

Κυβερνοασφάλεια στην Δημόσια Διοίκηση

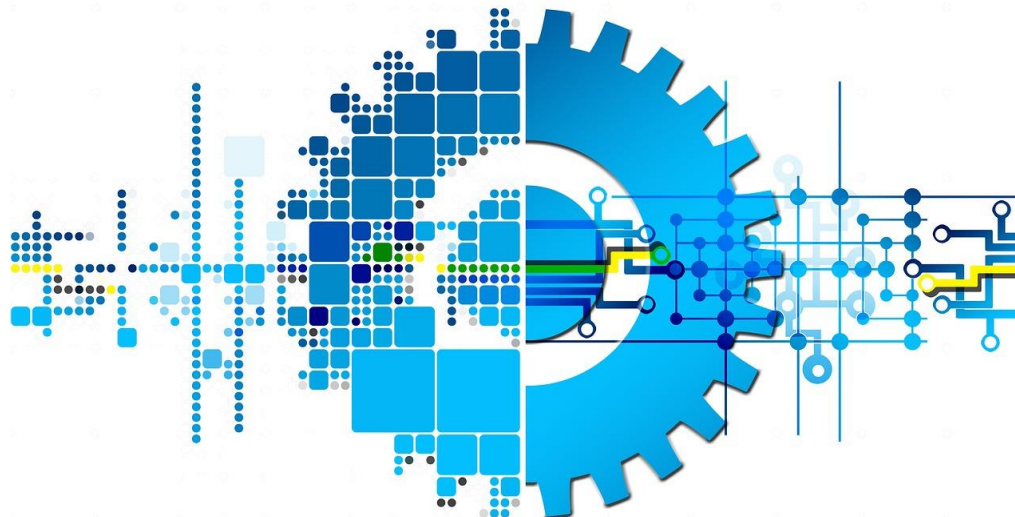
ΕΘΝΙΚΗ ΣΧΟΛΗ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΣΥΝΤΟΝΙΣΤΡΙΑ:

ΑΝΑΣΤΑΣΙΑ ΠΑΠΑΣΤΥΛΙΑΝΟΥ

ΕΙΣΗΓΗΤΗΣ:

ΑΝΑΣΤΑΣΙΟΣ ΠΑΠΑΘΑΝΑΣΙΟΥ



ΚΖ' ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ «ΔΗΜΗΤΡΙΟΣ ΤΖΑΝΑΚΗΣ»

Α' ΕΙΔΙΚΗ ΦΑΣΗ

ΑΘΗΝΑ 2021

6 – Ασφάλεια Κοινωνικών Δικτύων

Εθνική Σχολή Δημόσιας Διοίκησης & Αυτοδιοίκησης
Ιούνιος 2021

Ενότητες

- ▶ Κίνδυνοι ασφάλειας και ιδιωτικότητας στις εφαρμογές κοινωνικής δικτύωσης
- ▶ Η περίπτωση του Facebook
- ▶ Η περίπτωση του Twitter
- ▶ Ορθή Χρήση Μέσων Κοινωνικής Δικτύωσης

Ασφάλεια Κοινωνικών Δικτύων

- Ο όγκος των προσωπικών δεδομένων που διακινούνται καθημερινά μέσα από μία **Εφαρμογή Κοινωνικής Δικτύωσης (ΕΚΔ)** είναι εντυπωσιακά μεγάλος
- Λαμβάνοντας υπόψη ότι ένας χρήστης χρησιμοποιεί πολλαπλές εφαρμογές κοινωνικής δικτύωσης διευρύνονται ακόμα περισσότερο τα **όρια έκθεσης της ιδιωτικής ζωής** του ατόμου

Ασφάλεια Κοινωνικών Δικτύων

- Οι πάροχοι σχεδιάζουν τις εφαρμογές τους έτσι ώστε να **ενθαρρύνουν** συμπεριφορές που αυξάνουν τον αριθμό των χρηστών και των μεταξύ τους συνδέσεων
- Οι χρήστες γίνονται πιο **δεκτικοί** στα «αιτήματα φιλίας» που λαμβάνουν χωρίς να συνειδητοποιούν το μέγεθος ή το είδος του κοινού το οποίο έχει πρόσβαση στα δεδομένα του προφίλ τους

