DIMELI4AC

ΨΗΦΙΑΚΟΣ ΓΡΑΜΜΑΤΙΣΜΟΣ ΚΑΙ ΓΡΑΜΜΑΤΙΣΜΟΣ ΜΕΣΩΝ ΓΙΑ ΜΙΑ ΕΝΕΡΓΗ ΑΓΩΓΗ ΤΟΥ ΠΟΛΙΤΗ: Ένα σύνολο εργαλείων για την προώθηση της κριτικής σκέψης και των δημοκρατικών αξιών

ΕΝΟΤΗΤΑ 1: ΔΙΑΔΙΚΤΥΑΚΗ ΑΣΦΑΛΕΙΑ

Θέμα 2: Κακόβουλο Λογισμικό

Erasmus+

Περιγραφή Ενότητας

Το διαδίκτυο προσφέρει πληθώρα οφελών και είναι εντελώς απίθανο να αποφύγεις την παρουσία του. Ωστόσο, παρά τα οφέλη που παρέχει, μπορεί επίσης να φέρει και μια πλειάδα κινδύνων, οπότε ο καθένας μας πρέπει να τους αναγνωρίζει και να μαθαίνει τις γενικές πρακτικές ασφάλειας, σε σχέση με τη Διαδικτυακή Ασφάλεια, τα Κακόβουλα Λογισμικά και τις προσπάθειες για υποκλοπή προσωπικών δεδομένων, το λεγόμενο Phishing.

Θέματα

Αυτή η ενότητα θα καλύψει τα ακόλουθα θέματα:

- Ασφάλεια στον Κυβερνοχώρο
- Κακόβουλο Λογισμικό
- Υποκλοπή Προσωπικών Δεδομένων (Phishing)

Μαθησιακά Αποτελέσματα

Σε αυτή την ενότητα, θα μάθεις να:

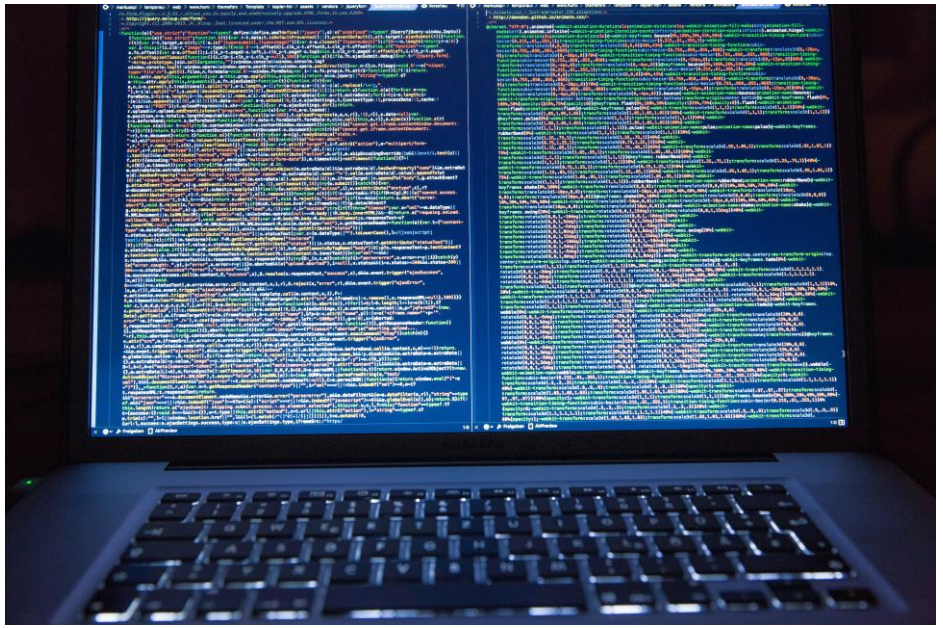
- Προστατεύεις τον εαυτό σου στο διαδίκτυο, γνωρίζοντας τις βασικές πρακτικές, οι οποίες είναι σημαντικές, ώστε να βεβαιωθείς, πως δεν πέφτεις θύμα διαδικτυακών επιθέσεων.
- Γνωρίζεις πώς να προστατεύεις τον εαυτό σου από κακόβουλα λογισμικά, τα οποία μπορούν να θέσουν σε κίνδυνο προσωπικές σου πληροφορίες.
- Χρησιμοποιείς μέσα κοινωνικής δικτύωσης με έναν ασφαλή και συνειδητό τρόπο, για να προστατεύεις τις προσωπικές σου πληροφορίες από το να χρησιμοποιηθούν στο διαδίκτυο με δόλιο τρόπο.

