



ΕΡΓΟ RETAIL

ΠΡΟΣΘΕΤΟ ΥΛΙΚΟ

Η κυβερνοασφάλεια στη
διαδικασία της
ψηφιοποίησης

RETAIL PROJECT



Erasmus+

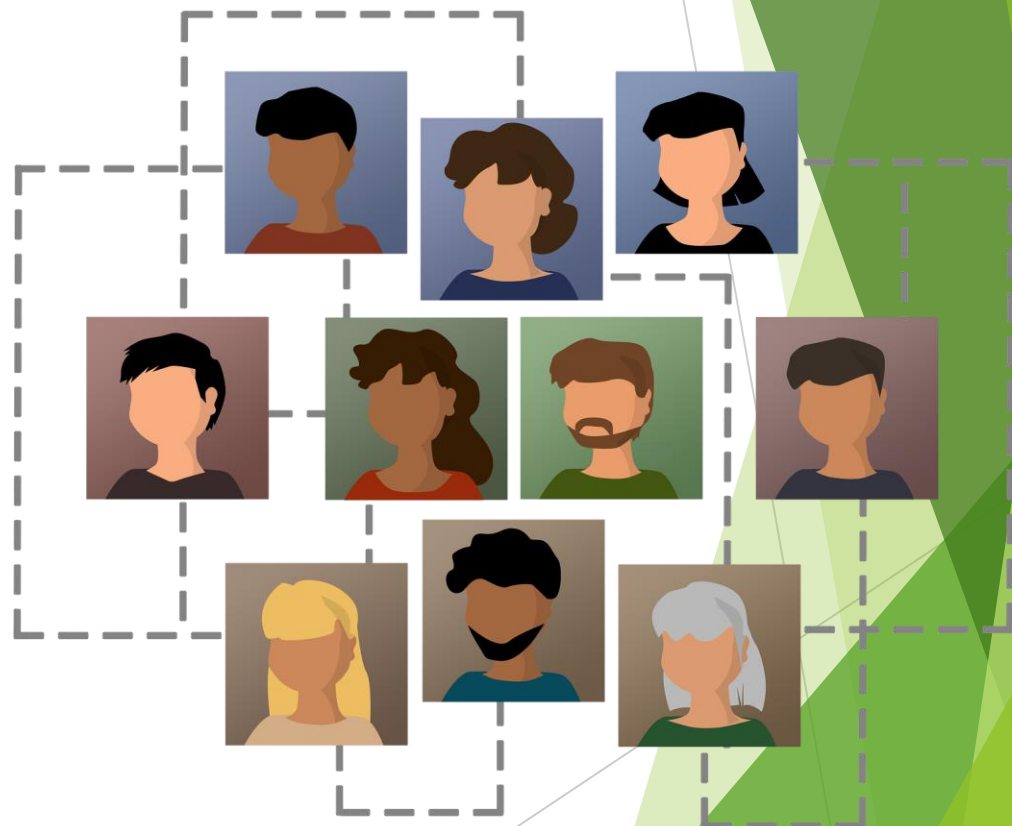
Έργο χρηματοδοτούμενο από:

**Erasmus+ / Βασική Δράση 2 -
Συνεργασία για την καινοτομία και
την ανταλλαγή καλών πρακτικών,
Στρατηγικές συμπράξεις για την
εκπαίδευση ΕΕΚ**

Έργο Retail [www: retail.erasmus.site](http://www.retail.erasmus.site)

1. Εισαγωγή στο θέμα
2. Περιεχόμενα εκμάθησης
 - Κεφάλαιο 1: Οι πιο συνηθισμένες απειλές στον κυβερνοχώρο
 - ▶ Κεφάλαιο 2: Πώς να προστατεύσετε την επιχείρησή σας;
 - Κεφάλαιο 3: Νέες τεχνολογίες και ασφάλεια στον κυβερνοχώρο
3. Πρακτική δραστηριότητα
4. Χρήσιμα εργαλεία
5. Πηγές

