Πανεπιστήμιο Πατρών

Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΨΗΦΙΑΚΗ ΚΑΙΝΟΤΟΜΙΑ ΚΑΙ ΔΙΟΙΚΗΣΗ»

Διπλωματική Εργασία

«Κοινωνική Μηχανική: Τεχνικές Επίθεσης & Άμυνας»

ΝΤΖΟΛΑ ΝΙΚΟΛΙΤΣΑ

Επιβλέπων Καθηγητής

Σταματίου Ιωάννης

Πάτρα,

Μάρτιος 2022

Πανεπιστήμιο Πατρών, Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας

Ντζόλα Νικολίτσα

Αφιερώνω την διπλωματική μου εργασία στις κόρες μου Ευαγγελία και Θεώνη

ΠΕΡΙΛΗΨΗ

Οι εξελίξεις στον τομέα της ψηφιακής τεχνολογίας και των πληροφορικών συστημάτων έχουν βελτιώσει σε πολλούς τομείς τη ζωή μας. Ωστόσο, προσωπικές και ευαίσθητες πληροφορίες ενδέχεται να αποτελέσουν στόχο κακόβουλων ενεργειών με στόχο την εξαπάτηση μας. Η Κοινωνική Μηχανική στηρίζεται στην ψυχολογική χειραγώγηση των ανθρώπων με σκοπό την απόσπαση εμπιστευτικών πληροφοριών, προκειμένου οι επιτιθέμενοι να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικά συστήματα.

Οι επιθέσεις κοινωνικής μηχανικής επικεντρώνονται στη χρήση πειθούς από τον επιτιθέμενο. Η κοινωνική μηχανική αποτελεί μια από τις μεγαλύτερες προκλήσεις που αντιμετωπίζει η ασφάλεια των δικτύων, επειδή εκμεταλλεύεται τη τάση του ανθρώπου να εμπιστεύεται. Αυτή η εργασία ερευνά τι είναι η κοινωνική μηχανική, παρουσιάζει τις τεχνικές επίθεσης μέσω πραγματικών περιστατικών, όπως αυτές αφηγούνται από τον ίδιο τον κοινωνικό μηχανικό, τις τεχνικές άμυνας που χρησιμοποιούνται για την αντιμετώπιση τέτοιων επιθέσεων καθώς και στατιστικά στοιχεία που δείχνουν τον αντίκτυπο σε παγκόσμιο επίπεδο των επιθέσεων κοινωνικής μηχανικής.

Λέξεις κλειδιά: Κοινωνική Μηχανική, Επιθέσεις Κοινωνικής Μηχανικής, Τεχνικές Άμυνας

ABSTRACT

Developments in digital technology and information systems have improved our lives in many fields. However, personal, and sensitive information may be the target of malicious acts aimed at deceiving us. Social engineering relies on the psychological manipulation of people, in order to extract confidential information in order for attackers to gain unauthorized access to computer systems.

Social engineering attacks focus on the intruder's use of persuasion. Social engineering is one of the biggest challenges facing network security because it exploits the human tendency to trust. This study explores what social engineering is, presents fact-finding attack techniques as narrated by the social engineer himself, the defense techniques used to deal with such attacks, and statistics showing the global impact of social engineering attacks.

