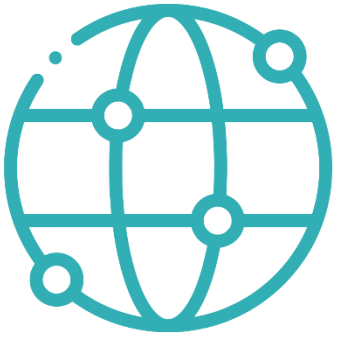
Ενότητα 10:
Κυβερνοασφάλεια και Κυβερνοανθεκτικότητα στις Τουριστικές ΜμΕ

DIGITOUR



Co-funded by the
Erasmus+ Programme
of the European Union

Τίτλος έργου: Ανάπτυξη της Ψηφιακής Ετοιμότητας των Μικρομεσαίων Επιχειρήσεων (ΜμΕ) στον τομέα του Τουρισμού

Ακρωνύμιο έργου: DIGITOUR

Κωδικός έργου: 2021-2-IE01-KA220-VET-000048348

Διδακτική Ενότητα: Κυβερνοασφάλεια & Κυβερνοανθεκτικότητα στις Τουριστικές ΜμΕ

Κύρια ομάδα-στόχος: ΜμΕ στον τομέα του τουρισμού

Δευτερεύουσες ομάδες-στόχοι: εξειδικευμένοι πάροχοι ΕΕΚ, εκπρόσωποι του τουριστικού κλάδου, και εκπαιδευτές/τριες που παρέχουν ενδοεπιχειρησιακή κατάρτιση.

Εκτιμώμενη διάρκεια: 120 – 150 λεπτά

Στόχοι:

- Κατανόησης των προκλήσεων, των κινδύνων αλλά και της σημασίας των συστημάτων Κυβερνοασφάλειας.

- Εξοικείωση με τις βασικές έννοιες-κλειδιά και τους τεχνικούς όρους που σχετίζονται με το αντικείμενο, που θα βοηθήσουν τους/τις εκπαιδευόμενους/ες να ενισχύσουν την ασφάλεια και την ανθεκτικότητα της επιχείρησης στον κυβερνοχώρο.

Co-funded by the Erasmus+ Programme of the European Union

- Κατανόηση της σημασίας που έχει για μια επιχείρηση η εφαρμογή συστημάτων Κυβερνοασφάλειας & Κυβερνοανθεκτικότητας και τα οφέλη από αυτήν την εφαρμογή, με την καλλιέργεια σχετικών δεξιοτήτων.

Μαθησιακά αποτελέσματα: με την ολοκλήρωση αυτής της ενότητας, οι εκπαιδευόμενοι/ες θα είναι σε θέση:

- Να περιγράψουν τη σημασία των όρων «Κυβερνοασφάλεια» και «Κυβερνοανθεκτικότητα» και να κατανοούν γιατί είναι απολύτως απαραίτητες στους τουριστικούς παρόχους κάθε είδους·
- Να προχωρήσουν στην κατανόηση βασικών και θεμελιωδών εννοιών γύρω από την ασφάλεια και την ανθεκτικότητα στον κυβερνοχώρο·
- Να γνωρίζουν τους κυριότερους κινδύνους και επιθέσεις στον κυβερνοχώρο που αφορούν τον τουριστικό κλάδο·
- Να είναι ενήμεροι/ες σχετικά με τις καλές πρακτικές για την επίτευξη της ασφάλειας και της ανθεκτικότητας μίας επιχείρησης στον κυβερνοχώρο·
- Να αναλύουν τους βασικούς πυλώνες των αποτελεσματικών, ασφαλών και ανθεκτικών συστημάτων και να γνωρίζουν τα κύρια πρότυπα ασφάλειας και ανθεκτικότητας στον κυβερνοχώρο.

Το παρόν πρόγραμμα έχει χρηματοδοτηθεί με την υποστήριξη της Ευρωπαϊκής Επιτροπής. Η παρούσα δημοσίευση αντικατοπτρίζει αποκλειστικά τις απόψεις του συντάκτη της, και συνεπώς η Επιτροπή δεν

φέρει καμία ευθύνη για οποιουδήποτε είδους τυχόν χρήση των πληροφοριών που εμπεριέχονται σε αυτή. Επιτρέπεται η αναπαραγωγή, με αναφορά της πηγής.

Περιεχόμενα

Co-funded by the
Erasmus+ Programme
of the European Union

10.1 Εισαγωγή: Κατευθυντήριες Αρχές και Ορισμοί

Τι είναι η Κυβερνοασφάλεια (cyber security);

Αν και υπάρχουν ποικίλοι ορισμοί για την Κυβερνοασφάλεια, σε γενικές γραμμές, όλοι συγκλίνουν στην έννοια της ασφάλειας στον κυβερνοχώρο.

Ως κυβερνοχώρος ορίζεται το δυναμικό και εικονικό περιβάλλον, στο οποίο συνδέονται διαφορετικά συστήματα ηλεκτρονικών υπολογιστών.

https://northafricapost.com/42416-morocco-is-not-a-cyber-jungle-defense-administration-tells-amnesty.html

Ο όρος Κυβερνοασφάλεια αποτελείται από **2 βασικές έννοιες-κλειδιά:**

1. Το πρώτο συνθετικό *κυβερνο- (cyber)* αφορά την τεχνολογία που σχετίζεται με πληροφοριακά συστήματα, δίκτυα ή/και δεδομένα.
2. Η *ασφάλεια* σχετίζεται με την έννοια της προστασίας, η οποία περιλαμβάνει την ασφάλεια συστημάτων, την ασφάλεια δικτύων και την ασφάλεια εφαρμογών και πληροφοριών.

Η ΕΕ ορίζει την Κυβερνοασφάλεια ως «*τις δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων*».

Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα, γνωστές ως τριάδα CIA, αποτελούν τις 3 βασικές αρχές της Κυβερνοασφάλεια.

- ***Εμπιστευτικότητα (Confidentiality):*** τα μέτρα για την εξασφάλιση της εμπιστευτικότητας αποτρέπουν την αποκάλυψη ευαίσθητων πληροφοριών χωρίς εξουσιοδοτημένη πρόσβαση (π.χ. κρυπτογράφηση δεδομένων, έλεγχος ταυτότητας δύο παραγόντων).

- ***Ακεραιότητα (Integrity):*** τα μέτρα για την ακεραιότητα εξασφαλίζουν τη διατήρηση της συνέπειας, της ακρίβειας και της αξιοπιστίας των δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής τους, εμποδίζοντας την τροποποίησή τους από μη εξουσιοδοτημένα μέρη (π.χ. δημιουργία αντιγράφων ασφαλείας, άδεια πρόσβασης αρχείων).
- ***Διαθεσιμότητα (Availability):*** τα μέτρα για την διαθεσιμότητα διασφαλίζουν ότι οι πληροφορίες είναι συνεχώς και εύκολα προσβάσιμες στα εξουσιοδοτημένα μέρη, και συντηρούν τα υλικά και λογισμικά συστήματα στα οποία αυτές αποθηκεύονται και εμφανίζονται.