Ασφάλεια Κοινωνικών Δικτύων

- Η κοινωνική δικτύωση, είναι μια μορφή συγκέντρωσης ατόμων σε «**κοινότητες**» με στόχο την διαμόρφωση κοινωνικών σχέσεων
- Τα κοινωνικά δίκτυα στο Διαδίκτυο, είναι άτυπα **εργαλεία διαχείρισης ταυτότητας** που υποστηρίζουν την κοινωνική δικτύωση και χαρακτηρίζονται από ευκολία στη χρήση, διευκολύνουν τη δημιουργία αυθόρμητων σχέσεων, διευρύνουν την αλληλεπίδραση και την επικοινωνία μεταξύ των χρηστών τους

Εμπλεκόμενοι/ οντότητες στις ΕΚΔ

Πάροχοι Υπηρεσιών Κοινωνικής Δικτύωσης

- Προσφέρουν τα μέσα και τις δυνατότητες για την επεξεργασία των δεδομένων των χρηστών

Χρήστες

- Χρησιμοποιούν τις υπηρεσίες και αλληλεπιδρούν με τους άλλους χρήστες

Τρίτες Οντότητες

- Μπορεί να είναι πάροχοι εφαρμογών, άλλων υπηρεσιών κ.ά.

Κίνδυνοι Ασφάλειας & Ιδιωτικότητας

**Υπάρχουν κίνδυνοι που
ελλοχεύουν στις Εφαρμογές
Κοινωνικής Δικτύωσης;**

Κίνδυνοι Ασφάλειας & Ιδιωτικότητας

Κλοπή Ταυτότητας

- Πρόκειται για την περίπτωση όπου κάποιος χρήστης των ΕΚΔ παριστάνει ψευδεπίγραφα κάποιον άλλον χρήστη και μπορεί να εκδηλωθεί με:
 - α) την κλοπή της γνήσιας διαδικτυακής ταυτότητας (προφίλ)
 - β) τη δημιουργία ενός νέου προφίλ που θα περιλαμβάνει, αυθαίρετα, προσωπικά δεδομένα χρήστη εν αγνοία του (π.χ. ονοματεπώνυμο ή φωτογραφίες)

Κίνδυνοι Ασφάλειας & Ιδιωτικότητας

Έκθεση μεγάλου αριθμού προσωπικών δεδομένων και χρήση της πληροφορίας για άλλο σκοπό

- Στις ΕΚΔ ο χρήστης εκθέτει, καταχωρεί και δημοσιεύει μεγάλο αριθμό προσωπικών του στοιχείων, ενώ παράλληλα έχει λανθασμένη αίσθηση ότι οι πληροφορίες που ανεβάζει είναι διαθέσιμες μόνο στους φίλους του

Κίνδυνοι Ασφάλειας & Ιδιωτικότητας

Παρενόχληση – Stalking – Cyberbullying

- Όταν οι χρήστες των ΕΚΔ δημοσιοποιούν προσωπικές πληροφορίες (π.χ. αριθμό τηλεφώνου, διεύθυνση οικίας κ.ά.) μπορούν να χρησιμοποιηθούν από κακόβουλους χρήστες, για διαδικτυακή παρακολούθηση, παρενόχληση, ηλεκτρονικό εκφοβισμό (Cyberbullying)

Κίνδυνοι Ασφάλειας & Ιδιωτικότητας

Εντοπισμός – Προσδιορισμός θέσης

- Πολλοί χρήστες επιλέγουν να δημοσιεύσουν στις ΕΚΔ το που βρίσκονται κάθε στιγμή, συνειδητά ή αυτόματα, με χρήση κατάλληλων εφαρμογών
- Η πληροφορία αυτή μπορεί να χρησιμοποιηθεί από χρήστες με κακόβουλους σκοπούς (π.χ. διαρρήκτες) και να δημιουργηθεί κίνδυνος για την φυσική ασφάλεια του χρήστη

Κίνδυνοι Ασφάλειας & Ιδιωτικότητας

Δημοσιοποίηση προσωπικών δεδομένων από τρίτους

- Όσο προσεκτικός είναι ένας χρήστης σχετικά με τις πληροφορίες που δημοσιοποιεί στις ΕΚΔ, δεν είναι σε θέση να ελέγξει πληροφορίες, που άλλοι χρήστες δημοσιοποιούν για αυτόν (π.χ. ανέβασμα μιας φωτογραφίας χωρίς γνώση λοιπών εικονιζόμενων)

Κίνδυνοι Ασφάλειας & Ιδιωτικότητας

- **Παραχώρηση των δεδομένων** των χρηστών από τις ίδιες τις εταιρίες των ΕΚΔ σε τρίτες εταιρίες, για στοχευμένη διαφήμιση

