημαντικό αντίκτυπο στα συστήματα τηλεκπαίδευσης παγκοσμίως. Μία από τις κύριες επιπτώσεις της πανδημίας στην ασφάλεια των συστημάτων τηλεκπαίδευσης ήταν η αύξηση των επιθέσεων στον κυβερνοχώρο. Το γεγονός αυτό είναι εμφανές και στη εικόνα 19 όπου παρατηρείτε σημαντική αύξηση των ευπαθειών τις χρονιές που ως βασικό μέτρο αντιμετώπισης του Covid-19 ήταν ο εγκλεισμός και η τηλεκπαίδευση.



Εικόνα 19 : Ευπάθειες συστημάτων τηλεκπαίδευσης

5

Καλές πρακτικές και μηχανισμοί προστασίας

Μια σύγκριση της τελευταίας κατάταξης των δέκα κορυφαίων ευπαθειών του OWASP (2021) με την προηγούμενη κατάταξη (2017) δείχνει ότι οι ευπάθειες του 2017 εξακολουθούν να είναι παρούσες. Ομοίως, η ανάλυση των MITRE CWE Top 25 που δημοσιεύθηκαν το 2019, το 2020 και το 2022 αντίστοιχα δείχνει ότι οι περισσότερες ευπάθειες εξακολουθούν να υφίστανται. Η ειδοποιός διαφορά, όμως, είναι ότι η κατάταξη της ταξινόμησης έχει αλλάξει και υπάρχουν αρκετές νέες ευπάθειες. Αυτό σημαίνει ότι δεν υπάρχουν διορθωτικά μέτρα για τη μόνιμη αντιμετώπιση αυτών των τρωτών σημείων και ότι πρέπει να εφαρμοστούν οι βέλτιστες πρακτικές πρόληψης.

Ο σχεδιασμός μετριασμού των κινδύνων είναι η διαδικασία σχεδιασμού του τρόπου πρόληψης και αντιμετώπισης των κινδύνων που ενδέχεται να προκύψουν κατά τη χρήση των συστημάτων τηλεκπαίδευσης. Στα προηγούμενα κεφάλαια παρουσιάστηκαν ευπάθειες και επιθέσεις που έχουν εντοπισθεί σε συστήματα τηλεκπαίδευσης. Ως εκ τούτου, το επόμενο βήμα είναι η προετοιμασία στρατηγικών για την αντιμετώπιση αυτών των κινδύνων.

5.1 Στρατηγικές μετριασμού κινδύνων

Κρυπτογράφηση: Η κρυπτογραφία είναι μια τεχνική που εγγυάται την εμπιστευτικότητα των δεδομένων και δεν τα αποκαλύπτει σε μη εξουσιοδοτημένα μέρη. Πρόκειται για τη διαδικασία μετατροπής δεδομένων από την αρχική τους μορφή σε μη κατανοητή μορφή. Η κρυπτογραφία διαδραματίζει σημαντικό ρόλο στο σχεδιασμό και την υλοποίηση σχεδόν όλων των ψηφιακών συστημάτων. Ειδικότερα τα κρυπτογραφικά συστήματα χρησιμοποιούν έναν αριθμό μαθηματικών αλγορίθμων που σχετίζονται με την ασφάλεια των πληροφοριών για την προστασία των δεδομένων, συμπεριλαμβανομένης της εμπιστευτικότητας, της ακεραιότητας

και της αυθεντικοποίησης. Υπάρχουν δύο τύποι συστημάτων κρυπτογράφησης: η κρυπτογράφηση συμμετρικού κλειδιού και η κρυπτογράφηση ασύμμετρου κλειδιού [40].

Οι κρυπτογραφικές αποτυχίες εμφανίζονται, όταν οι κρυπτογραφικές μέθοδοι δεν εφαρμόζονται ή εφαρμόζονται εσφαλμένα. Αυτά περιλαμβάνουν ευαίσθητα δεδομένα που μεταδίδονται ή αποθηκεύονται ως απλό κείμενο σε βάσεις δεδομένων ή αρχεία, χρήση παρωχημένων ή αδύναμων αλγορίθμων κρυπτογράφησης, κακή διαχείριση κλειδιών κρυπτογράφησης, αδύναμοι κωδικοί πρόσβασης ή εύκολα μαντεύσιμες φράσεις πρόσβασης κρυπτογράφησης κ.α.[14]. Για την πρόληψη των κρυπτογραφικών αποτυχιών αρχικά προτείνεται η επανεξέταση και ο εντοπισμός όλων των ευαίσθητων δεδομένων σύμφωνα με τους νόμους περί προστασίας της ιδιωτικής ζωής που ισχύουν για την ψηφιακή μάθηση, η χρήση των πιο πρόσφατων και ασφαλών πρωτοκόλλων και αλγορίθμων για τη διασφάλιση ότι όλα τα ευαίσθητα δεδομένα κρυπτογραφούνται σε κατάσταση ηρεμίας και κατά τη μεταφορά τους. Επίσης τα ευαίσθητα δεδομένα δεν πρέπει να αποθηκεύονται άσκοπα. Χρησιμοποιώντας κρυπτογράφηση σε ένα σύστημα τηλεκπαίδευσης προστατεύονται τα ευαίσθητα δεδομένα, όπως το όνομα, η ηλικία, η διεύθυνση και ο αριθμός τηλεφώνου ενός μαθητή.

Η κρυπτογράφηση σε συστήματα ηλεκτρονικής μάθησης χρησιμοποιείται για τους ακόλουθους λόγους:

Εμπιστευτικότητα: Για προστασία ευαίσθητων πληροφοριών, όπως προσωπικά στοιχεία και στοιχεία πληρωμής, από μη εξουσιοδοτημένη πρόσβαση.

Ακεραιότητα: Για να διασφαλιστεί ότι οι πληροφορίες που μεταδίδονται μεταξύ του χρήστη και του συστήματος ηλεκτρονικής μάθησης παραμένουν αμετάβλητες.

Έλεγχος ταυτότητας: Επιβεβαίωση της ταυτότητας του χρήστη που έχει πρόσβαση στο σύστημα και αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Συμμόρφωση: Για συμμόρφωση με νομικές και ρυθμιστικές απαιτήσεις για την προστασία δεδομένων, όπως GDPR και HIPAA.

Απόρρητο: Προστασία του απορρήτου των χρηστών αποτρέποντας μη εξουσιοδοτημένη πρόσβαση στα δεδομένα και τις δραστηριότητές τους στην πλατφόρμα τηλεκπαίδευσης.

Συνολικά, η κρυπτογράφηση είναι απαραίτητη για τη διατήρηση της ασφάλειας και του απορρήτου των χρηστών και των πληροφοριών που έχουν πρόσβαση και ανταλλάσσουν στα συστήματα τηλεκπαίδευσης.