Keywords: Social Engineering, Attack, Prevention

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Ένα από τα προβλήματα της σύγχρονης ψηφιακής εποχής είναι η προστασία ευαίσθητων πληροφοριών και δεδομένων.
Η εφαρμογή τεχνολογικών μέτρων, δεν είναι άκρως αποτελεσματική, διότι οι επιτιθέμενοι βασίζονται στον ανθρώπινο παράγοντα που είναι απρόβλεπτος.
Η Κοινωνική Μηχανική είναι η επιστήμη που βασίζεται στην τεχνική της ψυχολογικής χειραγώγησης των ανθρώπων μέσω της οποίας οι επιτιθέμενοι εκμαιεύουν από τα θύματά τους σημαντικά δεδομένα και εμπιστευτικές πληροφορίες, με σκοπό την εξαπάτηση είτε των ίδιων, είτε άλλων ανθρώπων, είτε οργανισμών.
Σκοπός της εργασίας είναι η επίδειξη των τεχνικών που εφαρμόζουν οι κοινωνικοί μηχανικοί στις επιθέσεις τους - μέσω της αφήγησης πραγματικών περιστατικών επιθέσεων - καθώς των μεθόδων που έχουν αναπτυχθεί για την αντιμετώπιση και την προστασία απέναντι σε τέτοιου είδους επιθέσεις.
Αναλυτικότερα, στο πρώτο κεφάλαιο αναφέρουμε ορισμούς, έννοιες, τα γενικά χαρακτηριστικά της Κοινωνικής Μηχανικής και γιατί είναι σημαντική.
Στο δεύτερο κεφάλαιο αναφέρουμε τέσσερις περιπτώσεις πραγματικών επιθέσεων, όπως αυτές παρουσιάζονται από τον ίδιο τον επιτιθέμενο, τον γκουρού της Κοινωνικής Μηχανικής, Kevin Mitnick, στο βιβλίο του «The Art of Human Hacking».
Στη συνέχεια παρουσιάζονται οι τρόποι εφαρμογής, οι τεχνικές που χρησιμοποιούνται κατά τη διάρκεια των επιθέσεων καθώς και τα κριτήρια βάση των οποίων ταξινομούνται σε διαφορετικές κατηγορίες οι επιθέσεις.
Στο τέταρτο κεφάλαιο αναφέρονται οι τεχνικές άμυνας που έχουν αναπτυχθεί με στόχο την προστασία από επιθέσεις Κοινωνικής Μηχανικής. Γίνεται σαφές πόσο σημαντική είναι η προστασία μας απέναντι στις επιθέσεις και ότι μπορεί να μην είναι εφικτό να αποτρέψουμε μία επίθεση, αλλά μπορούμε να μειώσουμε την πιθανότητα ολοκλήρωσης μιας επίθεσης με επιτυχία.
Στο πέμπτο κεφάλαιο βλέπουμε με στατιστικά δεδομένα, τον αυξανόμενο αριθμό επιθέσεων παγκοσμίως τα τελευταία χρόνια, καθώς και την επίπτωση τους σε κοινωνικό, πολιτικό, οικονομικό επίπεδο.
Στο έκτο κεφάλαιο αναφέρουμε τα συμπεράσματα που εξήχθησαν από τη μελέτη του συγκεκριμένου θέματος και τέλος ακολουθούν οι βιβλιογραφικές αναφορές που μελετήθηκαν.

Με την ολοκλήρωση της διπλωματικής μου εργασίας, θα ήθελα να ευχαριστήσω από καρδίας τους ανθρώπους που με στήριξαν. Ευχαριστώ θερμά τον επιβλέπον καθηγητή, κ. Σταματίου Ιωάννη, για την εμπιστοσύνη και την καθοδήγηση του καθ' όλη τη διάρκεια της συνεργασίας μας. Επιπλέον θα ήθελα να εκφράσω την ευγνωμοσύνη μου στην οικογένεια μου και το σύζυγο μου για την συμπαράσταση και την κατανόηση τους καθ' όλη τη διάρκεια των σπουδών μου και ιδιαιτέρως την αδελφή μου Βάσω που ήταν συνεχώς δίπλα μου στη προσπάθεια αυτή.

1. ΕΙΣΑΓΩΓΗ

Ο τομέας της ασφάλειας πληροφοριών είναι ένας ταχέως αναπτυσσόμενος κλάδος. Η προστασία των πληροφοριών είναι ζωτικής σημασίας για οργανισμούς και κυβερνήσεις και η ανάπτυξη αντίμετρων κατά της παράνομης πρόσβασης σε πληροφορίες είναι ένας τομέας που τυγχάνει αυξανόμενης προσοχής. Οι οργανισμοί και οι κυβερνήσεις έχουν έννομο συμφέρον να προστατεύουν ευαίσθητες πληροφορίες και να διασφαλίζουν την εμπιστοσύνη των πελατών και των πολιτών αντίστοιχα.

Η τεχνολογία από μόνη της δεν αποτελεί επαρκή προστασία έναντι της κλοπής πληροφοριών. Το προσωπικό είναι συχνά ο αδύναμος κρίκος σε ένα σύστημα ασφάλειας πληροφοριών. Το προσωπικό μπορεί να επηρεαστεί ώστε να αποκαλύψει ευαίσθητες πληροφορίες που στη συνέχεια να επιτρέπουν σε μη εξουσιοδοτημένα άτομα να έχουν πρόσβαση στα προστατευμένα συστήματά τους.

Μια καινούργια επιστήμη, αυτή της Κοινωνικής Μηχανικής, άρχισε να επεκτείνετε σε αυτά τα πλαίσια. Μια επιστήμη που συνδυάζει στοιχεία ψυχολογίας, υποκριτικής τέχνης με την βοήθεια των εξελιγμένων γνώσεων προγραμματισμού και τεχνικών επιθέσεων (Αναγνωστόπουλος, 2021).

Αυτό που καθιστά την κοινωνική μηχανική ιδιαίτερα επικίνδυνη είναι ότι βασίζεται σε ανθρώπινο λάθος, παρά σε ευπάθειες λογισμικών και λειτουργικών συστημάτων (https://www.imperva.com/learn/application-security/social-engineering-attack,).

Στην παρούσα εργασία θα αναφερθούμε στις πτυχές της Κοινωνικής Μηχανικής και θα εμβαθύνουμε στις τεχνικές των επιθέσεων καθώς και στις τεχνικές άμυνας που είναι πολύ σημαντικές για την προστασία των πληροφοριών.