1. Εισαγωγή στο θέμα



Ο Covid-19 ανάγκασε πολλές εταιρείες να επιταχύνουν την μετάβασή τους στην ψηφιακή εποχή. Η ψηφιοποίηση μπορεί να υποστηρίξει τις δραστηριότητες μιας εταιρείας και να της επιτρέψει να αναπτυχθεί με πρωτοφανή τρόπο υποστηρίζοντας τις λειτουργίες της, ωστόσο, μπορεί επίσης να είναι μια πύλη για κυβερνοεπιθέσεις ή κλοπή δεδομένων. Ως εκ τούτου, είναι σημαντικό να προετοιμαστούμε για αυτά τα δεδομένα και να γνωρίζουμε πώς μπορούμε να εξασφαλίσουμε τις επιχειρήσεις μας.

Κάθε εταιρεία πρέπει φυσικά να πραγματοποιεί δράσεις προσαρμοσμένες στο προφίλ και το επίπεδο της ψηφιοποίησης, αλλά υπάρχουν μερικά κοινά σημεία που πρέπει να προσέξετε όταν εργάζεστε για να διασφαλίσετε την ασφάλεια στον κυβερνοχώρο.

2. Περιεχόμενα

Αυτή η πρόσθετη ενότητα αποτελείται από 3 κεφάλαια, μια Πρακτική δραστηριότητα, αναφορές και περαιτέρω εργαλεία.

- Κεφάλαιο 1: Οι πιο συχνές απειλές στον κυβερνοχώρο
- Κεφάλαιο 2: Πώς να προστατεύσετε την επιχείρησή σας;
- Κεφάλαιο 3: Νέες τεχνολογίες και ασφάλεια στον κυβερνοχώρο



2.1. Οι πιο συνηθισμένες απειλές στον κυβερνοχώρο



ΠΕΡΙΕΧΟΜΕΝΟ ΚΕΦΑΛΑΙΟΥ 1
Οι πιο συνηθισμένες απειλές στον κυβερνοχώρο

1. Κακόβουλο λογισμικό- Malware

Το Malware είναι συντομογραφία για "κακόβουλο λογισμικό" και μπορεί να είναι ένα τμήμα κώδικα / προγράμματος του οποίου ο σκοπός είναι να διαταράξει τις λειτουργίες, να κλέψει δεδομένα ή να βλάψει το υλικό. Αυτά περιλαμβάνουν δημοφιλή trojans, worms και spyware.

2. Ψάρεμα- Phishing

Αυτό υποδύεται ένα άτομο ή ίδρυμα και επιχειρεί να εκβιάσει χρήματα / δεδομένα από τον χρήστη

3. Man-in-the-Middle

Ένας χάκερ «μπαίνει» μεταξύ των αλληλεπιδράσεων 2 οντοτήτων μέσω, για παράδειγμα, κακής ασφάλειας Wi-Fi με σκοπό την κλοπή πληροφοριών, προσωπικών δεδομένων κ.λπ.

2.2.1. Πώς να Προστατέψετε την επιχείρησή σας;

Βασικά, υπάρχουν δύο βασικά στοιχεία που πρέπει να προσέξετε

Ανθρώπινο δυναμικό



Οι στατιστικές δείχνουν ότι η συντριπτική πλειοψηφία των απειλών στον κυβερνοχώρο οφείλεται σε κακή εκπαίδευση των εργαζομένων και ανθρώπινο λάθος.

ΠΕΡΙΕΧΟΜΕΝΟ ΚΕΦΑΛΑΙΟΥ 2

Πώς να Προστατέψετε την επιχείρησή σας;

Ανθρώπινο δυναμικό και ασφάλεια στον κυβερνοχώρο

Πόροι υλικού και ασφάλεια στον κυβερνοχώρο

Προστασία Προσωπικών δεδομένων

Πόροι υλικού



Αυτό περιλαμβάνει όλους τους υπολογιστές, φορητούς υπολογιστές, λογισμικό, προγράμματα προστασίας από ιούς και πιθανές πύλες που χρησιμοποιούνται για επιθέσεις από χάκερ.