Κατανεμημένο τείχος προστασίας: Ένα κατανεμημένο τείχος προστασίας είναι ένα σύστημα ασφάλειας δικτύου που επιβάλλει πολιτικές ασφαλείας σε πολλαπλά τμήματα και τοποθεσίες δικτύου, παρέχοντας κεντρική διαχείριση και έλεγχο. Ένα κατανεμημένο τείχος προστασίας διαφέρει από ένα παραδοσιακό τείχος προστασίας και βοηθά σημαντικά στην ασφάλεια των

συστημάτων τηλεκπαίδευσης, καθώς μπορεί να κλιμακωθεί σε πολλαπλά τμήματα και τοποθεσίες δικτύου, παρέχοντας υψηλότερο επίπεδο ασφάλειας για μεγαλύτερα δίκτυα (επεκτασιμότητα). Επίσης, ένα κατανεμημένο τείχος προστασίας παρέχει κεντρική διαχείριση και έλεγχο, καθιστώντας ευκολότερη την παρακολούθηση και την επιβολή πολιτικών ασφαλείας σε ένα μεγάλο δίκτυο [48]. Πιο συγκεκριμένα μπορεί να τμηματοποιήσει το δίκτυο σε μικρότερα, πιο ασφαλή τμήματα, βελτιώνοντας την ασφάλεια και μειώνοντας την επιφάνεια επίθεσης και να παρακολουθεί την κυκλοφορία του δικτύου σε πραγματικό χρόνο, παρέχοντας μεγαλύτερη ορατότητα στη δραστηριότητα του δικτύου. Τέλος, ένα κατανεμημένο τείχος προστασίας μπορεί να ενσωματωθεί με υπάρχοντα εργαλεία ασφαλείας, βελτιώνοντας τη συνολική ασφάλεια του δικτύου.

Βιομετρικός έλεγχος ταυτότητας: Ο έλεγχος ταυτότητας συνήθως γίνεται με παραδοσιακές τεχνικές, όπως κωδικοί πρόσβασης, έξυπνες κάρτες και ψηφιακές υπογραφές. Ο βιομετρικός έλεγχος ταυτότητας είναι μια νέα μέθοδος επαλήθευσης της ταυτότητας ενός ατόμου με βάση τα μοναδικά φυσικά ή συμπεριφορικά χαρακτηριστικά του, όπως τα δακτυλικά αποτυπώματα, η αναγνώριση προσώπου, οι σαρώσεις ίριδας, η αναγνώριση φωνής και άλλα. Αυτά τα βιομετρικά στοιχεία μπορούν να χρησιμοποιηθούν για την παροχή πρόσβασης σε ασφαλή συστήματα, συσκευές ή φυσικές τοποθεσίες. Το πλεονέκτημα του βιομετρικού ελέγχου ταυτότητας είναι ότι είναι δύσκολο να αναπαραχθεί ή να κλαπεί, σε αντίθεση με τους παραδοσιακούς κωδικούς πρόσβασης [35].

Ο βιομετρικός έλεγχος ταυτότητας μπορεί να χρησιμοποιηθεί σε εξετάσεις και εργασίες σε συστήματα τηλεκπαίδευσης ως μέθοδος επαλήθευσης της ταυτότητας του ατόμου που συμμετέχει στις εξετάσεις ή συμμετέχει σε μια ομαδική εργασία. Αυτό μπορεί να βοηθήσει στη διασφάλιση της αυθεντικότητας και της ακεραιότητας των αποτελεσμάτων της εξέτασης. Για παράδειγμα, ο βιομετρικός έλεγχος ταυτότητας μπορεί να χρησιμοποιηθεί για να επιβεβαιώσει ότι το άτομο που συμμετέχει στην εξέταση είναι το ίδιο άτομο που εγγράφηκε στο μάθημα και ότι δεν έχει λάβει βοήθεια από άλλους κατά τη διάρκεια της εξέτασης. Σε εργασίες, ο βιομετρικός έλεγχος ταυτότητας μπορεί να χρησιμοποιηθεί για να επιβεβαιώσει ότι το άτομο που εργάζεται στην εργασία είναι το ίδιο άτομο που του έχει ανατεθεί η εργασία και για να αποτρέψει άλλους από την πρόσβαση και την τροποποίηση της εργασίας τους με δόλιο τρόπο [48].

Είναι σημαντικό, όμως, να σημειωθεί ότι η χρήση βιομετρικού ελέγχου ταυτότητας σε εξετάσεις και εργασίες ενδέχεται να εγείρει ανησυχίες σχετικά με το απόρρητο και την ασφάλεια, καθώς τα βιομετρικά δεδομένα θεωρούνται ευαίσθητες πληροφορίες. Ως εκ τούτου, είναι σημαντικό για τους οργανισμούς και τις πλατφόρμες τηλεκπαίδευσης να διαθέτουν

κατάλληλα μέτρα ασφαλείας για την προστασία του απορρήτου και της ασφάλειας των βιομετρικών δεδομένων που συλλέγονται και αποθηκεύονται.

Διαχείριση Ψηφιακών Δικαιωμάτων και Ψηφιακή υδατοσήμανση: Η ψηφιακή υδατογράφηση και η διαχείριση ψηφιακών δικαιωμάτων (Digital rights management -DRM) είναι και οι δύο τεχνολογίες που χρησιμοποιούνται στα συστήματα τηλεκπαίδευσης για την προστασία του ψηφιακού περιεχομένου, όπως διαδικτυακό υλικό μαθημάτων, εκπαιδευτικά βίντεο και άλλα ψηφιακά στοιχεία. Η ψηφιακή υδατογράφηση ενσωματώνει αόρατες πληροφορίες αναγνώρισης, όπως το όνομα του ιδιοκτήτη και την ημερομηνία δημιουργίας στο περιεχόμενο που μπορεί να είναι ήχος, βίντεο, εικόνες. Αυτές οι πληροφορίες βοηθούν στην παρακολούθηση και προστασία του περιεχομένου και διασφαλίζουν ότι οι δημιουργοί και οι εκδότες αποδίδονται σωστά. Το DRM, από την άλλη πλευρά, περιορίζει τη μη εξουσιοδοτημένη διανομή και αντιγραφή του περιεχομένου μέσω της χρήσης κρυπτογράφησης, ψηφιακών πιστοποιητικών και συμφωνιών αδειοδότησης. Το DRM βοηθά να διασφαλιστεί ότι οι δημιουργοί και οι εκδότες διατηρούν τον έλεγχο της πνευματικής τους ιδιοκτησίας και ότι το περιεχόμενο χρησιμοποιείται μόνο με τρόπους που έχουν εξουσιοδοτηθεί από αυτούς [49].

Με το συνδυασμό ψηφιακής υδατογράφησης και DRM, το περιεχόμενο των συστημάτων τηλεκπαίδευσης μπορεί να προστατεύεται και να παρακολουθείται πιο αποτελεσματικά. Ειδικά για τα συστήματα τηλεκπαίδευσης το DRM είναι μια σημαντική στρατηγική που πρέπει να ενσωματωθεί για τη μείωση των κινδύνων που έχουν σχέση με τις υπηρεσίες, τους πόρους και τα περιουσιακά στοιχεία των συστημάτων τηλεκπαίδευσης [20]. Η ψηφιακή υδατογράφηση παρέχει έναν τρόπο παρακολούθησης της χρήσης του περιεχομένου, ενώ το DRM ελέγχει την πρόσβαση και τη χρήση του περιεχομένου, διασφαλίζοντας ότι προστατεύονται τα δικαιώματα των δημιουργών και των εκδοτών.