1.1. Κυβερνοασφάλεια και Κυβερνοέγκλημα

Μόλις το 1984, Ο Gibson, στο βιβλίο επιστημονικής φαντασίας «Νευρομάντης», όρισε τον κυβερνοχώρο ως: «μια συναινετική παραίσθηση που βιώνουν καθημερινά δισεκατομμύρια νόμιμοι χρήστες, σε κάθε χώρα, από παιδιά που διδάσκονται μαθηματικές έννοιες...Μια γραφική απεικόνιση δεδομένων που αφαιρούνται από τις τράπεζες κάθε υπολογιστή στο ανθρώπινο σύστημα. Αδιανόητα περίπλοκο. Γραμμές φωτός κυμαίνονταν στον μη- χώρο του μυαλού, συστάδες και αστερισμοί δεδομένων. Σαν τα φώτα της πόλης, που υποχωρούν...» (http://vr.arch.uth.gr/VR-Arch/PDF/VR-01_Cyberspace.pdf).

Κυβερνοέγκλημα ορίζεται η κάθε αξιόποινη πράξη που λαμβάνει χώρα στον Κυβερνοχώρο και προβλέπεται με νομική διάταξη *(https://el.wikipedia.org/wiki/%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1)*.

Σύμφωνα με το Ευρωπαϊκό Συμβούλιο, κυβερνοέγκλημα ορίζεται κάθε αδίκημα κατά συστημάτων ηλεκτρονικών υπολογιστών αλλά και κάθε αδίκημα που διαπράττεται μέσω της χρήσης συστημάτων ηλεκτρονικών υπολογιστών.

Σύμφωνα με την Ευρωπαϊκή Ένωση ως Κυβερνοέγκλημα ορίζονται οι εγκληματικές πράξεις που διαπράττονται στο διαδίκτυο με τη χρήση ηλεκτρονικών δικτύων επικοινωνιών και συστημάτων πληροφοριών (https://el.wikipedia.org/wiki/%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1).

Μεμονωμένα πρόσωπα ή ομάδες ατόμων που χρησιμοποιούν τη τεχνολογία και εκτελούν εγκλήματα στον κυβερνοχώρο ονομάζονται κυβερνοεγκληματίες (Αναγνωστόπουλος, 2021).

Εικόνα 1.1 : Κυβερνοασφάλεια

(https://www.philenews.com/koinonia/eidiseis/article/1025005/kampanaki-ga-kybernoasfaleia-dechomaste-epitheseis)

1.2. Τι είναι η Κοινωνική Μηχανική

Κοινωνική μηχανική είναι η χειραγώγηση ατόμων μέσω του τεχνάσματος της εμπιστοσύνης με σκοπό την εκμαίευση προσωπικών και εμπιστευτικών πληροφοριών που μπορούν να χρησιμοποιήσουν για τέλεση απάτης (Βάββας, 2010).

Εικόνα 1.2 : Η τέχνη της χειραγώγησης
(https://www.philenews.com/eidiseis/paraskinio/article/934790)

1.3. Γιατί είναι σημαντική η κοινωνική μηχανική ;

Εν δυνάμει όλοι μας μπορούμε να αποτελέσουμε στόχο κάποιου κοινωνικού μηχανικού καθώς όλοι σχεδόν οι άνθρωποι διαθέτουν ηλεκτρονικούς υπολογιστές και χρησιμοποιούν συνεχώς το διαδίκτυο.

Ανταγωνιστές που προσπαθούν να αποκτήσουν πλεονέκτημα, υπάλληλοι που δεν είναι ευχαριστημένοι και θέλουν να εκδικηθούν ή να αποκομίσουν οικονομικό όφελος, ακόμα και μέλη οργανωμένου εγκλήματος μπορεί να εφαρμόσουν επιθέσεις κοινωνικής μηχανικής (Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ, 2020)

Το 2019 έρευνα της Zogby Analytics παρουσίασε ότι το 44% των μικρομεσαίων επιχειρήσεων έχει πέσει θύμα κοινωνικής μηχανικής τον τελευταίο χρόνο. Το 88% των επιχειρήσεων θεωρεί ότι είναι πιθανός στόχος ενώ το 46% πολύ πιθανό στόχο επίθεσης.

Το FBI εκτιμά ότι, μόνο το 2018 περισσότερα από 2,7 δισεκατομμύρια δολάρια χάθηκαν από αμερικανικές εταιρίες λόγων κυβερνοεπιθέσεων. Σε αυτά συμπεριλαμβάνονται 1,2 δισεκατομμυρίων δολαρίων που οφείλονται σε υποκλοπές εταιρικών email που επέτρεψαν μεταφορές χρημάτων χωρίς εξουσιοδότηση (https://www.eset.com/gr/social-engineering-business/) .