Υπόμνημα

	Λέξεις κλειδιά
	Σενάρια
	Συμβουλές
	Ερωτήσεις
	Δραστηριότητες
	Πηγές

Θέμα 2

Κακόβουλο Λογισμικό



Θέμα 2 – Τι σημαίνει Κακόβουλο Λογισμικό? (1/3)

Κακόβουλο Λογισμικό είναι κάθε **λογισμικό**, το οποίο αποσκοπεί να καταστρέψει ή να προκαλέσει ζημιά σε υπολογιστές και υπολογιστικά συστήματα εν αγνοία του ιδιοκτήτη.

Ο όρος Malware είναι σύντομη μορφή του "malicious software" ("κακόβουλο λογισμικό") και χαρακτηρίζεται **από την πρόθεση του δημιουργού του να βλάψει κάποιον άλλο με κακόβουλο περιεχόμενο,** δρώντας ενάντια στο συμφέρον του ιδιοκτήτη του υπολογιστή.

Θέμα 2 – Τι σημαίνει Κακόβουλο Λογισμικό? (2/3)

Υπάρχουν πολλοί τύποι κακόβουλου λογισμικού, οι οποίοι σχεδιάζονται για να μολύνουν τον Η/Υ ενός χρήστη και να προκαλέσουν βλάβη σε αυτόν. Οι επιθέσεις κακόβουλου λογισμικού αποτελούν μια συνεχή ανησυχία στον κόσμο των υπολογιστών και αναπτύσσονται σε συχνότητα και πολυπλοκότητα, αφήνοντας τις επιχειρήσεις και τα άτομα ανίκανους να προστατευτούν απέναντί τους.

Οι πιο σοβαρές επιθέσεις κακόβουλου λογισμικού συνδυάζουν **επιδεξιότητα, ακρίβεια** και τεχνικές **κοινωνικής μηχανικής**, για να διαπεράσουν και να θέσουν σε κίνδυνο συστήματα. Το κακόβουλο λογισμικό σχεδιάζεται σήμερα κατά κύριο λόγο από επαγγελματίες εγκληματίες.

Θέμα 2 – Τι σημαίνει Κακόβουλο Λογισμικό? (3/3)

Το κακόβουλο λογισμικό είναι ένας από τους πιο κοινούς τρόπους, για να καταστραφεί η συσκευή σου. Το **κακόβουλο λογισμικό μπορεί να:**

- Μεταβάλλει ή να διαγράψει αρχεία.
- Κλέψει ευαίσθητες πληροφορίες.
- Στείλει εκ μέρους σου emails.
- Πάρει τον έλεγχο του υπολογιστή σου και όλου του λογισμικού που τρέχει πάνω σε αυτόν.

Θέμα 2 – Κατηγοριοποίηση Κακόβουλου Λογισμικού

Το κακόβουλο λογισμικό χωρίζεται συνήθως σε κατηγορίες – αυτό εξαρτάται από τον τρόπο με τον οποίο εισάγεται στο σύστημα που γίνεται στόχος και από το είδος της παραβίασης πολιτικής που αποσκοπεί να προκαλέσει.

Η παραδοσιακή κατηγοριοποίηση έγινε από τον Peter Denning στα τέλη του 1980.

Εδώ δίνονται μερικοί γενικοί ορισμοί των τύπων κακόβολου λογισμικού:

Virus	Worms	Trojan Horse	Logic Bomb
Rabbit	Backdoor	Rootkit	Spyware

Θέμα 2 – Τύποι Κακόβουλου Λογισμικού (1/3)

Κακόβουλο Λογισμικό, το οποίο διαδίδεται από υπολογιστή σε υπολογιστή, ενσωματώνοντας αντίγραφα του εαυτού του σε αρχεία. Μπορεί να ληφθεί μέσω συνημμένου αρχείου σε κάποιο e-mail ή να βασιστεί για παράδειγμα σε ένα CD-ROM που περιλαμβάνει το αρχείο.

Κακόβουλο Λογισμικό με ανεξάρτητη δομή που διανέμεται από τον ένα υπολογιστή στον άλλο, αναπαράγοντας αυτόματα αντίγραφα του εαυτού του μέσω ενός δικτύου, χωρίς τη χρήση μολυσμένων αρχείων ή ανθρώπινης δράσης.