Εκπαίδευση και ευαισθητοποίηση χρηστών: Η παροχή στους χρήστες εκπαίδευσης πόρων που θα τους βοηθήσουν να κατανοήσουν πώς να χρησιμοποιούν τα συστήματα τηλεκπαίδευσης με ασφάλεια και υπευθυνότητα μπορεί να μειώσει τον κίνδυνο ανθρώπινου λάθους και τυχαίας παραβίασης δεδομένων. Η εκπαίδευση των χρηστών σχετικά με την ασφάλεια των συστημάτων τηλεκπαίδευσης περιλαμβάνει την εκπαίδευσή τους για το πώς να προστατεύουν τον εαυτό τους και τις πληροφορίες τους, ενώ συμμετέχουν σε διαδικτυακές δραστηριότητες μάθησης. Αυτό περιλαμβάνει θέματα, όπως η ασφάλεια του κωδικού πρόσβασης, η αποφυγή απατών ηλεκτρονικού ψαρέματος, η ασφαλής κοινή χρήση προσωπικών πληροφοριών και η αναγνώριση και αναφορά ύποπτης συμπεριφοράς. Η απλή συνειδητοποίηση των κινδύνων είναι συχνά το κλειδί για την πρόληψη και την προστασία [12].

Η εκπαίδευση των χρηστών για την ασφάλεια της ηλεκτρονικής μάθησης είναι σημαντική για διάφορους λόγους. Προστατεύει ευαίσθητες πληροφορίες καθώς συχνά στα συστήματα τηλεκπαίδευσης συχνά υπάρχει ανταλλαγή προσωπικών και ευαίσθητων πληροφοριών, όπως ονόματα, διευθύνσεις. Η εκπαίδευση των χρηστών σχετικά με την ασφάλεια των συστημάτων τηλεκπαίδευσης τους βοηθά να κατανοήσουν πώς να διατηρούν αυτές τις πληροφορίες ασφαλείς και να αποφεύγουν να πέφτουν θύμα εγκλήματος στον κυβερνοχώρο. Επίσης αποτρέπει περιστατικά ασφαλείας καθώς τα συστήματα τηλεκπαίδευσης μπορεί να είναι ευάλωτα σε απειλές ασφαλείας, όπως εισβολή, phishing και επιθέσεις κακόβουλου λογισμικού. Εκπαιδεύοντας τους χρήστες για το πώς να αναγνωρίζουν και να ανταποκρίνονται σε αυτές τις απειλές, οι οργανισμοί μπορούν να ελαχιστοποιήσουν τον κίνδυνο συμβάντων ασφαλείας και να προστατεύσουν τα συστήματά τους. Όταν οι χρήστες εκπαιδεύονται σχετικά με την ασφάλεια της ηλεκτρονικής μάθησης, είναι πιο σίγουροι για την ικανότητά τους να συμμετέχουν με ασφάλεια σε διαδικτυακές εκπαιδευτικές δραστηριότητες. Αυτό μπορεί να οδηγήσει σε αυξημένη δέσμευση και ικανοποίηση από την εμπειρία χρήσης των συστημάτων τηλεκπαίδευσης.

Η ευαισθητοποίηση είναι ζωτικής σημασίας για την ασφάλεια των συστημάτων τηλεκπαίδευσης, διότι βοηθά τους χρήστες να κατανοήσουν τους κινδύνους που συνδέονται με τη διαδικτυακή μάθηση και να λάβουν προληπτικά μέτρα για την πρόληψη περιστατικών ασφαλείας. Αυτό μπορεί να γίνει μέσω τακτικών υπενθυμίσεων, πόρων και εκπαιδευτικού υλικού. Επιπλέον, η παροχή στους χρήστες με σαφή κατανόηση του τι θεωρείται ασφαλής συμπεριφορά και τι όχι, θα τους βοηθήσει να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με τις διαδικτυακές τους δραστηριότητες. Φυσικά, η εκπαίδευση ασφάλειας από μόνη της δεν αρκεί, αλλά είναι ένα σημαντικό επίπεδο ασφάλειας που προστίθεται στα υπάρχοντα μέτρα ασφαλείας [33].

5.2 Πρακτικές συμβουλές στους χρήστες για ασφαλή τηλεκπαίδευση

Η ασφάλεια των συστημάτων τηλεκπαίδευσης εξαρτάται κυρίως από τον οργανισμό που προσφέρει ή παραδίδει το διαδικτυακό μάθημα και εναπόκειται στον οργανισμό να εφαρμόσει τις στρατηγικές ασφάλειας που έχουν αναφερθεί για την αντιμετώπιση των διαφόρων τρωτών σημείων που αντιμετωπίζει το σύστημα τηλεκπαίδευσης. Ωστόσο, οι ενδιαφερόμενοι θα πρέπει να συμμορφώνονται με τις αρχές ασφαλείας και τις βέλτιστες πρακτικές. Ακολουθούν οδηγίες για τον μετριασμό των κινδύνων και των επιπτώσεων από τις επιθέσεις.

Καταρχάς απαιτείται να γίνεται χρήση ισχυρών κωδικών πρόσβασης και ενεργοποίηση ελέγχου ταυτότητας δύο παραγόντων για όλους τους λογαριασμούς όπου είναι δυνατόν. Οι κωδικοί πρόσβασης πρέπει να έχουν τις ελάχιστες απαιτήσεις πολυπλοκότητας, όπως ελάχιστο μήκος, χρήση ειδικών χαρακτήρων και συνδυασμός κεφαλαίων και πεζών γραμμάτων. Επίσης οι χρήστες πρέπει να ενθαρρύνονται να αλλάζουν συχνά τους κωδικούς πρόσβασής τους. Είναι καλή πρακτική, ακόμη, να συμπεριλαμβάνουν έναν πολλαπλών παραγόντων έλεγχο ταυτότητας για τη διασφάλιση πρόσθετης ασφάλειας.

Είναι σημαντικό για τις πλατφόρμες τηλεκπαίδευσης να πραγματοποιούνται τακτικές ενημερώσεις λογισμικού, διότι συχνά περιλαμβάνουν ενημερώσεις κώδικα ασφαλείας που αντιμετωπίζουν ευπάθειες στις πλατφόρμες. Η τακτική ενημέρωση του λογισμικού βοηθά στην προστασία της εκάστοτε πλατφόρμας και των χρηστών της από πιθανές απειλές ασφαλείας. Χρειάζεται προσοχή κατά τη λήψη ενημερώσεων μόνο από επίσημους ιστοχώρους για την αποτροπή εγκατάστασης επικίνδυνου κακόβουλου λογισμικού.