2.2.2.

Ανθρώπινο δυναμικό και ασφάλεια στον κυβερνοχώρο

Οι άνθρωποι πόροι διαδραματίζουν κρίσιμο ρόλο στη διασφάλιση της ασφάλειας στον κυβερνοχώρο

Εκτιμάται ότι έως και το 90% των προβλημάτων ασφάλειας στον κυβερνοχώρο σχετίζονται με ανθρώπινο λάθος. Οι απειλές ασφαλείας μπορούν να εκδηλωθούν σε μια ποικιλία (δυννητικά επικίνδυνων) συμπεριφορών, όπως: σύνδεση εξωτερικών συσκευών (όπως μονάδες USB) που ενδέχεται να φέρουν επικίνδυνο κακόβουλο λογισμικό ή να ανοίγουν μηνύματα ηλεκτρονικού ταχυδρομείου που προέρχονται από άγνωστες πηγές. Υπάρχουν πολλές επικίνδυνες πρακτικές, αλλά η πιο κοινή πηγή του προβλήματος είναι τα κενά στην εκπαίδευση των εργαζομένων σχετικά με την ασφάλεια στον κυβερνοχώρο.

- Για να αντιμετωπιστεί αυτό στις ΜΜΕ, συνιστάται να:
- Δημιουργήσετε ένα σχέδιο πολιτικών, διαδικασιών και αντιμέτρων ασφαλείας.
- Βεβαιωθείτε ότι υπάρχουν επαγγελματικές εκπαιδεύσεις εργαζομένων στο χώρο εργασίας με επιδείξεις των διαφόρων επικίνδυνων συμπεριφορών που πρέπει να αποφεύγονται

ΠΕΡΙΕΧΟΜΕΝΟ ΚΕΦΑΛΑΙΟΥ 2

Πώς να προστατέψετε την επιχείρησή σας;

Ανθρώπινο δυναμικό και ασφάλεια στον κυβερνοχώρο

Πόροι υλικού και ασφάλεια στον κυβερνοχώρο

Προστασία προσωπικών δεδομένων

2.2.3.

Πόροι υλικού και ασφάλεια στον κυβερνοχώρο

Οι πόροι υλικού πρέπει να εξασφαλίζονται σωστά για την προστασία των δεδομένων που συλλέγονται από την εταιρεία

Είναι πολύ σημαντικό να διασφαλίσετε ότι ο εξοπλισμός σας προστατεύεται σωστά από πιθανές επιθέσεις στον κυβερνοχώρο.

Για το σκοπό αυτό διατίθενται διάφορα εργαλεία.

Η πιο προφανής προστασία είναι να έχετε λογισμικό προστασίας από ιούς. Μπορείτε να βρείτε μια λίστα παραδειγμάτων εδώ: <https://www.usnews.com/360-reviews/antivirus>

Τα τείχη προστασίας είναι επίσης αναγκαία. Αν και η αποτελεσματικότητά τους δεν είναι τόσο υψηλή όσο ήταν κάποτε και ένας εξειδικευμένος χάκερ μπορεί να τα παρακάμψει, εξακολουθούν να είναι η πρώτη γραμμή άμυνας και μπορούν να αποτρέψουν την μη εξουσιοδοτημένη είσοδο στο σύστημα.

Εάν αποφασίσετε να κάνετε συναλλαγές στο διαδίκτυο, αυτό φυσικά ανοίγει ένα εντελώς νέο σύνολο προκλήσεων ασφάλειας (ειδικά για τους πελάτες). Θα πρέπει να ξεκινήσετε διασφαλίζοντας ότι το κατάστημά σας είναι σωστά ασφαλισμένο με SSL και TLS (η τεχνολογία που είναι υπεύθυνη για την κρυπτογράφηση και το HTTPS - το δημοφιλές λουκέτο δίπλα στη διεύθυνση του ιστότοπου).