Κίνδυνοι Ασφάλειας & Ιδιωτικότητας

- **Παραχώρηση στοιχείων σε εφαρμογές**, οι οποίες όμως δεν πιστοποιούνται πάντα για την ασφάλειά τους (ενδέχεται να αποκτούν πρόσβαση σε προσωπικές πληροφορίες ή να περιέχουν ιομορφικό λογισμικό)

Κίνδυνοι Ασφάλειας & Ιδιωτικότητας

Εξειδικευμένες απάτες

- Οι πληροφορίες που δημοσιεύουν οι χρήστες μπορεί να χρησιμοποιηθούν για επιθέσεις ηλεκτρονικής εξαπάτησης (phishing) ή κοινωνικής μηχανικής (social engineering)

Κίνδυνοι Ασφάλειας & Ιδιωτικότητας

- **Εύκολη μετάδοση επιβλαβούς ηλεκτρονικού περιεχόμενου** (όπως ιομορφικό λογισμικό, πορνογραφικό υλικό κ.ά.)
- **Πιθανά προβλήματα στην αγορά εργασίας** (π.χ. ένα βίντεο σπουδαστή σε εύθυμη κατάσταση μπορεί να σταθεί εμπόδιο σε μια μελλοντική προσπάθεια εύρεσης εργασίας)

Κίνδυνοι Ασφάλειας & Ιδιωτικότητας

- Οι ΕΚΔ μπορεί να γίνουν πολύ **εθιστικές**, οδηγώντας σταδιακά σε κοινωνική απομόνωση
- Οι **όροι χρήσης** μπορούν να αλλάξουν οποτεδήποτε το έχει αποδεχτεί ο χρήστης κατά την εγγραφή στον κοινωνικό δίκτυο
- Οι χρήστες **αποποιούνται των πνευματικών τους δικαιωμάτων** για οτιδήποτε ανεβάζουν, αφού πλέον ανήκει στο κοινωνικό δίκτυο

Facebook

Δημιουργία ψηφιακού φακέλου

- Τα προφίλ των χρηστών μπορούν να συγκεντρωθούν από τρίτους οι οποίοι θα δημιουργήσουν έναν ψηφιακό φάκελο προσωπικών δεδομένων που θα περιλαμβάνει στιγμιότυπα του κάθε προφίλ σε βάθος χρόνου

Facebook

Συλλογή δευτερευόντων πληροφοριών

- Πέραν των πληροφοριών που ο χρήστης εν γνώσει του κοινοποιεί μέσω του προφίλ του, το Facebook είναι σε θέση να συλλέγει πληροφορίες που προκύπτουν από τη χρήση της υπηρεσίας
- Η δυνατότητα αυθεντικοποίησης των χρηστών σε συνεργαζόμενους ιστότοπους χρησιμοποιώντας το λογαριασμό τους στο Facebook, διευρύνει τις δυνατότητες παρακολούθησης των ενεργειών τους

Facebook

Αναγνώριση προσώπου

- Οι φωτογραφίες που δημοσιεύονται στο προφίλ του χρήστη συνδέονται είτε άμεσα, μέσω των ετικετών που προσαρτώνται σε κάθε πρόσωπο της φωτογραφίας, είτε έμμεσα με τον κάτοχο του προφίλ και αποτελούν ένα ψηφιακό αναγνωριστικό του χρήστη, το οποίο δίνει τη δυνατότητα συσχέτισης διαφορετικών προφίλ του Facebook ή και διαφορετικών ΕΚΔ
- Δυνατότητα συλλογής περισσότερων πληροφοριών για έναν χρήστη από αυτές που ο ίδιος επιθυμεί να αποκαλύψει

Facebook

CBIR (Content-based Image Retrieval)

- Τεχνολογία διασταύρωσης χαρακτηριστικών από διαφορετικές φωτογραφίες με σκοπό τον εντοπισμό χρηστών
- Επιτρέπει την εξαγωγή **δεδομένων θέσης** από φαινομενικά ανώνυμα προφίλ και δίνει τη δυνατότητα άσκησης επιθετικού μάρκετινγκ ή άλλων ενεργειών που συνδέονται με την ακούσια αποκάλυψη δεδομένων θέσης