Η κοινωνική μηχανική δεν αποτελεί απειλή μόνο για έναν οργανισμό, μια εταιρεία ή έναν μεμονωμένο πολίτη. Υπάρχουν περιστατικά που αποδεικνύουν ότι η κοινωνική μηχανική μπορεί να εξελιχθεί ακόμα και σε απειλή πολιτικής σταθερότητας καθώς ολόκληροι λαοί μέσω της οργανωμένης παραπληροφόρησης μπορούν να χειραγωγηθούν ώστε να αλλάξει η πολιτική σκήνη της χώρας.

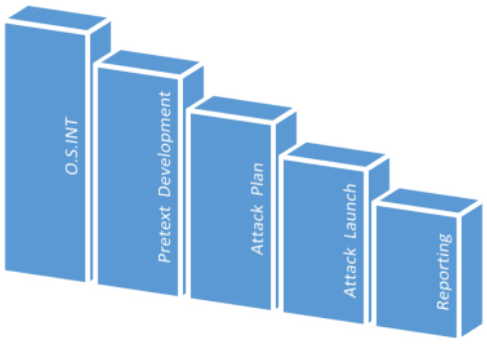
Παράδειγμα μιας τέτοιας περίπτωσης αποτελεί η κυβερνοεπίθεση το 2007 κατά της Εσθονίας.

Κατά την ανεξαρτοποίηση της Εσθονίας το 1991 από τη Σοβιετική Ένωση, δόθηκε μεγάλη έμφαση στην πληροφοριακή ανάπτυξης της χώρας. Οι πολίτες απέκτησαν ψηφιακές ταυτότητες και σήμερα σχεδόν το 99% των ηλεκτρονικών και τραπεζικών

υπηρεσιών διεξάγονται ηλεκτρονικά. Το 2007 όμως διαδοχικές κυβερνοεπιθέσεις λαμβάνουν χώρα με αποτέλεσμα πολλές υπηρεσίες να μην είναι διαθέσιμες στους πολίτες καθώς και πολλές λειτουργίες των τραπεζών. Οι επιθέσεις αυτές είχαν πολιτική χροιά λόγω διαφορών που υπήρχαν μεταξύ Εσθονίας και Ρωσίας. Όμως η εξιχνίαση τέτοιων επιθέσεων είναι δύσκολη υπόθεση (Βλάχου κ.α, 2020).
Μια ακόμη περίπτωση πολιτικής κοινωνικής επίθεσης αποτελεί η υπόθεση της βρετανικής εταιρίας συμβούλων «Cambridge Analytica». Η εταιρία μέσω ενός ερωτηματολογίου σχετικά με το ψυχολογικό προφίλ των χρηστών του Facebook χρησιμοποίησε τα προσωπικά δεδομένα περίπου 87 εκατομμυρίων χρηστών, χωρίς τη συγκατάθεσή τους ώστε να παρέχει υποστήριξη στην προεκλογική εκστρατεία το 2016 του Ντόναλντ Τράμπ. Επίσης η εταιρία κατηγορήθηκε και για επιρροή στο Brexit, χωρίς ωστόσο να επιβεβαιώνεται η εμπλοκή της στην υπόθεση αυτή (https://el.wikipedia.org/wiki/%CE%A3%CE%BA%CE%AC%CE%BD%CE%B4%CE%B1%CE%BB%CE%BF_%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD_Facebook-Cambridge_Analytica).
Φυσικά ακόμα και σήμερα, πλήθος κυβερνοεπιθέσεων διεξάγονται μεταξύ Ουκρανίας και Ρωσίας στο πλαίσιο της πολεμικής σύρραξης των δύο χώρων.
Από τα ανωτέρω γίνεται αντιληπτό πως όλοι μας ξεχωριστά αλλά και οι οργανισμοί (δημόσιοι & ιδιωτικοί) πρέπει να αναπτύξουν ή και να βελτιώσουν τα συστήματα ασφαλείας τους απέναντι στις κυβερνοεπιθέσεις.

1.3.1. Η «Πυραμίδα» της κοινωνικής μηχανικής

Η πυραμίδα της Κοινωνικής Μηχανικής όπως φαίνεται στο παρακάτω σχήμα μας δείχνει τις ενέργειες που χρειάζονται καθώς και το χρόνο που είναι απαραίτητος σε κάθε στάδιο της.



Σχήμα 1.1. : Η «πυραμίδα» της Κοινωνικής Μηχανικής

(*Αναγνωστόπουλος 2020)*

- **O.S.INT** (Open Source Intelligent – Πληροφορίες Ανοιχτών Πηγών).

Είναι οι διαθέσιμες πληροφορίες στο κοινό που εμφανίζονται σε έντυπη ή ηλεκτρονική μορφή όπως για παράδειγμα τα μέσα κοινωνικής δικτύωσης, τα μέσα μαζικής ενημέρωσης ή και εξειδικευμένες αναζητήσεις μέσω μηχανής αναζήτησης. Είναι το στάδιο που καταλαμβάνει την περισσότερη διάθεση χρόνου και περιλαμβάνει το μεγαλύτερο μερίδιο της πυραμίδας.