Συνολικά, η Κυβερνοασφάλεια αφορά καθετί που συντελεί στην προστασία ενός οργανισμού, των εργαζομένων του και των περιουσιακών στοιχείων του, ενάντια σε κυβερνοαπειλές ή κυβερνοεπιθέσεις.

https://thingscouplesdo.com/what-is-cia-triad-and-how-does-it-work/

Τι είναι η Κυβερνοανθεκτικότητα (cyber resilience);

Στον επιχειρηματικό κόσμο, η Κυβερνοανθεκτικότητα προσφέρει μια πιο ολοκληρωμένη προσέγγιση για την αδιάλειπτη συνέχεια της ψηφιακής λειτουργίας μιας επιχείρησης. Πρόκειται για μία νέα ιδέα, η οποία αναφέρεται και ως digital fitness.

Η ΕΕ ορίζει την Κυβερνοανθεκτικότητα ως «την ικανότητα για προστασία των ηλεκτρονικών δεδομένων και συστημάτων από κυβερνοεπιθέσεις, καθώς και για

ταχεία επαναλειτουργία μιας επιχείρησης σε περίπτωση επιτυχημένης επίθεσης».

Σε ένα περιβάλλον προηγμένων και σύνθετων απειλών, οι παραδοσιακές τακτικές προστασίας που εστιάζουν στην Κυβερνοασφάλεια αδυνατούν να ανταποκριθούν αποτελεσματικά. Κανένας οργανισμός δεν μπορεί ταυτόχρονα να ελέγχει όλες τις μεταβλητές, να ανιχνεύει τα τρωτά σημεία και να εφαρμόζει πολιτικές ασφαλείας σε διαφορετικά συστήματα.

Για να διαχειριστούν αυτές τις ανταγωνιστικές προκλήσεις, οι οργανισμοί θα πρέπει να αλλάξουν μεθόδους, και αντί να εστιάζουν στην άμυνα εναντίον κακόβουλων λογισμικών, να υιοθετήσουν μία πιο ρεαλιστική και ανθεκτική προσέγγιση, την Κυβερνοανθεκτικότητα (Symantec, 2014).

Η ιδέα της Κυβερνοανθεκτικότητας μπορεί να γίνει αντιληπτή ως ένα πλαίσιο, αποτελούμενο από 5 βασικούς άξονες.

1. **Προετοιμασία/ Αναγνώριση:** κατανόηση του τρόπου προστασίας της επιχείρησης και αναγνώριση πιθανών κινδύνων με σκοπό τον εντοπισμό τρωτών σημείων στο σύστημα ασφαλείας·
2. **Προστασία:** η κατανόηση του τοπίου των κυβερνοαπειλών της επιχείρησης (π.χ. του βαθμού ευαλωτότητας και αντοχής της σε ενδεχόμενους κινδύνους) εξασφαλίζει την ύπαρξη υποδομών προστασίας·
3. **Ανίχνευση:** μετά την εγκατάσταση των μέτρων προστασίας, μπορούν να καθοριστούν οι κατάλληλες ενέργειες για την ταχεία ανίχνευση μίας επίθεσης, τον προσδιορισμό των συστημάτων που έχουν προσβληθεί και την διασφάλιση έγκαιρης αντίδρασης·
4. **Αντίδραση:** σε αυτό το στάδιο είναι κρίσιμη η καθοδήγηση ως προς το ποιες ενέργειες μπορούν να συμβάλουν στην επιτάχυνση του χρόνου αντίδρασης και να περιορίσουν τις συνέπειες της επίθεσης αφότου αυτή εντοπιστεί·
5. **Αποκατάσταση:** το στάδιο ανάπτυξης και εφαρμογής των κατάλληλων συστημάτων για την ανάκτηση δεδομένων σε περίπτωση κυβερνοεπίθεσης,

το οποίο αποτελεί βασικό συστατικό κάθε ανθεκτικής στρατηγικής ασφαλείας.

https://www.amdhservicesltd.com/how-to-build-a-cyber-resilient-infrastructure

Πώς συνδέονται η Κυβερνοασφάλεια με την Κυβερνοανθεκτικότητα;

Οι έννοιες Κυβερνοασφάλεια και Κυβερνοανθεκτικότητα ενδέχεται συχνά να φαίνονται εναλλάξιμες, δεδομένου ότι αναφέρονται αμφότερες στο ζήτημα της ασφάλειας στον κυβερνοχώρο. Παρ' όλα αυτά, δεν ταυτίζονται:

- Η Κυβερνοασφάλεια αφορά τις ενέργειες περιορισμού των απειλών ενός οργανισμού, διατηρώντας μια ενεργητική προνοητική διάθεση ενάντια στον ολοένα και αυξανόμενο κίνδυνο των κυβερνοεπιθέσεων.

- Η Κυβερνοανθεκτικότητα αφορά τις ενέργειες ενός οργανισμού να περιορίσει όσο το δυνατόν περισσότερο την πιθανή ζημιά και τις απώλειες που μπορεί να προκληθούν άπαξ και λάβει χώρα μία επίθεση, ενώ παράλληλα εξακολουθεί να εκτελεί κανονικά την καθιερωμένη δραστηριότητά του.

10.2 Κυβερνοασφάλεια και Κυβερνοανθεκτικότητα εντός πλαισίου

Κυβερνοασφάλεια και Κυβερνοανθεκτικότητα στον Τουρισμό

Όσον αφορά τους τομείς του τουρισμού και των ταξιδιών, η ψηφιοποίηση έχει διευκολύνει πολύ τις επιχειρήσεις στον σημερινό ψηφιακό κόσμο.

Η ασφάλεια και η ανθεκτικότητα στον κυβερνοχώρο είναι τόσο σημαντικές, όσο και η ψηφιακή καινοτομία την οποία διαφυλάσσουν:

- Η ψηφιακή καινοτομία επαναπροσδιόρισε την τουριστική εμπειρία, και κατέστησε τον τουριστικό κλάδο πιο επιρρεπή σε κινδύνους για την ασφάλεια.
- Η Κυβερνοασφάλεια και η Κυβερνοανθεκτικότητα αποτελούν εργαλεία που διαμορφώνουν τον κλάδο και μπορούν να διασφαλίσουν ένα ασφαλέστερο μέλλον για τον τουρισμό και τις τουριστικές Μικρομεσαίες Επιχειρήσεις (ΜμΕ).