Η χρήση αξιόπιστου λογισμικού προστασίας από ιούς για προστασία από κακόβουλο λογισμικό και άλλες διαδικτυακές απειλές είναι απαραίτητη. Το λογισμικό προστασίας από ιούς είναι σημαντικό για τις πλατφόρμες τηλεκπαίδευσης, επειδή συμβάλλει στην προστασία από κακόβουλο λογισμικό, ιούς και άλλες απειλές στον κυβερνοχώρο που θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια του συστήματος τηλεκπαίδευσης. Το κακόβουλο λογισμικό μπορεί να μολύνει υπολογιστές, να κλέψει ευαίσθητες πληροφορίες και να προκαλέσει διάφορα άλλα συμβάντα ασφαλείας. Χρησιμοποιώντας λογισμικό προστασίας από ιούς, μειώνεται ο κίνδυνος αυτών των τύπων επιθέσεων και αυξάνεται η προστασία των πληροφοριών και των συστημάτων που χρησιμοποιούνται.

Η κρυπτογράφηση από άκρο σε άκρο κατά τη μετάδοση ευαίσθητων πληροφοριών, όπως κωδικούς πρόσβασης ή προσωπικές πληροφορίες είναι κρίσιμης σημασίας σε ένα σύστημα τηλεκπαίδευσης, γιατί μπορεί να χρησιμοποιηθεί για την προστασία των πληροφοριών που μεταδίδονται μεταξύ των μαθητών, των δασκάλων και του προσωπικού, καθώς και των πληροφοριών που είναι αποθηκευμένες σε διακομιστές, υπολογιστές και άλλες συσκευές. Αυτό βοηθά να διασφαλιστεί ότι οι ευαίσθητες πληροφορίες παραμένουν εμπιστευτικές και προστατευμένες, ακόμη και αν υποκλαπούν από μη εξουσιοδοτημένους χρήστες κατά τη μετάδοση. Η κρυπτογράφηση είναι επίσης σημαντική, επειδή συμβάλλει στη συμμόρφωση με τους κανονισμούς περί απορρήτου, (GDPR).

Η αποφυγή της χρήσης δημόσιου Wi-Fi για πρόσβαση στα συστήματα τηλεκπαίδευσης είναι σημαντική για λόγους ασφαλείας. Τα δημόσια δίκτυα Wi-Fi είναι συχνά μη ασφαλή και ανοιχτά σε οποιονδήποτε, γεγονός που τα καθιστά πρωταρχικό στόχο για κακόβουλους παράγοντες που θέλουν να κλέψουν ευαίσθητες πληροφορίες ή να εγκαταστήσουν κακόβουλο λογισμικό σε συσκευές ανυποψίαστων χρηστών. Για την προστασία από αυτούς τους

κινδύνους, συνιστάται οι μαθητές, οι καθηγητές και το προσωπικό να αποφεύγουν τη χρήση δημόσιων δικτύων Wi-Fi για πρόσβαση σε ευαίσθητες πληροφορίες, όπως λογαριασμούς ηλεκτρονικής μάθησης και εμπιστευτικά δεδομένα.

Επιπλέον, οι χρήστες θα πρέπει επίσης να λαμβάνουν μέτρα για την ασφάλεια των συσκευών τους και να διασφαλίζουν ότι το λογισμικό τους είναι ενημερωμένο, συμπεριλαμβανομένων του λειτουργικού τους συστήματος, των προγραμμάτων περιήγησης και άλλων εφαρμογών. Αυτό βοηθά στη μείωση του κινδύνου επιθέσεων στον κυβερνοχώρο και στην προστασία ευαίσθητων πληροφοριών, ακόμη και όταν χρησιμοποιείται μια ιδιωτική, ασφαλή σύνδεση στο Διαδίκτυο.

Παράλληλα δεν πρέπει να υπάρξει ολιγωρία για την πολιτική απορρήτου, καθώς η παραμέλησή της μπορεί να έχει σοβαρές συνέπειες, όπως τη μη εξουσιοδοτημένη πρόσβαση, την κακή χρήση ή κλοπή ευαίσθητων πληροφοριών, όπως είναι τα προσωπικά ή οικονομικά δεδομένα. Είναι σημαντικό να διασφαλιστεί ότι η πολιτική απορρήτου ορίζεται με σαφήνεια, κοινοποιείται σε όλους τους χρήστες και ελέγχεται και ενημερώνεται τακτικά ώστε να συμμορφώνεται με τυχόν αλλαγές στους κανονισμούς και τις βέλτιστες πρακτικές. Επιπλέον, είναι σημαντικό να υπάρχουν ισχυρά τεχνικά μέτρα, όπως η κρυπτογράφηση και ο ασφαλής έλεγχος ταυτότητας, για την προστασία του απορρήτου των χρηστών ηλεκτρονικής μάθησης. Η Εικόνα 20 παρουσιάζει τις συμβουλές για ασφαλή τηλεκπαίδευση προς τους χρήστες των συστημάτων τηλεκπαίδευσης.

Εικόνα 20 : Συμβουλές για ασφαλή τηλεκπαίδευση [50]

6

Επίλογος

Αυτό το κεφάλαιο συνοψίζει όσα έχουν μελετηθεί στο πλαίσιο αυτής της διπλωματικής διατριβής και παραθέτει τα συμπεράσματα που προέκυψαν στο τέλος της μελέτης. Επιπλέον, προτείνει μερικές ιδέες για μελλοντική έρευνα και επέκταση της διπλωματικής εργασίας.

6.1 Σύνοψη και συμπεράσματα

Η τηλεκπαίδευση δεν είναι απλώς μια βραχυπρόθεσμη απάντηση σε μια παγκόσμια πανδημία αλλά είναι εδώ για να μείνει. Εξάλλου οι περισσότεροι συμφωνούν ότι η τηλεκπαίδευση δε θα σταματήσει να υφίσταται ακόμη και όταν η πανδημία τελειώσει. Η ακαδημαϊκή εκδοτική εταιρεία Pearson Education σε μια πρόσφατη έρευνα της, διαπίστωσε ότι σχεδόν το 90% των 7.000 ατόμων που ερωτήθηκαν αναμένουν ότι η τηλεκπαίδευση θα συνεχίσει να διαδραματίζει στο μέλλον σημαντικό ρόλο σε όλα τα επίπεδα εκπαίδευσης [8].

Η συνεχώς αυξανόμενη δημοτικότητα των ψηφιακών υπηρεσιών στην εκπαίδευση συμβάλλει, επίσης, στην αυξανόμενη ζήτηση για κυβερνοασφάλεια. Οι μαθητές, οι δάσκαλοι και οι γονείς, αφού εργάστηκαν αναγκαστικά με την τηλεκπαίδευση, απόκτησαν την ευκαιρία να συνειδητοποιήσουν εκ των πραγμάτων τη σημασία της ασφάλειας και την αναγκαιότητά της για τη διατήρηση μιας κανονικής μαθησιακής διαδικασίας. Ωστόσο, καθώς η τηλεκαπαίδευση γίνεται πιο δημοφιλής, οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν αυτό το δεδομένο προς όφελός τους. Αυτό σημαίνει ότι τα εκπαιδευτικά ιδρύματα θα συνεχίσουν να αντιμετωπίζουν όλο και περισσότερους κινδύνους στον κυβερνοχώρο. Κατά συνέπεια οι πτυχές της ασφάλειας και του απορρήτου των συστημάτων τηλεκπαίδευσης προκαλούν μεγάλη ανησυχία. Αυτή η εργασία, λοιπόν, επιχείρησε να παρουσιάσει μια συγκριτική αξιολόγηση των συστημάτων τηλεκπαίδευσης σε σχέση με τις επιθέσεις στις οποίες εκτέθηκαν, να αναδείξει τα τρωτά τους σημεία και να προτείνει τεχνικές μετριασμού των κινδύνων.