- **Pretext Development** (Ανάπτυξη Προσχήματος).

Είναι η διαδικασία που περιλαμβάνει μια κατάσταση ή ένα πρόσχημα, που δημιουργήθηκε από έναν εισβολέα για να παρασύρει το θύμα και να το ξεγελάσει ώστε να δώσει απόρρητες πληροφορίες. Η διαδικασία αυτή βασίζεται στις πληροφορίες που έχει συλλέξει ο επιτιθέμενος στο πρώτο στάδιο και είναι το επόμενο βήμα που ακολουθείται. Επίσης σε αυτό το στάδιο ο επιτιθέμενος αποφασίζει τι εργαλεία θα χρησιμοποιήσει στην επίθεση του.

- **Attack Plan** (Σχέδιο Επίθεσης)

Σε αυτό το στάδιο ο επιτιθέμενος έχοντας αναπτύξει το σχέδιο του, αποφασίζει τον τρόπο και τον χρόνο που θα εκδηλώσει την επίθεσή του. Εκτός από το αρχικό στάδιο ο επιτιθέμενος πρέπει να οργανώσει και ένα εναλλακτικό σχέδιο σε περίπτωση που δημιουργηθεί κάποιο πρόβλημα και δεν υλοποιηθεί ο αρχικός του σχεδιασμός.

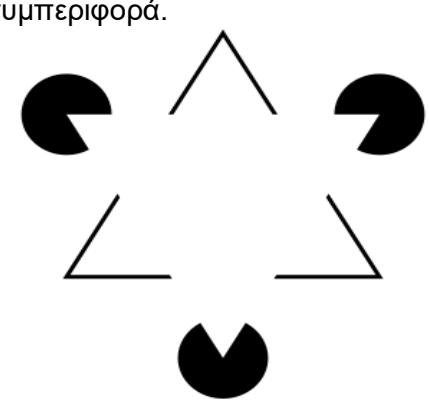
- **Reporting** (Αναφορά).

Η διαδικασία αυτή χρησιμοποιείται μόνο από τους επαγγελματίες της ασφάλειας υπολογιστών για να επισημάνουν τα αποτελέσματα της επίθεσης, να προτείνουν νέες λύσεις και να αυξήσουν τα μέτρα ασφαλείας (Αναγνωστόπουλος, 2021).

1.3.2. Χαρακτηριστικά του Κυβερνοχώρου που εκμεταλλεύεται η Κοινωνική Μηχανική

Σύμφωνα με τον Michael Benedikt, ο κυβερνοχώρος είναι ένα νέο σύμπαν, ένα παράλληλο σύμπαν δημιουργημένο και συντηρούμενο από ένα σύνολο υπολογιστών του κόσμου και τις γραμμές επικοινωνίας τους. Ένας κόσμος στον οποίο η παγκόσμια διακίνηση γνώσης, μυστικών, μετρήσεων, ψυχαγωγίας και εξωγήινων επιδράσεων παίρνει μορφή με τέτοιο τρόπο ώστε εικόνες, ήχοι και παρουσίες απούσες στη γη, ανθίζουν σε μια τεράστια ηλεκτρονική νύχτα (http://vr.arch.uth.gr/VR-Arch/PDF/VR-01_Cyberspace.pdf).

Τα χαρακτηριστικά του κυβερνοχώρου ταξινομούνται σε τρία βασικά στάδια. Μελετώντας αυτά τα στάδια επισημαίνουμε γιατί η Κοινωνική Μηχανική επιδρά με μεγάλη ευκολία στην ανθρώπινη συμπεριφορά.



Εικόνα 3: Κυβερνοχώρος

(*https://el.wikipedia.org/wiki/%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%87%CF%8E%CF%81%CE%BF%CF%82*)

- **Εικονικός κόσμος**

Ο κάθε χρήστης, κακόβουλος ή μη μπορεί να δημιουργήσει μια νέα προσωπικότητα η οποία χτίζεται από τα στοιχεία που δίνει ο ίδιος. Ο χρήστης μπορεί να δημιουργήσει διάφορες ηλεκτρονικές προσωπικότητες, αφού υπάρχει ανωνυμία, με τα χαρακτηριστικά που ο ίδιος επιθυμεί. Η αλληλεπίδραση αυτής της ψεύτικης προσωπικότητας δημιουργεί μια ψευδαίσθηση και αυτό έχεις ως συνέπεια ο χρήστης να ταυτίζει την πραγματική του ζωή με τον εικονικό κόσμο του κυβερνοχώρου.

- **Αλληλεπίδραση**

Είναι ένας χώρος ψυχαγωγίας και κοινωνικής διάδρασης ο οποίος δίνει τη δυνατότητα στους χρήστες μέσω chat, social media, παιχνιδιών κ.α να έρχονται σε επαφή, χρησιμοποιώντας τα εικονικά στοιχεία που έχουν δημιουργήσει, χωρίς κανένα έλεγχο.