Πλέον, η τεχνολογία παίζει καθοριστικό ρόλο σχεδόν σε κάθε πτυχή της ταξιδιωτικής και της τουριστικής εμπειρίας:

- από το να εμπνέει τους τουρίστες, κατά το στάδιο στο ταξίδι του καταναλωτή πριν την αγορά,
- έως και την online καταχώρηση κριτικής ή σχολίων στο στάδιο μετά την αγορά.

Συχνά περιλαμβάνει ηλεκτρονικές συναλλαγές, ευαίσθητες πληροφορίες των καταναλωτών, ενσωμάτωση στο υπολογιστικό νέφος (cloud), και τεχνολογία ψηφιακών πληρωμών, τα οποία ως αποτέλεσμα έχουν αυξήσει το ψηφιακό αποτύπωμα των τουριστικών επιχειρήσεων, αφήνοντάς τες εκτεθειμένες σε κυβερνοαπειλές και κυβερνοεπιθέσεις, ορισμένες εκ των οποίων μπορεί να συνιστούν και κυβερνοεγκλήματα (Παρασκευάς, 2020).

Από το 2010, έχουν αναφερθεί αρκετές παραβιάσεις Κυβερνοασφάλειας, ακόμα κι από τις μεγαλύτερες ξενοδοχειακές αλυσίδες παγκοσμίως:

- Το 2020, ο όμιλος ξενοδοχείων Marriott International είχε την ευθύνη για ένα περιστατικό παραβίασης δεδομένων, καθώς απέτυχε να προστατέψει τα προσωπικά δεδομένα των πελατών του και άφησε να διαρρεύσουν ονοματεπώνυμα, ηλεκτρονικές διευθύνσεις, αριθμοί λογαριασμών επιβράβευσης, και πολλές άλλες ευαίσθητες πληροφορίες.
- Αυτή η επίθεση υπολογίζεται ότι αφορούσε περίπου 340 εκατομμύρια επισκέπτες. Δύο χρόνια νωρίτερα, το 2018, η Marriott International είχε λάβει από ένα εργαλείο εσωτερικής ασφάλειας ειδοποίηση, η οποία αφορούσε απόπειρα μη εξουσιοδοτημένης πρόσβασης στη βάση δεδομένων των κρατήσεων τους στις ΗΠΑ.
- Περαιτέρω έρευνα των ειδικών στην Κυβερνοασφάλεια αποκάλυψε ότι μη εξουσιοδοτημένη πρόσβαση στο σύστημα κρατήσεων του ξενοδοχείου είχε λάβει χώρα ήδη από το 2014 (Secure Stay, 2020).

https://gritdaily.com/marriott-hit-by-second-data-breach-2020/

Ο αντίκτυπος των κυβερνοαπειλών ή/και των κυβερνοεπιθέσεων μπορεί να βλάψει σημαντικά τη φήμη μίας επωνυμίας και την εμπιστοσύνη των καταναλωτών, και να επιφέρει σημαντικές οικονομικές, νομικές και κανονιστικές επιπτώσεις. Οι πάροχοι τουριστικών υπηρεσιών μπορεί να υποστούν τόσο άμεσες όσο και έμμεσες οικονομικές απώλειες (Παρασκευάς, 2020) –

- Άμεσες οικονομικές απώλειες: εταιρικά έξοδα που αφορούν υπηρεσίες πληροφορικής και ανάκτησης δεδομένων, καθώς και δικαστικά έξοδα και αμοιβές υπηρεσιών δημοσίων σχέσεων.
- Έμμεσες οικονομικές απώλειες: έξοδα πρόσληψης επιπλέον τεχνικού προσωπικού, κόστος επιμόρφωσης του γενικού προσωπικού σχετικά με την Κυβερνοασφάλεια και την Κυβερνοανθεκτικότητα, αναβάθμισης των συστημάτων Κυβερνοασφάλειας κ.ά.
- Ζημιά στην φήμη και την υπόληψη: σε περίπτωση παραβίασης δεδομένων, πρέπει να συνυπολογιστεί και το κόστος στη φήμη και την υπόληψη της εταιρείας, το οποίο μπορεί να αποβεί τεράστιο και να μειώσει την εμπιστοσύνη και τις κρατήσεις των πελατών. Οι τουριστικοί πάροχοι οφείλουν να αναγνωρίζουν την υποχρέωσή τους να διασφαλίζουν την προστασία των δεδομένων και των πληροφοριών για να αποφύγουν σημαντικές αρνητικές συνέπειες για την επιχείρησή τους.

Επομένως, είναι εξαιρετικά σημαντικό για τις επιχειρήσεις, και ειδικά για τις ΜμΕ που απασχολούνται στον τομέα των ταξιδιών και του τουρισμού, να κατανοήσουν την σπουδαιότητα της Κυβερνοασφάλειας και της

Κυβερνοανθεκτικότητας και να τις θέσουν χωρίς δεύτερη σκέψη ως προτεραιότητες.

Εξελίξεις μετά τον Covid-19

Στον απόηχο της παγκόσμιας πανδημίας, η οποία ανάγκασε την τουριστική βιομηχανία να μεταφέρει της δραστηριότητές της online, ο κλάδος των ταξιδιών και του τουρισμού κλήθηκε να επαναπροσδιορίσει τα προϊόντα, τις υπηρεσίες και την εμπειρία που προσφέρει στον καταναλωτή, ώστε να αντεπεξέλθει στην νέα πραγματικότητα.

Στην εποχή μετά τον Covid-19, το πλήθος των κυβερνοεπιθέσεων έχει αγγίξει επίπεδα άνευ προηγουμένου.

Το Παγκόσμιο Συμβούλιο Τουρισμού και Ταξιδιών (WTTC) αναφέρει ότι η εσπευσμένη ανάπτυξη των ψηφιακών δραστηριοτήτων άφησε την τουριστική βιομηχανία πιο ευάλωτη και εκτεθειμένη σε κινδύνους στον κυβερνοχώρο (World Travel & Tourism Council και Microsoft, 2022).

Το γεγονός αυτό ενθάρρυνε τις επιχειρήσεις να επανεξετάσουν τη στάση τους απέναντι στην ασφάλεια με σκοπό να γίνουν πιο ανθεκτικές, καθώς επίσης και τους επιχειρηματίες να προβούν σε ποιοτικές ενέργειες για την Κυβερνοασφάλεια και την Κυβερνοανθεκτικότητα.

https://www.idealarticleswriter.com/2023/03/-Understanding-Digital-Forensics-Process-Techniques-and-Tools-.html

Οι δράστες των κυβερνοαπειλών, όντας επιδέξιοι και σε εγρήγορση, είδαν τον Covid-19 ως ευκαιρία να εκμεταλλευτούν τα τρωτά σημεία των παρόχων

τουριστικών υπηρεσιών που επιχειρούσαν να διευκολύνουν τα ταξίδια και ταυτόχρονα να προστατεύσουν τη δημόσια υγεία. Οι συνεχόμενοι και αντιφατικοί περιορισμοί άφησαν πολύ ελεύθερο χώρο για κυβερνοεπιθέσεις.