Αυτό που ξεχωρίζει το worm (σκουλήκι) από τον virus (ιό) είναι: η ικανότητά του να αναπαράγει αντίγραφα του εαυτού του αυτόματα, χωρίς κάποια ανθρώπινη δράση. Σε αντίθεση με τους ιούς, τα worms δε χρειάζεται να τοποθετηθούν σε ένα υπάρχον πρόγραμμα.

Θέμα 2 – Τύποι Κακόβουλου Λογισμικού (2/3)

TROJAN HORSE Δούρειος Ίππος

Τύπος Κακόβουλου Λογισμικού συνήθως μεταμφιεσμένος ως νόμιμο λογισμικό. Τα Trojans μπορούν να χρησιμοποιηθούν από κλέφτες του κυβερνοχώρου και hackers που προσπαθούν να αποκτήσουν πρόσβαση στο σύστημα του χρήστη. Τα Trojans μπορούν να επιτρέψουν σε ηλεκτρονικούς εγκληματίες να σε κατασκοπεύσουν, να κλέψουν ευαίσθητα δεδομένα και να αποκτήσουν πρόσβαση από την ‘’πίσω πόρτα’’ στο σύστημά σου.

LOGIC BOMB

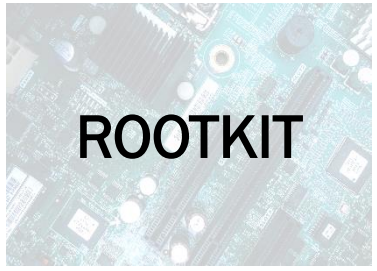
Κακόβουλο Λογισμικό που ενεργοποιείται από κάποιο εξωτερικό γεγονός, όπως η άφιξη συγκεκριμένης ημερομηνίας ή ώρας ή η δημιουργία ή διαγραφή συγκεκριμένου αντικειμένου δεδομένων, όπως ένα αρχείο ή μια καταχώρηση βάσης δεδομένων.

RABBIT

Κακόβουλο Λογισμικό που παίρνει τον έλεγχο όλου του χώρου των αρχείων σου και των διαδικασιών ελέγχου μιας πηγής σε ένα σύστημα Η/Υ, αρνούμενο την πρόσβαση στα αρχεία και τα δεδομένα σου, μέχρι να ικανοποιηθούν κάποιες απαιτήσεις.

Θέμα 2 – Τύποι Κακόβουλου Λογισμικού (3/3)

Κακόβουλο Λογισμικό, το οποίο μόλις φτάσει το στόχο, επιτρέπει την απόκτηση πρόσβασης στο σύστημα, χωρίς να περάσει από τις συνήθεις διαδικασίες σύνδεσης και επαλήθευσης ταυτότητας.



Αυτοματοποιημένο Λογισμικό πακέτο, το οποίο μπορεί να χρησιμοποιηθεί από κάποιον hacker, για να αποκτηθούν προνόμια διαχειριστή σε έναν Η/Υ ή σε ένα δίκτυο Η/Υ.

Λογισμικό, το οποίο εισβάλλει σε μηχανές και στέλνει κρυφά προσωπικές πληροφορίες σε κάποιον τρίτο, συμπεριλαμβανομένης της κλοπής της ταυτότητάς σου και των κωδικών σου, όπως επίσης και άλλων κρίσιμων και προσωπικών δεδομένων.

Θέμα 2 – Προστασία & Πρόληψη (1/2)

Μία από τις πιο γνωστές μορφές εξάπλωσης κακόβουλου λογισμικού είναι αυτή μέσω ηλεκτρονικής αλληλογραφίας. Αυτό γίνεται επειδή το κακόβουλο λογισμικό, μπορεί να ‘’μεταμφιέζεται’’, ώστε να μοιάζει με ένα e-mail που στάλθηκε από κάποια επιχείρηση, ένα σχολείο ή έναν προσωπικό φίλο.

Ένα ισχυρό πακέτο αντιιικού λογισμικού (antivirus) είναι το πρωταρχικό συστατικό τεχνολογικής άμυνας, που κάθε σύστημα προσωπικού ηλεκτρονικού υπολογιστή και κάθε συσκευή πρέπει να διαθέτει. Επιπλέον (1/2):

- **Απόφυγε ύποπτους συνδέσμους και emails**: όταν λαμβάνεις φαινομενικά ύποπτους συνδέσμους και emails, απόφυγέ τα ή διάγραψέ τα, ακόμα και αν προέρχονται από το σχολείο ή από κάποιο φίλο.
- **Απόφυγε ύποπτες ιστοσελίδες**: αν παρατηρήσεις κάτι ασυνήθιστο, όταν επισκέπτεσαι μια ιστοσελίδα, προφυλάξου και μην αποκαλύψεις προσωπικές πληροφορίες.
- **Κάνε προσεκτική επιθεώρηση του λογισμικού πριν το κατεβάσεις**: πριν εγκαταστήσεις οτιδήποτε στον Η/Υ σου ή σε κάποια συσκευή, ψάξε το πρόγραμμα και τις κριτικές του.