Η κοινωνική μηχανική βασίζεται στην λανθασμένη άποψη ότι η διαδικτυακή επικοινωνία αναπτύσσεται μεταξύ χρηστών τους οποίους γνωρίζουμε με βάση τα λεγόμενά τους και όχι με ότι ισχύει στην πραγματικότητα.

- **Πηγή πληροφόρησης**

Οι πληροφορίες είναι άγνωστες σε μεγάλο μέρος του κυβερνοχώρου καθώς τα προσωπικά δεδομένα και πληροφορίες λόγω έλλειψης πολιτικών ασφαλείας, μπορεί να υπάρχουν απροστάτευτες. Αυτές τις πηγές πληροφόρησης εκμεταλλεύονται οι κοινωνικοί μηχανικοί για να οργανώσουν τις επιθέσεις τους (Αναγνωστόπουλος, 2021).

2. ΠΡΑΓΜΑΤΙΚΑ ΠΕΡΙΣΤΑΤΙΚΑ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ

Η ιστορία αποτελεί ένα εξαιρετικό εργαλείο για να μας μάθει ποια πράγματα λειτούργησαν στο παρελθόν καθώς και τον λόγο που συνέβησαν. Μπορεί επίσης, να μας πει που πηγαίνουμε αλλά και πως μπορούμε να φτάσουμε εκεί. Η ιστορία της κοινωνικής μηχανικής δεν διαφέρει πολύ από αυτό. Σε όλη την διάρκεια της ιστορίας των επιχειρήσεων, υπήρξαν άνθρωποι που προσπάθησαν να εξαπατήσουν και να κλέψουν. Αυτό είχε σαν αποτέλεσμα, πολλοί άνθρωποι να αφιερώσουν την ζωή τους για την ασφάλεια ενάντια σε αυτές τις κακές δυνάμεις.
Ο Kevin Mitnick είναι ένας από τους πιο διάσημους κοινωνικούς μηχανικούς, έχοντας καταδικαστεί μεν για ηλεκτρονικά εγκλήματα αλλά με πολλούς να υποστηρίζουν ότι πρόκειται για τον καλύτερο κοινωνικό μηχανικό. Μερικές από τις πιο διάσημες και τολμηρές περιπτώσεις κοινωνικής μηχανικής που έχει εφαρμόσει και περιγράψει στο βιβλίο του «The Art of Human Hacking» θα παρουσιάσουμε στο κεφάλαιο αυτό.

2.1. Περίπτωση 1: Παράνομη Πρόσβαση στο Τμήμα Μηχανοκίνητων Οχημάτων

Το δίπλωμα οδήγησης μπορεί να αποδειχθεί ένα ιδιαίτερα χρήσιμο εργαλείο για την απόκτηση προσωπικών πληροφοριών. Η εξασφάλιση του αριθμού διπλώματος οδήγησης του στόχου, μπορεί να επιτρέψει σε έναν κοινωνικό μηχανικό να αποκτήσει όλες τις προσωπικές του πληροφορίες. Παρόλα αυτά, δεν υπάρχουν δωρεάν υπηρεσίες που επιτρέπουν σε κάποιον να έχει πρόσβαση σε προσωπικά δεδομένα άλλων. Ένας κοινωνικός μηχανικός θα πρέπει να καταβάλει μεγάλη προσπάθεια ώστε να λάβει και να χρησιμοποιήσει τις πληροφορίες αυτές.

Ο Στόχος
Ο Eric ήθελε να χρησιμοποιήσει το Ιδιωτικό Τμήμα Μηχανοκίνητων Οχημάτων καθώς και τα συστήματα της αστυνομίας για να αποκτήσει αριθμούς από διπλώματα οδήγησης διαφόρων ανθρώπων. Αυτό γινόταν συχνά και ο Eric εφάρμοζε μια μέθοδο απόκτησης αυτών των πληροφοριών, αλλά φοβόταν ότι οι επαναλαμβανόμενες κλήσεις του θα αποκάλυπταν την απάτη του ή θα έκαναν την αστυνομία να τον υποπτευτεί. Χρειαζόταν λοιπόν μια διαφορετική μέθοδο απόκτησης προσβασιμότητας στο δίκτυο του Τμήματος Μηχανοκίνητων Οχημάτων και σε συνδυασμό με μερικές γνώσεις που είχε γύρω από τον τρόπο λειτουργίας του συγκεκριμένου τμήματος, θα μπορούσε να συνεχίσει το σχέδιο του. Ο στόχος του ήταν διπλός. Δεν θα τον βοηθούσε μόνο το τμήμα μηχανοκίνητων οχημάτων αλλά και η αστυνομία (χωρίς να το ξέρει φυσικά) στο να αποκτήσει τις πληροφορίες που χρειαζόταν.