Αρχικά έγινε μια ανάλυση των χαρακτηριστικών των συστημάτων τηλεκπαίδευσης διαχωρίζοντάς τα σε ασύγχρονα συστήματα, κατά τα οποία οι μαθητές και ο εκπαιδευτικός δεν είναι υποχρεωτικό να βρίσκονται συγκεντρωμένοι μαζί την ίδια χρονική στιγμή στον ίδιο χώρο, και σε σύγχρονα συστήματα, στα οποία οι μαθητές με τους εκπαιδευτικούς δεν βρίσκονται στον ίδιο τόπο και χώρο αλλά διατηρούν οπτικοακουστική επικοινωνία. Στη συνέχεια παρουσιάστηκαν τα συστήματα τηλεκπαίδευσης για τα οποία ακολούθησε συγκριτική αξιολόγηση. Επίσης, έγινε μια σύντομη αναφορά στο Cloud Compouting και στα πλεονεκτήματα που προσφέρει στα συστήματα τηλεκπαίδευσης.

Ακολούθησε ανάλυση των χαρακτηριστικών ζητημάτων ασφαλείας που αφορούν τα συστήματα τηλεδιάσκεψης και ειδικότερα η εμπιστευτικότητα, η διαθεσιμότητα, η ακεραιότητα, η αυθεντικοποίηση και η μη άρνηση. Ακολούθως αναλύθηκαν οι τύποι επιθέσεων και τα ζητήματα απορρήτου και προσωπικών δεδομένων. Παράλληλα έγινε αναφορά στα πλεονεκτήματα αλλά και στους κινδύνους κατά τη χρήση των προσωπικών συσκευών (BYOD) των χρηστών συστημάτων τηλεκπαίδευσης. Για τον εντοπισμό των ευπαθειών χρησιμοποιήθηκαν το Common Weakness Enumeration του MITRE με τις 25 πιο επικίνδυνες αδυναμίες λογισμικού και το OWASP top 10 μια κορυφαία ταξινόμηση ευπαθειών λογισμικού για εφαρμογές του ιστού. Όσον αφορά τον προσδιορισμό των τρωτών σημείων των πλατφορμών τηλεδιάσκεψης, χρησιμοποιήθηκε η πλατφόρμα CVE Details.

Η συγκριτική αξιολόγηση των τριών πιο χρησιμοποιούμενων και δημοφιλών LMS στην Ελλάδα (Blackboard, Moodle και Open eclass), αποκάλυψε ότι το Blackboard είναι το πιο ασφαλές LMS, καθώς είναι ευάλωτο σε λίγους τύπους επιθέσεων, και το Moodle ήταν το πιο ευάλωτο και εκτεθειμένο σε επιθέσεις, ενώ για το Open eclass δεν υπάρχουν αρκετά στοιχεία, όσο διεξάγεται η παρούσα εργασία, για να εξαχθούν ασφαλή συμπεράσματα. Ομοίως, η εις βάθος μελέτη ευπαθειών των πιο δημοφιλών συστημάτων σύγχρονης τηλεκπαίδευσης (Cisco WebEx, Microsoft Teams και Zoom) αποκάλυψε ότι το Microsoft Teams είναι το πιο ασφαλές εργαλείο. Το Cisco Webex παρουσίασε μια κορύφωση των ευπαθειών κατά την περίοδο της καραντίνας για τον Covid-19. Το Zoom έχει τα περισσότερα περιστατικά ευπαθειών και προφανώς ως η δημοφιλέστερη πλατφόρμα τηλεκπαίδευσης αποτελεί βασικό στόχο επιθέσεων. Ωστόσο, όλες οι πλατφόρμες είναι πιο ευάλωτες σε επιθέσεις απομακρυσμένης εκτέλεσης κώδικα (Execute Code). Για το Google Meet τη δεύτερη δημοφιλέστερη πλατφόρμα τηλεκπαίδευσης δεν έχουν αναφερθεί ακόμη γνωστές ευπάθειες στη βάση δεδομένων CVE.

Επίσης, μέσω της εργασίας, έχουν παρουσιαστεί οι καλές πρακτικές και οι μηχανισμοί προστασίας από τρωτά σημεία που επισημαίνονται κατά την αξιολόγηση. Τα μέτρα μετριασμού είναι παρόμοια με εκείνα των περιόδων προ COVID-19, με τη διαφορά ότι η εστίαση είναι στην ευαισθητοποίηση και εκπαίδευση των χρηστών. Ένα βασικό βήμα για τα

εκπαιδευτικά ιδρύματα είναι η ενίσχυση της κατάρτισης και της υποστήριξης του προσωπικού, των εκπαιδευτικών και των φοιτητών σε θέματα ασφαλείας αλλά και προσωπικών δεδομένων.

Τέλος μέσα από την αξιολόγηση συμπεραίνεται ότι οι κίνδυνοι για την ασφάλεια και το απόρρητο δεν είναι υψηλότεροι από αυτούς που απαντώνται συνήθως στο Διαδίκτυο και ότι δεν υπάρχουν σημαντικές διαφορές μεταξύ των βασικών συστημάτων τηλεκπαίδευσης. Οι κορυφαίες πλατφόρμες έχουν αρχίσει να εστιάζουν σε δύο βασικούς άξονες, την ευκολία και την ασφάλεια. Ο ανταγωνισμός για το ποια πλατφόρμα θα επικρατήσει είναι περισσότερο θέμα ασφάλειας, καινοτομίας σε νέες υπηρεσίες, τιμής και διαλειτουργικότητας με άλλα προγράμματα [51].