Η εφαρμογή της εξ αποστάσεως εργασίας, η οποία οδήγησε σε περαιτέρω εξάρτηση από τις προσωπικές και φορητές συσκευές, μετατόπισε ακόμα περισσότερο την ευθύνη για την Κυβερνοασφάλεια των εταιρειών στους εργαζόμενους.

https://www.techtarget.com/searchitoperations/news/365534899/Securing-remote-access-grows-crucial-for-DevSecOps

Αν και τα κυβερνο-οικοσυστήματα στις εγκαταστάσεις των εταιρειών τείνουν να είναι ασφαλή, αυτού του είδους η προστασία μέχρι προηγουμένως δεν είχε επεκταθεί και στις οικίες των εργαζόμενων. Κατά συνέπεια, οι δράστες των επιθέσεων, οι οποίοι αποκτούσαν πρόσβαση στα οικιακά ή δημόσια δίκτυα Wi-Fi μπορούσαν εύκολα να παραβιάσουν τα συστήματα των εταιρειών, γεγονός που τόνισε την ανάγκη για μία πιο ολοκληρωμένη προσέγγιση της Κυβερνοασφάλειας, με έμφαση στην Κυβερνοανθεκτικότητα.

Παρ' όλο που οι οργανισμοί δεν είναι σε θέση να εγγυηθούν απολύτως την ασφάλεια των οικιακών ή των δημόσιων δικτύων Wi-Fi, η επιμόρφωση του προσωπικού μπορεί να συμβάλει στην προστασία των εργαζομένων ενάντια σε

επιθέσεις, όταν κάνουν χρήση συσκευών συνδεδεμένων στο Διαδίκτυο των Πραγμάτων (Internet of Things).

Οι κυβερνοαπειλές που προέκυψαν ως αποτέλεσμα του COVID-19 δεν πρέπει να αντιμετωπίζονται ως ανεξάρτητος οργανωτικός κίνδυνος, ομοίως ούτε και οι κίνδυνοι στον κυβερνοχώρο που σχετίζονται με τα υβριδικά μοντέλα εργασίας.

Ως εκ τούτου, για τη διασφάλιση της Κυβερνοανθεκτικότητας, οι οργανισμοί θα πρέπει να διευρύνουν τις προσπάθειές παρακολούθησης κυβερνοαπειλών, ώστε να συμπεριλάβουν πιθανά σημεία εισόδου επιθέσεων διαμέσου των οικιακών και των δημόσιων δικτύων Wi-Fi (World Travel & Tourism Council και Microsoft, 2022).

10.3 Ευαλωτότητα των τουριστικών ΜμΕ στον Κυβερνοχώρο

Με ποιους τρόπους είναι ευάλωτες οι τουριστικές ΜμΕ;

Σύμφωνα με το WTTC, περισσότερες από 7 στις 10 (72%) ΜμΕ στο Ηνωμένο Βασίλειο, στις ΗΠΑ και στην Ευρώπη έχουν πέσει θύμα τουλάχιστον μίας κυβερνοεπίθεσης (World Travel & Tourism Council και Microsoft, 2022).

Στην περίπτωση της βιομηχανίας των ταξιδιών και του τουρισμού, η οποία αποτελείται κυρίως από ΜμΕ, όπως πρακτορεία και τουριστικά γραφεία, το ποσοστό είναι ακόμα υψηλότερο, δεδομένου ότι οι ΜμΕ αποτελούν περίπου το 80% του συνόλου των επιχειρήσεων.

«Γνώριζες ότι κάθε 39 δευτερόλεπτα συμβαίνει μία κυβερνοεπίθεση, και ότι 291 αρχεία δεδομένων διαρρέουν κάθε δευτερόλεπτο;»

https://wisedistribution.co.uk/deception-technology/

Τα τελευταία χρόνια, οι τουριστικές ΜμΕ έχουν γίνει ιδιαίτερα ελκυστικός στόχος για τους εγκληματίες του κυβερνοχώρου:

- Το υψηλό επίπεδο ψηφιακής ωριμότητας έχει καταστήσει τις τουριστικές ΜμΕ μία εξαιρετικά ευάλωτη βιομηχανία όσον αφορά την Κυβερνοασφάλεια και την Κυβερνοανθεκτικότητα, ιδίως εξαιτίας της ελλιπούς άμυνάς τους στον τομέα της πληροφορικής και στα συστήματα των σημείων πώλησης (POS) (Fragniere & Yagci, 2021). Σύμφωνα με τον Hussain (2023), οι χάκερς έχουν αντιληφθεί ότι οι ΜμΕ αποτελούν

ευκολότερο στόχο συγκριτικά με μεγαλύτερες εταιρείες με ελλιπή Κυβερνοασφάλεια, είτε λόγω έλλειψης εξειδικευμένου και έμπειρου προσωπικού (δηλαδή ανθρώπινου σφάλματος), είτε λόγω ανεπαρκών πόρων.

- Οι τουριστικές ΜμΕ είναι εξαιρετικά ευάλωτες σε κυβερνοαπειλές, διότι αποθηκεύουν στον κυβερνοχώρο εξαιρετικά ευαίσθητα δεδομένα και αναλύσεις δεδομένων (analytics), τα οποία αποτελούν πολύτιμες πληροφορίες για τους εγκληματίες του κυβερνοχώρου που επιχειρούν να παραβιάσουν τέτοιου είδους δεδομένα, οδηγώντας στην κλοπή ταυτότητας και οικονομικών στοιχείων και θέτοντας σε κίνδυνο τη διακυβέρνηση δεδομένων και το απόρρητο των προσωπικών στοιχείων των πελατών και των εργαζομένων (διευθύνσεις e-mail πελατών, αριθμούς διαβατηρίων, στοιχεία πιστωτικών καρτών, κτλ.).
- Η βιομηχανία των τουριστικών ΜμΕ είναι ιδιαίτερα επιρρεπής σε κυβερνοαπειλές, καθώς αποτελεί φύσει κατακερματισμένο κλάδο και ολόκληρη η αλυσίδα εφοδιασμού της, η οποία περιλαμβάνει αναρίθμητους πράκτορες και τρίτους παρόχους υπηρεσιών, αποτελεί δυνάμει πεδίο εισόδου κυβερνοαπειλών. Η λήψη προληπτικών μέτρων Κυβερνοασφάλειας είναι απαραίτητη για την εξασφάλιση της Κυβερνοανθεκτικότητας και τη διατήρηση της αποτελεσματικής λειτουργίας της επιχείρησης.