Θέμα 2 – Προστασία & Πρόληψη (2/2)

Επιπλέον (2/2):

- **Εγκατάστησε κάποιο αντιικό λογισμικό (antivirus)**: τα αναπτυγμένα προγράμματα anti-virus θα κρατήσουν τη συσκευή σου προστατευμένη από κοινά κακόβουλα λογισμικά και άλλους διαδικτυακούς κινδύνους. Θα σε κρατήσουν ασφαλή απέναντι σε γνωστές επιθέσεις κακόβουλου λογισμικού.
- **Ενεργοποίησε το τείχος προστασίας σου (firewall)**: πρέπει να διασφαλίσεις ότι είναι σωστά εγκαταστημένο και ενεργοποιημένο πάντα.
- **Δημιούργησε ισχυρούς και μοναδικούς κωδικούς:** πολλοί άνθρωποι συνεχίζουν να χρησιμοποιούν εύκολα προβλέψιμους κωδικούς, ή τον ίδιο κωδικό σε όλους τους λογαριασμούς τους. Είναι σημαντικό ο καθένας να δημιουργεί έναν ασφαλή/ μοναδικό κωδικό για κάθε λογαριασμό
- **Διασφάλισε πως είναι εγκαταστημένες όλες οι ενημερώσεις ασφαλείας**: εγκατάστησε ενημερώσεις ασφαλείας για να προστατευτείς από το κακόβουλο λογισμικό.

Περίληψη

- Πρόσεξε το Κακόβουλο Λογισμικό. Το κακόβουλο λογισμικό είναι ένα επαναλαμβανόμενο πρόβλημα στη ζωή μας, με την συνεχώς αυξανόμενη παρουσία του στο διαδίκτυο. Κακόβουλο λογισμικό μπορεί να εξαπλωθεί μέσα από μια σειρά μέσων, από USB drive, μέχρι κατέβασμα, ιστοσελίδες κ.τ.λ.
- Υπάρχουν πολλοί τρόποι διασφάλισης της διαδικτυακής ασφάλειας. Αυτές οι συμβουλές και η υιοθέτησή τους, μπορούν να βοηθήσουν κάποιον να προστατέψει τον Η/Υ του, τα προσωπικά δεδομένα και δίκτυα απέναντι σε κινδύνους κακόβουλου λογισμικού.

Παραπομπές

- Sharp, R. (2007). An Introduction to Malware. Retrieved from: http://orbit.dtu.dk/files/4918204/malware.pdf
- Rouhani Zeidanloo, Hossein & Tabatabaei, Farzaneh & Vahdani Amoli, Payam & Tajpour, Atefeh. (2010). All About Malwares (Malicious Codes). Retrieved from: https://pdfs.semanticscholar.org/a45e/50583a13e04b920f6ba04473612734967aa7.pdf
- What is Malware? A Definition & Tips for Malware Prevention. (2018, September 11). Retrieved from https://digitalguardian.com/blog/what-malware-definition-tips-malware-prevention
- (n.d.). Retrieved from https://www.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it
- (n.d.). Retrieved from https://www.kaspersky.com/resource-center/threats/malware-creators

Επιπρόσθετες Πηγές

- What's the difference between viruses and malware?
  - https://www.youtube.com/watch?v=fKxuKWsA_JI
- Six simple Cybersecurity rules for all ages:
  - https://www.kaspersky.com/blog/tips-for-kids-all-episodes/9693/

Κοινοπραξία

Leibniz Universität Hannover

Institut für Didaktik der Demokratie

LIFELONG LEARNING PLATFORM
EUROPEAN CIVIL SOCIETY FOR EDUCATION

ANT1

CCS
Digital Education

Emphasys CENTRE

ELLINOGERMANIKI AGOGI

Αυτό το πρότζεκτ χρηματοδοτήθηκε με την υποστήριξη της Ευρωπαϊκής Επιτροπής. Το πρότζεκτ αντικατοπτρίζει μόνο τις απόψεις του συντάκτη του και η Επιτροπή δεν έχει κανένα μερίδιο ευθύνης για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτό.
Αριθμός Υποβολής: 2018-1-DE03-KA201-047411