**Εκφώνηση Εργασίας**

Εργασία Γ': Σχεδιασμός μιας Ανθρωποκεντρικής Εκστρατείας Ευαισθητοποίησης για την Κυβερνοασφάλεια (Awareness Campaign)

Περιγραφή:

Σε αυτή την ομαδική εργασία, οι φοιτητές σε ομαδες θα σχεδιάσουν μια ολοκληρωμένη εκστρατεία (campaign) ευαισθητοποίησης για την κυβερνοασφάλεια, προσαρμοσμένη σε ένα συγκεκριμένο κοινό-στόχο (π.χ., υπαλλήλους μιας εταιρείας, φοιτητές ενός πανεπιστημίου ή το ευρύ κοινό). Η εκστρατεία θα πρέπει να επικεντρώνεται στην αντιμετώπιση των ανθρώπινων ευπαθειών στην κυβερνοασφάλεια, όπως οι επιθέσεις phishing, η διαχείριση κωδικών πρόσβασης, η κοινωνική μηχανική και οι ασφαλείς διαδικτυακές συμπεριφορές.

Η εργασία θα απαιτεί:

1. Ταυτοποίηση του κοινού: Ανάλυση των κοινών προκλήσεων και συμπεριφορών του επιλεγμένου κοινού σε θέματα κυβερνοασφάλειας.

2. Ανάπτυξη περιεχομένου: Δημιουργία εκπαιδευτικού υλικού όπως αφίσες, βίντεο ή διαδραστικό περιεχόμενο που καλύπτουν τις ανάγκες του κοινού, προωθώντας παράλληλα βέλτιστες πρακτικές.

3. Συμπεριφορικές εκτιμήσεις: Εφαρμογή αρχών από την ψυχολογία της συμπεριφοράς και τους ανθρώπινους παράγοντες, ώστε η εκστρατεία να επηρεάζει αποτελεσματικά τις στάσεις και τις δράσεις.

4. Σχέδιο αξιολόγησης: Πρόταση μιας μεθόδου για την αξιολόγηση του αντίκτυπου της εκστρατείας, όπως μέσω ερευνών πριν και μετά ή μέσω προσομοιωμένων δοκιμών κυβερνοασφάλειας.

Τελικό παρουσίαση:

Θα είναι μια αναφορά που συνοψίζει το σχέδιο της εκστρατείας, τη λογική πίσω από αυτό, καθώς και μια παρουσίαση που θα αναδεικνύει το υλικό και τη στρατηγική. Στόχος είναι η ανάπτυξη πρακτικών, ανθρωποκεντρικών λύσεων για την ενίσχυση της ευαισθητοποίησης και της ανθεκτικότητας στην κυβερνοασφάλεια.

Υπάρχει η επιλογή να την κάνετε στα Αγγλικά ή στα Ελληνικά. Θα πρεπει να ανεβασετε την PowerPoint παρουσιαση σας.

**1. Ταυτοποίηση του κοινού: Ανάλυση των κοινών προκλήσεων και συμπεριφορών του επιλεγμένου κοινού σε θέματα κυβερνοασφάλειας.**

Για την συγκεκριμένη εκστρατεία, επιλέγουμε ως κοινό τους υπαλλήλους μιας ιδιωτικής εταιρείας (π.χ. μιας τράπεζας), η οποία καλύπτει ένα εύρος τμημάτων που αποτελείται από μεγάλο αριθμό εργαζομένων ( τμήματα ανθρωπίνου δυναμικού, τραπεζικοί υπάλληλοι, λογιστήριο, κτλ.) Συνεπώς απευθυνόμαστε σε άτομα με ηλικία από 18 έως 67 ετών, εργατικό δυναμικό το οποίο είναι συχνός στόχος επιθέσεων όπως η κοινωνική μηχανική και το ηλεκτρονικό ψάρεμα πληροφοριών, καθώς είναι μέρος κρίσιμης υποδομής που έχει πρόσβαση σε ευαίσθητα δεδομένα, το οποίο έχει διαφορετική γνώση και εξοικείωση με τέτοιες μορφές κινδύνου.

Συχνά συμβάντα που επηρεάζουν το cybersecurity posture σε ένα τέτοιο εργασιακό περιβάλλον:

* Χρησιμοποίηση αδύναμων κωδικών πρόσβασης και επαναχρησιμοποίηση κωδικών σε πολλές υπηρεσίες.
* Άνοιγμα phishing emails και επισυναπτόμενων αρχείων.
* Μετάβαση σε ανασφαλείς ιστοτόπους μέσω κλικ σε επικίνδυνους συνδέσμους.
* Ανεπαρκής ενημέρωση σχετικά με τις κυβερνοαπειλές.