6.2 Μελλοντικές επεκτάσεις

Η ασφάλεια είναι μια ατέρμονη διαδικασία που απαιτεί συνεχείς προσπάθειες για να συμβαδίσει με τις ταχέως εξελισσόμενες τεχνολογίες. Μια τεχνολογία που θα είχε ενδιαφέρον να μελετηθεί είναι η χρήση της μηχανικής μάθησης για την ενίσχυση της ασφάλειας των συστημάτων τηλεκπαίδευσης. Η μηχανική μάθηση έχει τη δυνατότητα να παίξει σημαντικό ρόλο στην ενίσχυση της ασφάλειας των συστημάτων τηλεκπαίδευσης στο μέλλον. Μερικές από τις πιθανές μελλοντικές επεκτάσεις της μηχανικής μάθησης σε αυτόν τον τομέα περιλαμβάνουν την ανίχνευση απάτης, καθώς οι αλγόριθμοι μηχανικής μάθησης μπορούν να χρησιμοποιηθούν για τον εντοπισμό και την πρόληψη της απάτης σε συστήματα τηλεκπαίδευσης, όπως η λογοκλοπή [10]. Αυτοί οι αλγόριθμοι μπορούν να αναλύσουν μοτίβα στη συμπεριφορά και τις υποβολές των μαθητών για να εντοπίσουν πιθανές περιπτώσεις απάτης και να λάβουν τις κατάλληλες ενέργειες για την αποτροπή της. Επίσης, οι αλγόριθμοι μηχανικής μάθησης μπορούν να χρησιμοποιηθούν για το φιλτράρισμα ακατάλληλου περιεχομένου σε συστήματα τηλεκπαίδευσης, όπως η ρητορική μίσους και ο διαδικτυακός εκφοβισμός. Επίσης οι αλγόριθμοι μηχανικής μάθησης μπορούν να χρησιμοποιηθούν για τον έλεγχο ταυτότητας των χρηστών σε συστήματα εξ αποστάσεως εκπαίδευσης και την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητα δεδομένα. Αυτό μπορεί να γίνει με τη χρήση βιομετρικών τεχνικών ελέγχου ταυτότητας, όπως η αναγνώριση προσώπου και η σάρωση δακτυλικών αποτυπωμάτων, για την επαλήθευση της ταυτότητας των χρηστών

Μια άλλη κατεύθυνση προς διερεύνηση για επέκταση της διπλωματικής είναι η τεχνολογία Blockchain και οι δυνατότητες που διαθέτει να ενισχύσει την ασφάλεια των συστημάτων τηλεκπαίδευσης. Το Blockchain θα μπορούσε να χρησιμοποιηθεί για την αποθήκευση και τη διαχείριση της επαλήθευσης των πιστοποιητικών και των διαπιστευτηρίων σε ένα σύστημα τηλεκπαίδευσης. Αυτό θα καταστήσει δυνατή την εύκολη επαλήθευση της γνησιότητας αυτών των πιστοποιητικών, διασφαλίζοντας ότι δεν μπορούν να αλλοιωθούν ή να παραποιηθούν.

Επίσης η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για την αποθήκευση και τη διαχείριση δεδομένων μαθητών, συμπεριλαμβανομένων των βαθμολογιών και των εγγραφών ολοκλήρωσης μαθημάτων, με ασφαλή και ασφαλή τρόπο. Αυτό διασφαλίζει ότι τα δεδομένα δεν μπορούν να αλλοιωθούν ή να διαγραφούν και να διατηρούνται με ασφαλή και αποκεντρωμένο τρόπο. Ωστόσο, είναι σημαντικό να σημειωθεί ότι, ενώ το blockchain έχει πολλές δυνατότητες, εξακολουθεί να είναι μια σχετικά νέα τεχνολογία και χρειάζεται περισσότερη έρευνα για την πλήρη αξιοποίηση των δυνατοτήτων του σε αυτόν τον τομέα [49].

7

Βιβλιογραφία

[1] E. Mougiakou, S. Papadimitriou, and M. Virvou, "Synchronous and Asynchronous Learning Methods under the light of General Data Protection Regulation," in 2020 11th International Conference on Information, Intelligence, Systems and Applications (IISA, 15-17 July 2020 2020, pp. 1-7, doi: 10.1109/IISA50023.2020.9284341.

[2] A. AlMufairej, L. BinGhaith, D. AlShareef, and N. S. M. Jamail, "Cyber Security Risk Management: E-Learning System," in 2022 Fifth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU), 28-29 March 2022 2022, pp. 146-149, doi: 10.1109/WiDS-PSU54548.2022.00041.

[3] N. Nazar, I. Darvishi, and A. Yeboah-Ofori, "Cyber Threat Analysis on Online Learning and Its Mitigation Techniques Amid Covid-19," in 2022 IEEE International Smart Cities Conference (ISC2), 26-29 Sept. 2022 2022, pp. 1-7, doi: 10.1109/ISC255366.2022.9922102.

[4] Y. Chen and W. He, "Security Risks and Protection in Online Learning: A Survey," International Review of Research in Open and Distance Learning, vol. 14, pp. 108-127, 12/01 2013, doi: 10.19173/irrodl.v14i5.1632.

[5] H. F. Aldheleai, M. U. Bokhari, and H. S. A. Hamatta, "User Security in e-Learning System," in 2015 Fifth International Conference on Communication Systems and Network Technologies, 4-6 April 2015 2015, pp. 767-770, doi: 10.1109/CSNT.2015.113.

[6] M. d. C. Freitas and M. M. d. Silva, "GDPR and Distance Teaching and Learning," in 2021 16th Iberian Conference on Information Systems and Technologies (CISTI), 23-26 June 2021 2021, pp. 1-6, doi: 10.23919/CISTI52073.2021.9476409.

[7] E. Djeki, J. Degila, C. Bondiombouy, and M. H. Alhassan, "Preventive Measures for Digital Learning Spaces' Security Issues," in 2022 IEEE Technology and Engineering

Management Conference (TEMSCON EUROPE), 25-29 April 2022 2022, pp. 48-55, doi: 10.1109/TEMSCONEUROPE54743.2022.9801945.

[8] Kaspersky, “Digital Education: The cyberrisks of the online classroom”, 2020 [Online], Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/09/03172621/education_report_04092020.pdf [Accessed: 31 October 2022].

[9] A. Adams and A. Blandford, "Security and Online learning: to protect or prohibit," in Usability Evaluation of Online Learning Program, C. Ghaoui Ed. UK: IDEA Publishing, 2003, pp. 331-359.

[10] K. V, V. M. Deshmukh, and S. Rath, "Secured Online Learning in COVID-19 Pandemic using Deep Learning Methods," in 2021 IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC), 3-4 Dec. 2021 2021, pp. 1-5, doi: 10.1109/ICMNWC52512.2021.9688338.

[11] Ελληνικό Μεσογειακό Πανεπιστήμιο. "Τι είναι η τηλεκπαίδευση.", [Online], Available: https://www.nmc.hmu.gr/el/node/65 [Accessed: 12 Δεκεμβρίου 2022].

[12] D. Fayzieva, S. Tashmatova, and D. Karimova, "Problems of Information Security in the System of Distance Education," in 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 9-11 May 2022 2022, pp. 1306-1310, doi: 10.1109/ICAAIC53929.2022.9793303.

[13] A. M. Gabor, M. Popescu, and N. Antoanela, "Security Issues Related To E-Learning Education," p. 60, 01/01 2017.

[14] E. Djeki, J. Degila, C. Bondiombouy and M. H. Alhassan, "Security Issues in Digital Learning Spaces," in 2021 IEEE International Conference on Computing (ICOCO), 17-19 Nov. 2021 2021, pp. 71-77, doi: 10.1109/ICOCO53166.2021.9673575.