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) διαπίστωσε ότι το 90% των ΜμΕ δήλωσε ότι ένα ζήτημα ασφάλειας στον κυβερνοχώρο θα μπορούσε να επιφέρει σοβαρές αρνητικές συνέπειες στις επιχειρήσεις τους ακόμη και εντός μίας εβδομάδας αφότου εκδηλωθεί, με το 57% να υποστηρίζει ότι κατά πάσα πιθανότητα αυτό θα τους οδηγούσε σε χρεωκοπία ή στο κλείσιμο της επιχείρησης.

https://www.enisa.europa.eu/

Πώς πρέπει να αντιδράσει μία ΜμΕ σε περίπτωση παραβίασης;

Στην περίπτωση παραβίασης των δεδομένων της, η επιχείρηση συνιστάται να γνωστοποιήσει την εν λόγω παραβίαση στον υπεύθυνο προστασίας δεδομένων και πληροφοριών, και να καταθέσει την σχετική ηλεκτρονική φόρμα γνωστοποίησης εντός 72 ωρών από την στιγμή που αντιλήφθηκε την παραβίαση.

Εάν η παραβίαση θέτει σε κίνδυνο το υποκείμενο στο οποίο αναφέρονται τα δεδομένα, η επιχείρηση οφείλει να ενημερώσει την αρμόδια εποπτεύουσα Αρχή.

Αυτές είναι 5 συγκεκριμένες ενέργειες στις οποίες μπορεί να προβεί μία ΜμΕ σε περίπτωση παραβίασης των δεδομένων της.

1. Αναγνώριση της πηγής και του μεγέθους της παραβίασης.
2. Ειδοποίηση της ειδικής ομάδας δράσης για τις παραβιάσεις και αντιμετώπιση της παραβίασης το συντομότερο δυνατόν.
3. Δοκιμή της επιδιόρθωσης της ασφάλειας.
4. Ενημέρωση των αρχών και όλων των θιγόμενων πελατών.
5. Προετοιμασία για την διαχείριση και τον έλεγχο της ζημιάς μετά την παραβίαση.

10.4 Κυβερνοαπειλές κατά των τουριστικών ΜμΕ

Τι είναι οι κυβερνοαπειλές;

Κάθε περίπτωση ή συμβάν που έχει τη δυνατότητα να επιφέρει αρνητικές επιπτώσεις στη λειτουργία, τα περιουσιακά στοιχεία και τους εργαζόμενους μίας επιχείρησης, και/ ή σε άλλους οργανισμούς, ή σε ένα έθνος, μέσω μη εξουσιοδοτημένης πρόσβασης, καταστροφής, αποκάλυψης, τροποποίησης πληροφοριών και/ή άρνησης παροχής υπηρεσιών εντός ενός συστήματος.

Υπάρχουν 3 βασικά είδη κυβερνοαπειλών:

1. Το κυβερνοέγκλημα, το οποίο περιλαμβάνει μεμονωμένους δράστες ή ομάδες ατόμων που στοχεύουν συγκεκριμένα συστήματα, με σκοπό το οικονομικό κέρδος ή την αποδιοργάνωση και την πρόκληση αναστάτωσης.
2. Η κυβερνοεπίθεση, που συχνά αφορά τη συλλογή πληροφοριών με πολιτικά κίνητρα.
3. Η κυβερνοτρομοκρατία, που αποτελεί την εσκεμμένη υπονόμευση ηλεκτρονικών συστημάτων, επιδιώκοντας να προκαλέσει πανικό ή φόβο.

Ποιοι είναι τα βασικά είδη κυβερνοαπειλών κατά των τουριστικών ΜμΕ;

Όσον αφορά τις απόπειρες κυβερνοαπειλής, οι τουριστικές ΜμΕ αποτελούν μία από τις πιο βαριά πληγείσες βιομηχανίες παγκοσμίως.

Οι κυβερνοεπιθέσεις στον τουριστικό τομέα στοχεύουν κυρίως στοιχεία πιστωτικών καρτών και ταυτοτήτων, προγράμματα επιβράβευσης ξενοδοχείων και δημόσια διαθέσιμα δεδομένα διαδικτύου (Walson, 2022).

Μία έκθεση της PwC για τις Προοπτικές των Ξενοδοχείων που καλύπτει το διάστημα από το 2018 ως το 2022, αναφέρει ότι η βιομηχανία των ξενοδοχείων είχε τον μεγαλύτερο αριθμό παραβιάσεων δεδομένων μετά τον τομέα του λιανικού εμπορίου.

Σύμφωνα με το WTTC, η απειλή μέσω απάτης ηλεκτρονικού ψαρέματος (phishing), κακόβουλων λογισμικών (malware) και λυτρισμικών (ransomware) παραμένει συνεχής, με τα ransomware να οφείλονται για το 23% των κυβερνοεπιθέσεων το 2021, ενώ 33% των επιθέσεων έγινε μέσω phishing. Οι εγκληματίες του κυβερνοχώρου αποκτούν πρόσβαση σε διαδικτυακά περιβάλλοντα κυρίως μέσω του phishing, της κλοπής διαπιστευτηρίων ή του

απομακρυσμένου ελέγχου υπολογιστών (World Travel & Tourism Council και Microsoft, 2022).

https://motyl-szary.com/2023/03/31/top-cybersecurity-threats-and-proactive-measures-to-protect-personal-and-business-data/

Οι συνηθέστερες μέθοδοι που χρησιμοποιούν οι κακόβουλοι δράστες, όταν επιχειρούν να απειλήσουν την Κυβερνοασφάλεια και την Κυβερνοανθεκτικότητα μίας τουριστικής επιχείρησης είναι οι εξής:

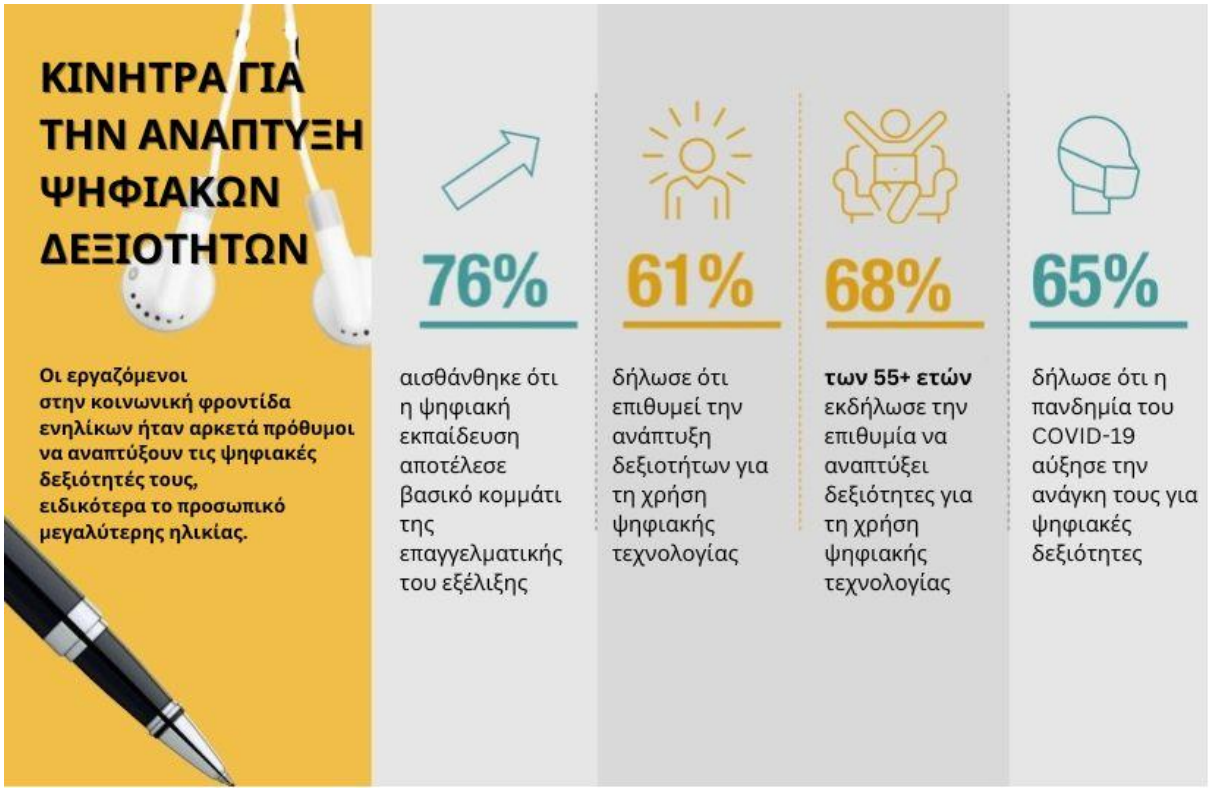
- Κακόβουλο λογισμικό (malware): πρόκειται για ένα από τα συνηθέστερα είδη κυβερνοαπειλής, το οποίο διαδίδεται ως συνημμένο αρχείο μέσω ενός ανεπιθύμητου e-mail ή με τη νομιμοφανή λήψη ενός αρχείου. Η επίθεση από malware θέτει σε κίνδυνο τα ευαίσθητα συστήματα και δεδομένα ενός οργανισμού, μολύνοντας τα με κακόβουλο λογισμικό, όπως ιούς (viruses), ιούς τύπου σκουληκιών (worms), τύπου δούρειου ίππου (trojan horses), και άλλα κατασκοπευτικά λογισμικά (spyware) (Παρασκευάς, 2020).
- Ηλεκτρονικό ψάρεμα (phishing): πρόκειται για το ανέκαθεν πιο διαδεδομένο είδος κυβερνοαπειλής και πραγματοποιείται κατά κύριο λόγο μέσω ηλεκτρονικής αλληλογραφίας, όταν οι εγκληματίες του κυβερνοχώρου αποστέλλουν στα θύματά τους e-mail, το οποίο φαίνεται να προέρχεται από κάποια νόμιμη εταιρεία (π.χ. μία τράπεζα) και ζητούν

ευαίσθητες πληροφορίες (π.χ. στοιχεία τραπεζικών λογαριασμών, κωδικούς πρόσβασης).

- Επιθέσεις στα σημεία πώλησης (POS): μία επίσης πολύ διαδεδομένη μέθοδος στον τομέα των ταξιδίων και του τουρισμού, η οποία προσφέρει στους δράστες της απειλής πολύτιμα δεδομένα, συμπεριλαμβανομένων στοιχείων πιστωτικών καρτών, όπως τον αριθμό ή τον προσωπικό κωδικό (PIN) της κάρτας.
- Επίθεση Man-in-the-middle: αυτό το είδος κυβερνοεπίθεσης λαμβάνει χώρα σε μη ασφαλή δίκτυα WiFi, όπου ο δράστης της επίθεσης μπορεί να υποκλέψει τα δεδομένα που μεταφέρονται από τη συσκευή του θύματος και από το δίκτυο.
- Λυτρισμικό (ransomware): σκοπός αυτού του είδους απειλής δεν είναι η κλοπή δεδομένων αλλά η άρνηση πρόσβασης στον ιδιοκτήτη τους, με σκοπό να τον αναγκάσει να πληρώσει άμεσα λύτρα στον δράστη της επίθεσης. Το λογισμικό ransomware είναι έτσι προγραμματισμένο ώστε να αναγνωρίζει τα πιο ευαίσθητα και πολύτιμα δεδομένα μίας επιχείρησης.
- Επιθέσεις Botnet: η χρήση εκτεταμένων δικτύων που συχνά αποτελούνται από πλήθος υπολογιστών, smartphones ή άλλων έξυπνων συσκευών (γνωστά κι ως «στρατιές ζόμπι»), με σκοπό να πραγματοποιούν κακόβουλες ενέργειες, όπως απόπειρες σύνδεσης, επιθέσεις spam, ή απόπειρες να θέσουν εκτός λειτουργίας δίκτυα, συσκευές δικτύου, ιστοσελίδες ή ολόκληρο το περιβάλλον πληροφορικής ενός οργανισμού.
- Επιθέσεις σε τρίτους παρόχους υπηρεσιών: οι δράστες των απειλών στοχεύουν επίσης κατά των ψηφιακών συνεργατών και των τρίτων παρόχων υπηρεσιών (μέλη DexteR) ενός οργανισμού, οι οποίοι συχνά θεωρούνται ο πιο αδύναμος κρίκος εντός του δικτύου και αποτελούν ελκυστικούς πόλους συγκέντρωσης ευαίσθητων δεδομένων της εταιρείας (IBM 2018, όπως αναφέρεται στο Παρασκευάς, 2020).