Η Ιστορία
Ο Eric ήξερε ότι το Τμήμα Μηχανοκίνητων Οχημάτων μπορούσε να δώσει εμπιστευτικές πληροφορίες σε ασφαλιστικά γραφεία, ιδιωτικούς ερευνητές και άλλες συγκεκριμένες ομάδες. Ο κάθε τομέας έχει πρόσβαση σε συγκεκριμένο είδος πληροφοριών.
Μια ασφαλιστική εταιρεία, παραδείγματος χάριν, έχει πρόσβαση σε διαφορετικές πληροφορίες σε σχέση με ένα ιδιωτικό ερευνητή, ενώ ένας εκπρόσωπος του νόμου μπορεί να αποκτήσει όλα τα είδη πληροφοριών. Ο στόχος του Eric ήταν να αποκτήσει όλες τις πληροφορίες.
Ο Eric ακολούθησε μερικά βήματα που απέδειξαν τις εξαιρετικές του ικανότητες στην κοινωνική μηχανική. Καταρχήν, κάλεσε τις πληροφορίες και ζήτησε τον τηλεφωνικό αριθμό των κεντρικών γραφείων του Τμήματος Μηχανοκίνητων Οχημάτων. Φυσικά,

ο τηλεφωνικός αριθμός που του δόθηκε ήταν για το κοινό, αλλά αυτός επιζητούσε κάτι που θα του επέτρεπε να διεισδύσει σε βάθος.
Στην συνέχεια κάλεσε στο γραφείο του νομικού τμήματος και ζήτησε τον τηλέτυπο, το οποίο είναι το γραφείο που στέλνονται και λαμβάνονται οι επικοινωνίες από άλλα γραφεία. Όταν πήρε στο τμήμα του τηλέτυπου, ζήτησε από τον εκπρόσωπο τον αριθμό στον οποίο καλούσε η αστυνομία όταν ήθελε να επικοινωνήσει με τα κεντρικά γραφεία του Τμήματος Μηχανοκίνητων Οχημάτων. Κάλεσε την αστυνομία και ακολούθησε ο εξής διάλογος :
“Ποιος είστε;” τον ρώτησαν.
Έπρεπε να σκεφτεί γρήγορα και απάντησε,
“Είμαι ο Al. Κάλεσα στο 503-555-5753.”
Αυτό που έκανε ήταν να δώσει ένα τηλεφωνικό αριθμό από την ίδια περιοχή και απλά διάλεξε τυχαία τα τέσσερα τελευταία ψηφία. Στην συνέχεια, απλά σταμάτησε να μιλάει. Ο αστυνομικός όμως έκανε κάποιες δικές του εικασίες: Ήταν εσωτερική κλήση και είχε ήδη τον αριθμό για μια ιδιωτική περιοχή (Τηλέτυπο). Σχεδόν είχε όλο τον αριθμό για το Τμήμα Μηχανοκίνητων Οχημάτων.
Με βάση αυτά τα δύο, ο αστυνομικός υπέθεσε ότι ο Eric είχε άδεια, με αποτέλεσμα να του δώσει τον αριθμό. Ο Eric ήθελε παραπάνω από έναν αριθμό και για να εκπληρώσει τον στόχο του, χρειαζόταν ένα πιο καλά οργανωμένο κόλπο, μια πολύ-επίπεδη και πολύπλευρη επίθεση με διαφορετικούς αποδέκτες.

Πρόσβαση Στο Τηλεφωνικό Σύστημα Της Πολιτείας
Ο Eric κάλεσε στον αριθμό που του έδωσαν για να μπει στο Τμήμα Μηχανοκίνητων Οχημάτων. Στον αντιπρόσωπο που του απάντησε είπε ότι ήταν από την Nortel και ήταν απαραίτητο να μιλήσει με έναν τεχνικό επειδή δούλευε με τον DMS-100, έναν τηλεφωνικό διακόπτη που χρησιμοποιούταν ευρέως.
Όταν κατάφερε να μιλήσει με τον τεχνικό, του είπε ότι τηλεφωνούσε από το Κέντρο Τεχνικής Βοήθειας της Texas Nortel και του εξήγησε ότι προσπαθούσε να αναβαθμίσει όλους τους τηλεφωνικούς διακόπτες. Αυτό μπορούσε να γίνει από μακριά και ο τεχνικός δεν χρειαζόταν να κάνει τίποτα εκτός από του να δώσει τον αριθμό πρόσβασης για τον διακόπτη, έτσι ώστε ο Eric να μπορούσε να κάνει όλες τις ενημερώσεις κατευθείαν από το Κέντρο Τεχνικής Βοήθειας.
Αυτή η ιστορία φάνηκε απολύτως πιστευτή, έτσι ο τεχνικός συναίνεσε, δίνοντας στον Eric όλες τις πληροφορίες που χρειαζόταν. Οπλισμένος τώρα με τις πληροφορίες που ήθελε, μπορούσε να καλέσει κατευθείαν σε έναν από τους τηλεφωνικούς διακόπτες της πολιτείας.