[15] A. Scerbakov, N. Scerbakov, and F. Kappe, Security Vulnerabilities in Modern Lms. 2019, doi: 10.33965/el2019_201909C038.

[16] G. E. Violettas, T. L. Theodorou, and G. C. Stephanides, "E-Learning Software Security: Tested for Security Vulnerabilities & Issues," in 2013 Fourth International Conference on e-Learning "Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity", 7-9 May 2013 2013, pp. 233-240, doi: 10.1109/ECONF.2013.66.

[17] E-learning Asia, "The first Moodle certified Premium Partner in South East Asia", [Online], available: https://www.e-learning.asia/news-topics/nt202210051/ [Accessed: 31 December 2022].

[18] L. Salvador, C. Alvarez, and P. D. Nguyen, "Digital Education: Security Challenges and Best Practices," Security science journal, vol. 2, pp. 65-76, 12/13 2021, doi: 10.37458/ssj.2.2.4.

[19] University of Otago, "About blackboard", [Online], available: https://help.otago.ac.nz/blackboard/ [Accessed: 20 December 2022].

[20] Ελληνικό Ακαδημαϊκό Διαδίκτυο, "Open eClass " GUnet., [Online], available: https://www.openeclass.org [Accessed: 18 December 2022].

[21] A.-P. Correia, C. Liu, and F. Xu, "Evaluating videoconferencing systems for the quality of the educational experience," Distance Education, vol. 41, no. 4, pp. 429-452, 2020/10/01 2020, doi: 10.1080/01587919.2020.1821607.

[22] Z. Kristóf, "International Trends of Remote Teaching Ordered in Light of the Coronavirus (COVID-19) and its Most Popular Video Conferencing Applications that Implement Communication," Central European Journal of Educational Research, vol. 2, pp. 84-92, 07/13 2020, doi: 10.37441/CEJER/2020/2/2/7917.

[23] M. Dias, R. de Oliveira Albergarias Lopes, and A. Teles, "Will Virtual Replace Classroom Teaching? Lessons from Virtual Classes via Zoom in the Times of COVID-19," Journal of Advances in Education and Philosophy, vol. 4, pp. 208-213, 05/18 2020, doi: 10.36348/jaep.2020.v04i05.004.

[24] S. Dash, S. Samadder, A. Srivastava, R. Meena, and P. Ranjan, "Review of Online Teaching Platforms in the Current Period of COVID-19 Pandemic," (in eng), Indian J Surg, vol. 84, no. Suppl 1, pp. 1-6, Jun 18 2021, doi: 10.1007/s12262-021-02962-4.

[25] S. Ismail and S. Ismail, "Teaching Approach using Microsoft Teams: Case Study on Satisfaction versus Barriers in Online Learning Environment," Journal of Physics: Conference Series, vol. 1874, p. 012020, 05/01 2021, doi: 10.1088/1742-6596/1874/1/012020.

[26] R. Singh and S. Awasthi, Updated Comparative Analysis on Video Conferencing Platforms- Zoom, Google Meet, Microsoft Teams, WebEx Teams and GoToMeetings. 2020.

[27] H. Dhika, F. Destiawati, S. Surajiyo, and M. Jaya, Distance Learning During the Pandemic Period of COVID-19 with Zoom and Webex Comparison. 2021.

[28] Z. Khalid, F. Iqbal, F. Kamoun, M. Hussain, and L. A. Khan, "Forensic Analysis of the Cisco WebEx Application," in 2021 5th Cyber Security in Networking Conference (CSNet), 12-14 Oct. 2021 2021, pp. 90-97, doi: 10.1109/CSNet52717.2021.9614647.

[29] A. El Mhouti, M. Erradi, and A. Nasseh, "Using cloud computing services in e-learning process: Benefits and challenges," Education and Information Technologies, vol. 23, pp. 1-17, 03/01 2018, doi: 10.1007/s10639-017-9642-x.

[30] R. Bansal, A. Gupta, R. Singh, and V. K. Nassa, "Role and Impact of Digital Technologies in E-Learning amidst COVID-19 Pandemic," in 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), 3-3 July 2021 2021, pp. 194-202, doi: 10.1109/CCICT53244.2021.00046.

[31] R. Priya and J. Jayanthi, "Security Attacks and Threats in E-Learning", Int. J. Emerg. Technol. Comput. Sci. Electron., vol. 21, no. 3, pp. 629-633, 2016.

[32] D. Luminita, "Information security in E-learning Platforms," Procedia - Social and Behavioral Sciences, vol. 15, pp. 2689-2693, 12/31 2011, doi: 10.1016/j.sbspro.2011.04.171.

[33] S. Mohd Wahid, "Cyber Security Behaviorin Online Distance Learning: Utilizing National E-Learning Policy," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, pp. 1719-1728, 04/10 2021, doi: 10.17762/turcomat.v12i5.2167.

[34] S. Farid, M. Alam, J. Itmazi, G. Qaisar, and A. Haq, "Security Threats and Measures in E-learning in Pakistan: A Review," vol. 22, pp. 98-107, 01/01 2017.

[35] S. Kausar, X. Huahu, A. Ullah, Z. Wenhao, and M. Y. Shabir, "Fog-Assisted Secure Data Exchange for Examination and Testing in E-learning System," Mobile Networks and Applications, 2020/01/18 2020, doi: 10.1007/s11036-019-01429-x.

[36] V. Negrescu and M. Caradaica, "M-Learning and Security Issues in the Coronavirus Era," Analele Universitatii Ovidius Constanta, vol. 9, pp. 7-25, 03/16 2021.

[37] M. Bhatia and J. K. Maitra, "E-learning Platforms Security Issues and Vulnerability Analysis," in 2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES), 14-15 Sept. 2018 2018, pp. 276-285, doi: 10.1109/CCTES.2018.8674115.

[38] C. Ling, U. Balcı, J. Blackburn, and G. Stringhini, "A First Look at Zoombombing," in 2021 IEEE Symposium on Security and Privacy (SP), 24-27 May 2021 2021, pp. 1452-1467, doi: 10.1109/SP40001.2021.00061.

[39] T. Reisinger, I. Wagner, and E. A. Boiten, "Security and Privacy in Unified Communication," ACM Comput. Surv., vol. 55, no. 3, 2022/2 2022, doi: 10.1145/3498335.

[40] F. D. Salimovna, Y. N. Salimovna, and I. S. Z. ugli, "Security issues in E-Learning system," in 2019 International Conference on Information Science and Communications Technologies (ICISCT), 4-6 Nov. 2019 2019, pp. 1-4, doi: 10.1109/ICISCT47635.2019.9011971.

[41] N. Salameh and A. Ali, "E-learning virtual meeting applications: A comparative study from a cybersecurity perspective," Indonesian Journal of Electrical Engineering and Computer Science, vol. 24, p. 1121, 11/01 2021, doi: 10.11591/ijeecs.v24.i2.pp1121-1129.