10.5 Καλές Πρακτικές στον Κυβερνοχώρο για τουριστικές ΜμΕ

Ένα κρίσιμο συστατικό στοιχείο της Κυβερνοασφάλειας και της Κυβερνοανθεκτικότητας είναι **η επιμόρφωση του προσωπικού για την απόκτηση ψηφιακών δεξιοτήτων**. Εργαζόμενοι, οι οποίοι έχουν εκπαιδευτεί κατάλληλα ως προς το πώς να αποφεύγουν να πέσουν θύματα κυβερνοεπιθέσεων και γνωρίζουν τι περιστατικά οφείλουν να αναφέρουν, μπορούν να ενισχύσουν το σύστημα ασφάλειας μίας τουριστικής ΜμΕ και να περιορίσουν τον κίνδυνο κυβερνοαπειλής, π.χ. τη μη εξουσιοδοτημένη πρόσβαση στα συστήματα μίας επιχείρησης στον κυβερνοχώρο.



https://www.digitalsocialcare.co.uk/digital-skills-and-training/

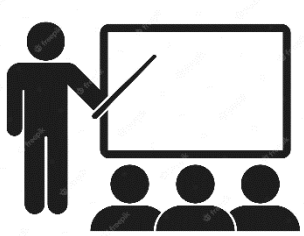
Το Παγκόσμιο Συμβούλιο Τουρισμού και Ταξιδιών (WTTC) αναγνωρίζει 7 καλές πρακτικές, οι οποίες μπορούν να εφαρμοστούν για την περαιτέρω ενίσχυση της Κυβερνοανθεκτικότητας:

1. Ένταξη της διαχείρισης των κυβερνοκινδύνων στο σχέδιο διαχείρισης κινδύνων του οργανισμού

Οι κυβερνοκίνδυνοι οφείλουν να αποτελούν προτεραιότητα, και να αντιμετωπίζονται παράλληλα με τους λοιπούς κινδύνους που αφορούν την επιχείρηση και τη λειτουργία της. Οι επιχειρήσεις οφείλουν να ελέγχουν και να αναβαθμίζουν τακτικά τις διαδικασίες διαχείρισης κινδύνου και να κατανέμουν τον προϋπολογισμό τους ανάλογα με το επίπεδο κινδύνου και τις ενέργειες μετριασμού που απαιτούνται. Οι κατάλληλα καταρτισμένοι εργαζόμενοι είναι απαραίτητοι για τον σχεδιασμό και την ενημέρωση πολιτικών για τους κινδύνους στον κυβερνοχώρο, την εφαρμογή βέλτιστων πρακτικών και την προληπτική και συνεχή διαχείριση των εν λόγω κινδύνων.

2. Εκπαίδευση και επιμόρφωση όλου του προσωπικού

Η εκπαίδευση για τον κατατοπισμό του νέου προσωπικού και η επιμόρφωση του υπάρχοντος προσωπικού είναι κρίσιμης σημασίας ούτως ώστε να διασφαλιστεί η αποτελεσματική χρήση των ψηφιακών συστημάτων και διαδικασιών, και η ασφάλεια. Αν και δεν απαιτείται να κατέχουν όλοι οι εργαζόμενοι τον ίδιο βαθμό εκπαίδευσης, είναι σημαντικό το σύνολο του προσωπικού να κατέχει βασική γνώση των αρχών της Κυβερνοασφάλειας. Αυτό μειώνει τις πιθανότητες μίας κυβερνοεπίθεσης εκ των έσω.



3. Επέκταση της προστασίας και πέραν του φυσικού χώρου εργασίας

Λόγω της μετάβασης στην εξ αποστάσεως και την υβριδική εργασία, θα πρέπει να διευρυνθεί η διενέργεια ελέγχων στον κυβερνοχώρο. Είναι εξαιρετικά σημαντικό να λαμβάνεται υπόψη το πώς τα υβριδικά μοντέλα εργασίας δύνανται να επηρεάσουν την ασφάλεια και να αυξήσουν την ευαλωτότητα ενός οργανισμού, συμπεριλαμβανομένης της ασφάλειας των οικιακών δικτύων Wi-Fi, του βαθμού κυβερνο-υγιεινής (cyber-hygiene) των εργαζομένων στις προσωπικές συσκευές τους κ.ά.

4. Υιοθέτηση της προσέγγισης μηδενικής εμπιστοσύνης στην Κυβερνοασφάλεια (Zero-Trust)

Η προσέγγιση μηδενικής εμπιστοσύνης διαφοροποιείται από τις προγενέστερες μεθόδους, οι οποίες βασίζονταν στον υψηλό βαθμό εμπιστοσύνης εντός του οργανισμού. Στηρίζεται στην ρητή επαλήθευση των αιτημάτων πρόσβασης, μειώνει τα προνόμια πρόσβασης, και αντιμετωπίζει κάθε ενέργεια ως παραβίαση ή διαρροή. Αυτό επιτρέπει μεγαλύτερη ευελιξία στην πρόσβαση, μειώνοντας παράλληλα την έκθεση των κεντρικών συστημάτων.

https://pbosecure.com/blogs/apply-zero-trust-information-security-framework-to-icsot-environment

5. Διενέργεια συνεχούς αξιολόγησης της κατάστασης απειλής

Αυτό περιλαμβάνει την ενίσχυση της ανθεκτικότητας απέναντι στις κυβερνοαπειλές με τη δημιουργία σχέσεων με τους ειδήμονες σε αυτόν τον τομέα, τη χρήση ανάλυσης δεδομένων για την βελτίωση των μέτρων προστασίας, τη διενέργεια δοκιμών διείσδυσης για τον εντοπισμό ευάλωτων σημείων, το διαχωρισμού των συστημάτων για τον περιορισμό των επιπτώσεων μίας παραβίασης, και την προτεραιοποίηση της προστασίας των συστημάτων.

https://www.clipartmax.com/middle/m2H7i8G6K9m2A0Z5_a-checklist-with-a-warning-sign-to-depict-risk-identification-risk-assessment/

6. Τήρηση διαφάνειας

Είναι ζωτικής σημασίας να γίνονται γνωστά τα μέτρα ασφαλείας που εφαρμόζονται, όπως και οι λόγοι για τη συλλογή και τη χρήση δεδομένων, και η χρονική περίοδος αποθήκευσής τους. Οι τουριστικές ΜμΕ θα πρέπει να συγκεντρώνουν τον ελάχιστο δυνατό αριθμό προσωπικών δεδομένων και στοιχειών πληρωμής που απαιτείται, και να προσφέρουν υψηλότατα επίπεδα προστασίας ώστε να δημιουργήσουν ένα κλίμα εμπιστοσύνης. Επιπλέον, θα πρέπει να δίνουν έμφαση στην συμμόρφωση με τη νομοθεσία και τα πρότυπα σε ισχύ (π.χ. GDPR). Σε περίπτωση παραβίασης, θα πρέπει να ενημερώνονται άμεσα τα θιγόμενα μέρη και οι ρυθμιστικές αρχές, και να λαμβάνονται μέτρα για τον μετριασμό των επιπτώσεων της παραβίασης.