Facebook

Δυσκολία πλήρους διαγραφής προφίλ

- Το Facebook παρέχει τη δυνατότητα στο χρήστη να απενεργοποιήσει εύκολα το προφίλ του
- Δεν ισχύει όμως το ίδιο για την πλήρη διαγραφή του προφίλ, καθώς η δυνατότητα διαγραφής δεν είναι εξίσου ορατή και άμεση

Facebook

Δυσκολία πλήρους διαγραφής προφίλ

- Δευτερεύουσες πληροφορίες του χρήστη που συνδέονται με το προφίλ του, όπως τα σχόλια που έχει κάνει στα προφίλ τρίτων, είναι πρακτικά αδύνατον να αφαιρεθούν, αφού ο χρήστης θα πρέπει να τα εντοπίσει και να τα αφαιρέσει χειροκίνητα

Facebook

SPAM

- Spammers προσπαθούν να επωφεληθούν από την τεράστια ανάπτυξη του Facebook και τη δυνατότητα ελεύθερης διακίνησης μηνυμάτων που παρέχει, προκειμένου να διαδίδουν ανεπιθύμητα μηνύματα

Facebook

Ευπάθειες κώδικα και ιομορφικό λογισμικό

- Λόγω της υψηλής δημοτικότητάς του, το Facebook έχει αποτελέσει κατά καιρούς μέσο εξάπλωσης ιομορφικού λογισμικού το οποίο μπορεί να εκμεταλλευτεί ευπάθειες του κώδικα της πλατφόρμας της υπηρεσίας, των εφαρμογών τρίτων που χρησιμοποιούνται μέσα από αυτή, του συστήματος του χρήστη, ή την άγνοια των χρηστών σχετικά με τις μεθόδους προστασίας

Facebook

Διαρροή προσωπικών δεδομένων μέσω της χρήσης τρίτων εφαρμογών

- Η χρήση των εφαρμογών που παρέχονται μέσω του Facebook ενδέχεται να δίνει τη δυνατότητα σε τρίτους να αποκτήσουν πρόσβαση στα προσωπικά στοιχεία του χρήστη

Facebook

Ηλεκτρονική εξαπάτηση και κοινωνική μηχανική

- Το Facebook μπορεί να χρησιμοποιηθεί από έναν επιτιθέμενο ως εργαλείο συλλογής πληροφοριών για έναν χρήστη-στόχο, οι οποίες θα του επιτρέψουν να εξαπολύσει μία στοχευμένη επίθεση ηλεκτρονικής εξαπάτησης
- Μπορεί να χρησιμοποιηθεί ως μέσο διάδοσης συνδέσμων ηλεκτρονικής εξαπάτησης

Facebook

Διείσδυση σε δίκτυα και διαρροή πληροφοριών

- Ορισμένες πληροφορίες είναι διαθέσιμες μόνο σε Φίλους και μέλη μίας περιορισμένης ομάδας ανθρώπων
- Λόγω του ότι κάποιος μπορεί να κερδίσει εύκολα τη «φιλία» ενός χρήστη, αυτός ο μηχανισμός προστασίας δεν είναι ιδιαίτερα αποτελεσματικός
- Για την επικοινωνία μεταξύ των χρηστών δεν παρέχεται καμιά εγγύηση ως προς την ασφάλεια και την ιδιωτικότητα

Facebook

Πλαστοπροσωπία

- Η υλοποίηση αυτής της επίθεσης δεν απαιτεί ιδιαίτερες γνώσεις, αφού οποιοσδήποτε χρήστης μπορεί να δημιουργήσει ένα προφίλ, παρέχοντας στη συνέχεια τα στοιχεία του προσώπου που θέλει να υποδυθεί
- Παραλλαγές της επίθεσης αυτής είναι η κλωνοποίηση προφίλ και η μεταφορά υπάρχοντος προφίλ σε άλλες ΕΚΔ

Facebook

Πειρατεία προφίλ

- Ο επιτιθέμενος αποκτά τον πλήρη έλεγχο του προφίλ ενός χρήστη, χρησιμοποιώντας διάφορες τεχνικές και εκμεταλλευόμενος ευπάθειες όπως αδύναμα συνθηματικά και ελλιπή μέτρα προστασίας

Facebook

Παρακολούθηση και καταδίωξη

- Πρόκειται για επιθετικές συμπεριφορές ατόμων τα οποία επιδιώκουν να έρθουν σε επικοινωνία και φυσική επαφή με το θύμα
- Το Facebook ενθαρρύνει τη δημοσίευση προσωπικών πληροφοριών τα οποία αποκαλύπτουν τη θέση του χρήστη, τη συμπεριφορά του ή ακόμα και το αν είναι συνδεδεμένος με την υπηρεσία