[42] E. Vanezi et al., "GDPR Compliance in the Design of the INFORM e-Learning Platform: a Case Study," in 2019 13th International Conference on Research Challenges in Information Science (RCIS), 29-31 May 2019 2019, pp. 1-12, doi: 10.1109/RCIS.2019.8877022.

[43] A. Aborujilah, E. Y. Al-Alawi, D. A. Al-Hidabi, and A. Z. Al-Othmani, "Exploring Critical Challenges and Factors Influencing E-Learning Systems Security During COVID-19 Pandemic," in 2022 International Conference on Intelligent Technology, System and Service for Internet of Everything (ITSS-IoE), 3-5 Dec. 2022 2022, pp. 1-5, doi: 10.1109/ITSS-IoE56359.2022.9990935.

[44] M. Anghel and G.-C. Pereteanu, "Cyber Security Approaches in E-Learning," INTED2020 Proc., vol. 1, no. April 2021, pp. 4820–4825, 2020, doi: 10.21125/inted.2020.1323.

[45] MITRE, "CWE - 2022 CWE Top 25 Most Dangerous Software Weaknesses," CWE, 2022." [Online], Available: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html [Accessed: 30 December 2022].

[46] OWASP, "OWASP Top Ten Web Application Security Risks" 2021, [Online], Available: https://owasp.org/www-project-top-ten/ , [Accessed: 28 December 2022].

[47] MITRE, "CVE Details" [Online], Available: https://www.cvedetails.com/ [Accessed: 30 December 2022].

[48] H. Ibrahim, S. Karabatak, and A. A. Abdullahi, "A Study on Cybersecurity Challenges in E-learning and Database Management System," in 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 1-2 June 2020 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116415.

[49] Sharma, "E-Learning Platform Security Issues and Their Prevention Techniques : a Review," 2021.

[50] University Of Edinburgh, "Information Security Top 10", [Online], Available: https://infosec.ed.ac.uk/information-security-updates/information-security-top-10, [Accessed: 30 January 2023].

[51] J. Lewis, "Video Conferencing Technology and Risk," Center for Strategic and International Studies (CSIS), 2020. Accessed: 2023/02/19/. [Online]. Available: http://www.jstor.org/stable/resrep27641

[52] T. Isobe and R. Ito, "Security Analysis of End-to-End Encryption for Zoom Meetings," IEEE Access, vol. 9, pp. 90677-90689, 2021, doi: 10.1109/ACCESS.2021.3091722.

[53] H. Chang, M. Varvello, F. Hao and S. Mukherjee, "A Tale of Three Videoconferencing Applications: Zoom, Webex, and Meet," in IEEE/ACM Transactions on Networking, vol. 30, no. 5, pp. 2343-2358, Oct. 2022, doi: 10.1109/TNET.2022.3171467.

[54] N. Cavus and D. Sekyere-Asiedu, "A comparison of online video conference platforms: Their contributions to education during COVID-19 pandemic," World Journal on Educational Technology: Current Issues, vol. 13, pp. 1180-1191, 10/31 2021, doi: 10.18844/wjet.v13i4.6329.

[55] R. Hasan and R. Hasan, "Towards a Threat Model and Security Analysis of Video Conferencing Systems," 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), 2021, pp. 1-4, doi: 10.1109/CCNC49032.2021.9369505.

[56] Matt Woods “CIS Videoconferencing Security Guide” Center for Internet Security 2020 [Online], Available: https://www.cisecurity.org/insights/white-papers/videoconferencing-security-guide [Accessed 25 October 2022].

[57] L. Nataly Basto Zabala, C. Santiago Rodríguez Velasco and H. Dario Jaimes Parada, "Security scheme for Moodle platforms based on a multi-layered model," 2022 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI), 2022, pp. 1-5, doi: 10.1109/CONIITI57704.2022.9953679.

[58] S. A. Bhat, D. Alyahya, M. A. Dar and S. Shah, "Edge-Computing based Secure E-learning Platforms," 2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2022, pp. 324-328, doi: 10.1109/ICAIIC54071.2022.9722680.

[59] P. D. Nguyen, Z. Rajnai, and K. András, "E-Learning Security Risks and its Countermeasures," Emerging research and Solution in ICT, vol. 1, pp. 17-25, 04/01 2016, doi: 10.20544/ERSICT.01.16.P02.

[60] I. Cvitić, D. Perakovic, M. Periša, and A. Jurcut, "Methodology for Detecting Cyber Intrusions in e-Learning Systems during COVID-19 Pandemic," Mobile Networks and Applications, 06/06 2021, doi: 10.1007/s11036-021-01789-3.

[61] N. H. Gauthier and M. I. Husain, "Dynamic Security Analysis of Zoom, Google Meet and Microsoft Teams," in Silicon Valley Cybersecurity Conference, Cham, Y. Park, D. Jadav, and T. Austin, Eds., 2021// 2021: Springer International Publishing, pp. 3-24.

[62] Z. Khalid, F. Iqbal, F. Kamoun, L. A. Khan, and B. Shah, "Forensic investigation of Cisco WebEx desktop client, web, and Android smartphone applications," Annals of Telecommunications, 2022/08/12 2022, doi: 10.1007/s12243-022-00919-6.

[63] N. Rjaibi and L. Ben Arfa Rabai, "Deploying Suitable Countermeasures to Solve the Security Problems within an E-learning Environment," ACM International Conference Proceeding Series, vol. 2014, pp. 33-38, 09/09 2014, doi: 10.1145/2659651.2659721.

[64] R. Badhwar, "Secure Video Conferencing and Online Collaboration," in The CISO's Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms, R. Badhwar Ed. Cham: Springer International Publishing, 2021, pp. 87-92.

[65] M. A. H. B. Azhar, J. Timms, and B. Tilley, "Forensic Investigations of Google Meet and Microsoft Teams – Two Popular Conferencing Tools in the Pandemic," 2021, pp. 20-34.

[66] MITRE, "CVE Details - Moodle : Vulnerability Statistics" [Online], Available: https://www.cvedetails.com/product/3590/?q=moodle, [Accessed: 4 January 2023].

[67] MITRE, "CVE Details - Blackboard : Vulnerability Statistics" [Online], Available: https://www.cvedetails.com/vendor/504/Blackboard.html, [Accessed: 4 January 2023].

[68] MITRE, "CVE Details - Gunet : Vulnerability Statistics" [Online], Available: https://www.cvedetails.com/vendor/23640/Gunet.html, [Accessed: 4 January 2023].

[69] MITRE, "CVE Details - Zoom : Vulnerability Statistics" [Online], Available: https://www.cvedetails.com/vendor/2159/Zoom.html, [Accessed: 7 January 2023].

[70] MITRE, "CVE Details - Cisco Webex Meetings: Vulnerability Statistics" [Online], Available: https://www.cvedetails.com/product/32694/Cisco-Webex-Meetings.html?vendor_id=16 [Accessed: 7 January 2023].

[71] MITRE, "CVE Details - Microsoft Teams: Vulnerability Statistics" [Online], Available: https://www.cvedetails.com/product/77872/Microsoft-Teams.html?vendor_id=26 [Accessed: 7 January 2023].