ΠΕΡΙΕΧΟΜΕΝΟ ΚΕΦΑΛΑΙΟΥ 2

Πώς να προστατέψετε την επιχείρησή σας;

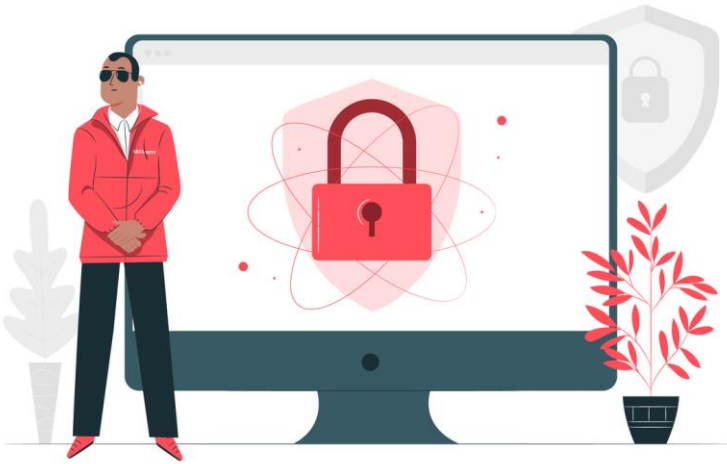
Ανθρώπινο δυναμικό και ασφάλεια στον κυβερνοχώρο

Πόροι υλικού και ασφάλεια στον κυβερνοχώρο

Προστασία προσωπικών δεδομένων

2.2.4. Προστασία Προσωπικών δεδομένων

Η φροντίδα για την ασφάλεια στον κυβερνοχώρο αφορά επίσης τη φροντίδα των δεδομένων και των πληροφοριών που αποθηκεύετε, συμπεριλαμβανομένων των προσωπικών πληροφοριών των πελατών και των υπαλλήλων σας.



ΠΕΡΙΕΧΟΜΕΝΟ ΚΕΦΑΛΑΙΟΥ 2

Πώς να προστατέψετε την επιχείρησή σας;
Ανθρώπινο δυναμικό και ασφάλεια στον κυβερνοχώρο

Πόροι υλικού και ασφάλεια στον κυβερνοχώρο

Προστασία προσωπικών δεδομένων

Ο Γενικός Κανονισμός Προσωπικών Δεδομένων (GDPR) ισχύει στην Ευρωπαϊκή Ένωση από το 2018 (ολόκληρος ο κανονισμός διατίθεται [εδώ](#)). Αυτό σημαίνει ότι η αποθήκευση δεδομένων πρέπει να συμμορφώνεται με ορισμένα μέτρα προστασίας.

Ο GDPR εισήγαγε νέα δικαιώματα για τους πολίτες (για παράδειγμα, το «δικαίωμα να ξεχνιούνται») και νέες υποχρεώσεις για τις επιχειρήσεις τόσο στις φυσικές όσο και στις διαδικτυακές τους δραστηριότητες. Μεταξύ αυτών των υποχρεώσεων είναι, για παράδειγμα, η υποχρέωση εισαγωγής αρχών απορρήτου στο στάδιο του σχεδιασμού (για παράδειγμα, ενός καταστήματος). Αυτές είναι: προστασία της ιδιωτικής ζωής βάσει σχεδίου ή απορρήτου από προεπιλογή.