Facebook

Εκφοβισμός

- Το Facebook διαθέτει ορισμένα χαρακτηριστικά που το καθιστούν χρήσιμο εργαλείο για έναν επιτιθέμενο ο οποίος επιθυμεί να εκφοβίσει το θύμα του:
- Η ευκολία με την οποία ο επιτιθέμενος μπορεί να παραμείνει ανώνυμος (χρησιμοποιώντας ένα ψεύτικο προφίλ)
- Η δυνατότητα χρήσης πολλαπλών καναλιών επικοινωνίας μέσα από την ίδια πλατφόρμα

Facebook

Απειλή «εκ των έσω»

- Το Facebook αντλεί το μεγαλύτερο ποσοστό των κερδών του από τη διαφήμιση, γεγονός που αποτελεί το σημαντικότερο κίνδυνο κατά της ιδιωτικότητας
- Ο χρήστης δε διαθέτει τη δυνατότητα να διασφαλίσει ότι ο πάροχος δεν θα καταχραστεί τα δεδομένα του ή ότι εφαρμόζει την πολιτική ιδιωτικότητας που ανακοινώνει

Twitter

Διαρροή προσωπικών δεδομένων και συμπεριφοράς

- Ο χρήστης είτε εσκεμμένα είτε ακούσια μπορεί να αποκαλύψει προσωπικά δεδομένα ή ευαίσθητες πληροφορίες για τον ίδιο ή και για άλλους χρήστες με πιθανά δυσάρεστα αποτελέσματα
- Η δυνατότητα προώθησης μηνυμάτων (retweeting) αυξάνει τον κίνδυνο αποκάλυψης ευαίσθητων προσωπικών δεδομένων

Twitter

Εντοπισμός θέσης

- Η δυνατότητα εντοπισμού της ακριβούς τοποθεσίας ενός χρήστη και η παρακολούθησή του ανά πάσα στιγμή

SPAM

- Αποστολή συνδέσμων σε ιστοσελίδες με διαφημιστικό περιεχόμενο, phishing και ιομορφικό λογισμικό

Twitter

Πειρατεία λογαριασμού

- Ο επιτιθέμενος αποκτά πρόσβαση στον λογαριασμό ενός χρήστη, χρησιμοποιώντας διάφορες τεχνικές και εκμεταλλευόμενος ευπάθειες όπως αδύναμα συνθηματικά και ελλιπή μέτρα προστασίας

Twitter

Πλαστοπροσωπία

- Ένας κακόβουλος χρήστης μπορεί να δημιουργήσει λογαριασμό στο Twitter, προβάλλοντας τις ιδιότητες ενός άλλου προσώπου που θέλει να υποδυθεί

Twitter

Trolls

- Ανώνυμοι χρήστες με πονηρά προκλητικές, σκόπιμα ανόητες ή επιτηδευμένα εκτός θέματος παρεμβάσεις, με πρωταρχική πρόθεση να προκαλέσουν αλυσίδα αντιδράσεων από άλλους χρήστες
- Αποτελεί συνηθισμένο λάθος, ειδικά ανάμεσα στους αρχάριους χρήστες, η προσπάθεια να απαντήσουν σε ή να κάνουν διάλογο με επιθετικά ή αγενή trolls

Γενικές Οδηγίες

Έλεγχος ρυθμίσεων με επιλογή όσων παρέχουν υψηλό βαθμό προστασίας

Αξιολόγηση πληροφοριών/ έλεγχος μεταδεδομένων που δημοσιεύονται

Εγκατάσταση και ενημέρωση αξιόπιστου αντι-ιομορφικού λογισμικού

Ενημέρωση για τις ευπάθειες των ΕΚΔ και αναβάθμιση του λογισμικού

Εφαρμογή μεθόδων προστασίας από επιθέσεις κοινωνικής μηχανικής

Χρήση ισχυρών συνθηματικών και τακτική αλλαγή κωδικών πρόσβασης

Κουλτούρα προσανατολισμένη στην προστασία της πληροφορίας

Αναφορά περιστατικών και απειλών ασφάλειας

Έλεγχος της πολιτικής ιδιωτικότητας και των όρων χρήσης των ΕΚΔ

Ευχαριστώ για την προσοχή σας

Ερωτήσεις





ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ



ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ
ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