7. Εφαρμογή ενός οργανωτικού προτύπου

Οι επικεφαλής των επιχειρήσεων θα πρέπει να συμμορφώνονται με την νομοθεσία της περιοχής στην οποία δραστηριοποιούνται. Η αποστολή της ΕΕ να καλλιεργήσει μία ενιαία προσέγγιση ως προς την Κυβερνοασφάλεια, την Κυβερνοανθεκτικότητα και την προστασία των δεδομένων οδήγησε στο να προκύψουν τα παρακάτω:

- Η Δράση της ΕΕ για την Κυβερνοανθεκτικότητα, η οποία επιδιώκει να εγκαθιδρύσει κοινούς κανόνες Κυβερνοασφάλειας για τα ψηφιακά προϊόντα και τις σχετικές υπηρεσίες που κυκλοφορούν στην ευρωπαϊκή αγορά.
- Η Δράση της ΕΕ για την Κυβερνοασφάλεια, που ισχυροποιεί τον ρόλο της ENISA και καθιερώνει ένα πλαίσιο πιστοποίησης της Κυβερνοασφάλειας για προϊόντα και υπηρεσίες.
- Το συνεχώς εξελισσόμενο τοπίο του κυβερνοχώρου κατέστησε απαραίτητη την ύπαρξη νόμων για την ενίσχυση της πολιτικής προστασίας. Αυτό το κενό ήρθε να καλύψει ο Γενικός Κανονισμός της ΕΕ για την Προστασία Δεδομένων (GDPR). Η τρέχουσα προτεραιότητα του ENISA είναι να ενθαρρύνει τη λήψη μέτρων προστασίας δεδομένων για να δείξει πώς οι τεχνολογίες στον τομέα της Κυβερνοασφάλειας μπορούν να υποστηρίξουν την υλοποίηση των αρχών προστασίας δεδομένων του GDPR (βλ. το κεφάλαιο 10.3 για τα βήματα αντιμετώπισης της παραβίασης δεδομένων).
- Στο πλαίσιο του Ευρωπαϊκού Έτους Δεξιοτήτων 2023, η Ευρωπαϊκή Επιτροπή στις 18 Απριλίου 2023 εξέδωσε ανακοίνωση σχετικά με την Ακαδημία Δεξιοτήτων για την Κυβερνοασφάλεια (Cybersecurity Skills Academy).

  Οι τουριστικές ΜμΕ θα πρέπει να λαμβάνουν υπόψη τέτοιου είδους κανονισμούς και πρωτοβουλίες πολιτικής όταν αναπτύσσουν και εφαρμόζουν ένα οργανωτικό πρότυπο, το οποίο θα πρέπει επίσης να ενημερώνεται από ειδικούς σε ζητήματα Κυβερνοασφάλειας, απορρήτου και νομικών.

Ο ENISA ανέπτυξε έναν οδηγό Κυβερνοασφάλειας για τις ΜμΕ, όπου επισημαίνονται 12 βήματα μέσω των οποίων μπορούν να θωρακιστούν οι επιχειρήσεις.

Τα βήματα είναι τα εξής:

1. Αναπτύξτε μία θετική κουλτούρα Κυβερνοασφάλειας
2. Προσφέρετε κατάλληλη και επαρκή επιμόρφωση
3. Διασφαλίστε την αποτελεσματική διαχείριση των τρίτων μερών
4. Καταρτίστε ένα σχέδιο αντιμετώπισης περιστατικών
5. Προφυλάξτε την πρόσβαση στα συστήματά σας
6. Προφυλάξτε τις συσκευές σας
7. Προφυλάξτε το δίκτυο σας
8. Βελτιώστε την υλική σας ασφάλεια
9. Προφυλάξτε τα αντίγραφα ασφαλείας σας
10. Αφιερώστε χρόνο και ασχοληθείτε με υπηρεσίες cloud
11. Προφυλάξτε τις ιστοσελίδες σας
12. Αναζητήστε και μοιραστείτε πληροφορίες

https://ecs-org.eu/enisa-introduces-the-european-cybersecurity-skills-framework/

Co-funded by the
Erasmus+ Programme
of the European Union

10.6 Επίλογος

- Η παρούσα διδακτική ενότητα εξέτασε τους τρόπους με τους οποίους η Κυβερνοασφάλεια και η Κυβερνοανθεκτικότητα διαδραματίζουν βασικό ρόλο στη λειτουργία των τουριστικών επιχειρήσεων, τα προβλήματα και τους κινδύνους που προκύπτουν από τις κυβερνοεπιθέσεις, και καλές πρακτικές πρόληψης και αντιμετώπισης.
- Οι ψηφιακές δεξιότητες μπορούν να λειτουργήσουν ως εργαλείο για τον τομέα του τουρισμού, ώστε να γίνουν καλύτερα κατανοητοί οι τρόποι που η Κυβερνοασφάλεια και η Κυβερνοανθεκτικότητα τον διαμορφώνουν και να δημιουργήσουν ένα ασφαλέστερο μέλλον.
- Η αποδοχή της ασφάλειας και της ανθεκτικότητας ως φυσικών και απαραίτητων στοιχείων για την ύπαρξη των επιχειρήσεων στον κυβερνοχώρο είναι προς το κοινό συμφέρον.

Co-funded by the
Erasmus+ Programme
of the European Union

10.7 Πρόσθετο Υλικό

Υλικό για ανάγνωση

https://link.springer.com/chapter/10.1007/978-3-319-16486-1_31
https://www.ttgmedia.com/news/news/smes-at-greatest-risk-of-cyber-attacks-says-wttc-33908

https://digitalcommons.usf.edu/m3publishing/vol17/iss9781732127593/7/

https://link.springer.com/referenceworkentry/10.1007/978-3-030-05324-6_100-1

https://securestay.medium.com/the-history-of-hotels-cyber-attacks-4b6a09c8bf30

https://www.ten-inc.com/presentations/Symantec-The-Cyber-Resilience-Blueprint.pdf

https://wttc.org/Portals/0/Documents/Reports/2022/WTTC_x_Microsoft-Codes_To_Resilience.pdf

https://idpc.org.mt/report-a-breach/

https://www.whoa.com/5-steps-to-take-after-a-small-business-data-breach/

Ιστοσελίδες

https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity

https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes/@@download/fullReport

https://www.enisa.europa.eu/topics/cybersecurity-policy/data-protection

https://www.eurotechconseil.com/en/blog/difference-between-cyber-security-and-cyber-resilience/

https://www.goallsecure.com/cyber-security-in-travel/

https://www.i-scoop.eu/cybersecurity/cyber-resilience/

https://mbb.org.mt/wp-content/uploads/2022/12/CRA-Brief-.pdf

https://www.omnicybersecurity.com/cyber-attacks-travel-tourism-industry/

https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

https://www.wcrcentre.co.uk/post/why-should-cyber-security-matter-to-an-sme-in-the-tourism-and-hospitality-industry

Βίντεο στο YouTube

https://www.youtube.com/watch?v=z5nc9MDbvkw

https://www.youtube.com/watch?v=JbEPJv7Ybcs

https://www.youtube.com/watch?v=inWWhr5tnEA