**2. Ανάπτυξη περιεχομένου: Δημιουργία εκπαιδευτικού υλικού όπως αφίσες, βίντεο ή διαδραστικό περιεχόμενο που καλύπτουν τις ανάγκες του κοινού, προωθώντας παράλληλα βέλτιστες πρακτικές.**

Η εκστρατεία που θα εφαρμόσουμε θα περιλαμβάνει πλούσιο εκπαιδευτικό υλικό σε παιχνιδοποιημένη μορφή μέσω πολλών αγωγών, με σκοπό να κάνει πιο εύκολη την ενασχόληση για τον μέσο χρήστη σε συνδυασμό με πρόγραμμα επιβράβευσης.

Προχωράμε σε ανάλυση του περιεχομένου που προσφέρουμε:

Το υλικό περιλαμβάνει εκτεταμένη θεματολογία όπως:

* Συμβουλές για διαχείριση και χρησιμοποίηση κωδικών
* Συμβουλές για ασφαλή χρήση USB και εξωτερικών συσκευών στον εργασιακό χώρο
* Πώς να εντοπίζεις phishing/smishing/vishing.
* Διαδικασίες backup.
* Συμβουλές διαχείρισης ευαίσθητων δεδομένων.
* Συμβουλές χρησιμοποίησης AI tools, όπως τα LLMs.

**Εκπαιδευτικό Υλικό (Infographics, Posters):**

Το εκπαιδευτικό υλικό θα αποδίδεται μέσω:

* Infographics τα οποία θα τοποθετούνται σε monitor που θα βρίσκονται σε στρατηγικά σημεία της εταιρείας όπως (υποδοχή, διάδρομοι, κουζίνα, meeting rooms)
* Posters τα οποία θα τοποθετούνται σε αντίστοιχους χώρους.

**Διαδραστικό Υλικό( Awareness Quizes, Phishing Simulations):**

Το διαδραστικό περιεχόμενο θα αποδίδεται μέσω email και θα περιέχει τα εξείς:

1η Περίπτωση: Awareness Quiz

Το email θα περιλαμβάνει εν συντομία κάποια δεδομένα στοιχεία και θα περιλαμβάνει ερώτηση πάνω στα προαναφερθέντα. ( Yes or No Question).

Αφού ο χρήστης απαντήσει μεταφέρεται σε landing page η οποία περιέχει σύνοψη του γιατί είναι λάθος ή σωστή η απάντηση που έδωσε ο χρήστης και ένα ενημερωτικό video.

2η Περίπτωση: Phishing Simulations

Το email θα περιλαμβάνει υλικό που είναι αληθοφανές ώστε να μπορεί να ξεγελάσει το χρήστη να κλικάρει σε ένα σύνδεσμο, ή σε κάποιο κουμπί ή να ανοίξει ένα αρχείο.

Αν ο χρήστης κάνει κλικ, μεταφέρεται σε landing page το οποίο περιγράφει τα ύποπτα στοιχεία που περιλαμβάνει το email και ένα ενημερωτικό βίντεο που περιγράφει το phishing.

**3. Συμπεριφορικές εκτιμήσεις: Εφαρμογή αρχών από την ψυχολογία της συμπεριφοράς και τους ανθρώπινους παράγοντες, ώστε η εκστρατεία να επηρεάζει αποτελεσματικά τις στάσεις και τις δράσεις.**

Η καμπάνια που ακολουθούμε περιέχει και μέτρα για ενίσχυσης της ενασχόλησης με το πρόγραμμα.

Πιο συγκεκριμένα:

-Gamification: Όλο το εκπαιδευτικό και διαδραστικό υλικό είναι σε μορφή σύντομου παιχνιδιού με ωραία και απλά γραφικά.

- Εύκολο Περιεχόμενο: Είμαστε σύντομοι, περιεκτικοί και αποφεύγουμε περίπλοκές ορολογίες.

-Πρόγραμμα Επιβράβευσης: Κρατάμε στατιστικά από όλο το διαδραστικό περιεχόμενο, επιβραβεύοντας τους χρήστες με τις περισσότερες απαντήσεις στα quiz και με τα λιγότερα κλικ στα simulations.

**4. Σχέδιο αξιολόγησης: Πρόταση μιας μεθόδου για την αξιολόγηση του αντίκτυπου της εκστρατείας, όπως μέσω ερευνών πριν και μετά ή μέσω προσομοιωμένων δοκιμών κυβερνοασφάλειας.**

Ως αρχική προσέγγιση θα πραγματοποιήσουμε μια αξιολόγηση γνώσεων με ερωτηματολόγιο, το οποίο θα εφαρμόσουμε και μετά τη λήξη της καμπάνιας για να επιβεβαιώσουμε το αντίκτυπο της καμπάνιας.