2.3. Νέες τεχνολογίες και ασφάλεια στον κυβερνοχώρο



ΠΕΡΙΕΧΟΜΕΝΟ ΚΕΦΑΛΑΙΟΥ 3

Νέες τεχνολογίες και ασφάλεια στον κυβερνοχώρο

Η τέταρτη βιομηχανική επανάσταση (Βιομηχανία 4.0) οδηγεί τις επιχειρήσεις σε μια νέα εποχή συνδεδεμένων συσκευών. Ενώ τα θετικά της είναι πολλά, φέρνει επίσης ορισμένους κινδύνους. Ένα από αυτά συνδέεται με το Διαδίκτυο των Πραγμάτων, το οποίο, με απλά λόγια, περιλαμβάνει τη σύνδεση πολλών συσκευών που μπορούν να αλληλεπιδράσουν χωρίς ανθρώπινη συμμετοχή. Αυτό εγκυμονεί τον κίνδυνο ένας τόσο μεγάλος αριθμός συνδεδεμένων συσκευών (εκτιμάται ότι θα υπάρχουν έως και 25,4 δισεκατομμύρια συσκευές IoT το 2030) να αποτελέσει μια πύλη εισόδου για χάκερ που, διερχόμενοι στις λιγότερο ασφαλείς συσκευές, θα είναι σε θέση να πρόσβαση στα σημαντικότερα στοιχεία της υποδομής των εταιρειών.

3. Πρακτική Δραστηριότητα

Για να εξασκηθείτε, σκεφτείτε το επίπεδο ασφάλειας στον κυβερνοχώρο στην εταιρεία σας.



1. Τι εκπαίδευση παρέχετε στους υπαλλήλους σας;
2. Πώς μπορείτε να βελτιώσετε τις δικές σας ικανότητες για την ασφάλεια στον κυβερνοχώρο;
3. Είναι απόλυτα προστατευμένα τα δεδομένα των πελατών σας;
4. Χρησιμοποιείτε ενημερωμένο λογισμικό προστασίας από ιούς;
5. Έχετε σχέδιο σε περίπτωση που συμβεί κυβερνοεπίθεση;

4. Χρήσιμα εργαλεία



GDPR

Σύνδεσμος: <https://gdpr-info.eu/>

Βίντεο σχετικά με την ασφάλεια στον κυβερνοχώρο

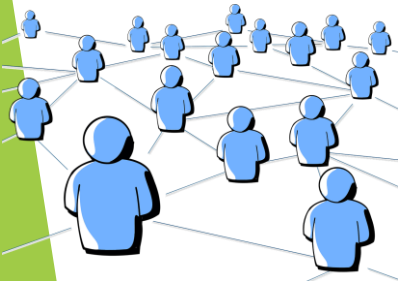
Σύνδεσμος :

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



Κυβερνοασφάλεια για μικρές επιχειρήσεις

Σύνδεσμος : <https://www.fcc.gov/general/cybersecurity-small-business>



5. Πηγές

Cybersecurity 101: Εισαγωγή στους κορυφαίους 10 κοινούς τύπους επιθέσεων στον κυβερνοχώρο::

Σύνδεσμος:

<https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/>

Γιατί η εκπαίδευση των υπαλλήλων σας σχετικά με την ευφυΐα στον κυβερνοχώρο και την ασφάλεια θα μειώσει τον κίνδυνο:

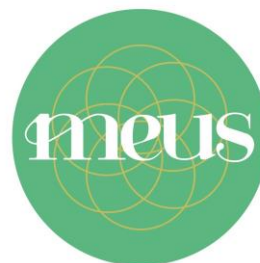
Σύνδεσμος: <https://www.cybintsolutions.com/employee-education-reduces-risk/>

Τι είναι το GDPR (πολωνικά)

Σύνδεσμος: <https://www.politykabezpieczenstwa.pl/pl/a/czym-jest-rodo-i-jakie-zmiany-wprowadza-nowa-ustawa-parlamentu-europejskiego>



Σύμπραξη έργου RETAIL



POLISH CHAMBER OF COMMERCE

Έργο Retail [www: retail.erasmus.site](http://www.retail.erasmus.site)

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν αποτελεί έγκριση του περιεχομένου, το οποίο αντικατοπτρίζει τις απόψεις μόνο των συγγραφέων και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.