Απόκτηση Κωδικού
Το επόμενο εμπόδιο ήταν αυτό που θα μπορούσε να τον αποκαλύψει, και συνεπώς να καταστρέψει το σχέδιο του. Οι διακόπτες Nortel που χρησιμοποιούσε το Τμήμα Μηχανοκίνητων Οχημάτων προστατεύονταν από κωδικό. Από παλιά εμπειρία που είχε στην χρήση διακοπτών της Nortel, ο Eric γνώριζε ότι η Nortel χρησιμοποιεί ένα προεπιλεγμένο λογαριασμό χρήστη, τον NTAS. Ο Eric κάλεσε λοιπόν αρκετές φορές δοκιμάζοντας κάποιους στάνταρ κωδικούς που είχε συναντήσει:
NTAS—απέτυχε
Account name—απέτυχε
Helper—απέτυχε
Patch—απέτυχε
Update—ΕΠΙΤΥΧΙΑ
Ο κωδικός ήταν η αγγλική λέξη “update”. Τώρα είχε τον πλήρη έλεγχο του διακόπτη και όλων των γραμμών που ήταν συνδεδεμένες σε αυτόν. Αναζήτησε λοιπόν τις τη-

λεφωνικές γραμμές στις οποίες στόχευε. Γρήγορα ανακάλυψε ότι 19 τηλεφωνικές γραμμές πήγαιναν στο ίδιο τμήμα.
Αφού έλεγξε μερικές από τις εσωτερικές ρυθμίσεις στον διακόπτη, ανακάλυψε ότι ο διακόπτης ήταν προγραμματισμένος να ψάχνει ανάμεσα σε 19 τηλεφωνικές γραμμές μέχρι να βρει μια η οποία δεν ήταν απασχολημένη. Επέλεξε την γραμμή 18 και εισήγαγε τον στάνταρ κωδικό προώθησης, και πρόσθεσε μια εντολή για προώθηση κλήσεων σε τηλεφωνική γραμμή της επιλογής του. Στην συνέχεια, ο Eric αγόρασε ένα φτηνό κινητό με προπληρωμένο χρόνο ομιλίας, το οποίο θα μπορούσε να ξεφορτωθεί εύκολα. Εισήγαγε τον αριθμό σαν τον αριθμό προώθησης όταν χτυπούσε η γραμμή 18.
Όταν το Τμήμα Μηχανοκίνητων Οχημάτων ήταν αρκετά απασχολημένο και οι 17 γραμμές ήταν κατειλημμένες , τότε η 18η κλήση δεν θα χτυπούσε στο Τμήμα Μηχανοκίνητων Οχημάτων αλλά στο κινητό του Eric.
Και αυτό δεν άργησε να συμβεί. Γύρω στις 8:00 π.μ. το επόμενο πρωί, το κινητό του άρχισε να χτυπάει. Κάθε φορά, ήταν ένας αστυνομικός ο οποίος προσπαθούσε να μάθει πληροφορίες για ένα άτομο. Έτσι, κατέγραφε τις κλήσεις από την αστυνομία είτε βρισκόταν στο σπίτι του, είτε έξω τρώγοντας μεσημεριανό, είτε στο αυτοκίνητό του, προσποιούμενος πάντα τον εκπρόσωπο του τμήματος μηχανοκίνητων οχημάτων.
Eric :“Τμήμα μηχανοκίνητων οχημάτων, πως μπορώ να σας βοηθήσω;”
“Εδώ Αστυνόμος Andrew Cole.”
“Γεια σου αστυνόμε, τι μπορώ να κάνω για σένα σήμερα;”
“Χρειάζομαι ένα φωνητικό αλγόριθμο (Soundex) για το δίπλωμα οδήγησης 005602789.”
“Φυσικά, να ελέγξω το αρχείο.” Ενώ έκανε ότι δούλευε στον υπολογιστή έκανε μερικές ερωτήσεις: “Αστυνόμε Cole, ποιο είναι το γραφείο σας;”
“Κομητεία Jefferson.”
Ο Eric στην συνέχεια, έκανε τις ακόλουθες ερωτήσεις: “Ποιος είναι ο κωδικός σας;”, “Ποιος είναι ο αριθμός σας στο δίπλωμα οδήγησης;”, “Ποια είναι η ημερομηνία γέννησης σας;”
Καθώς ο αστυνόμος αποκάλυπτε όλες τις προσωπικές πληροφορίες του, ο Eric προσποιούταν ότι τα έλεγχε. Στην συνέχεια, προφασιζόμενος ότι έλαβε επιβεβαίωση ρωτούσε τι λεπτομέρειες ήθελε αυτός που καλούσε. Αφού έκανε ότι έψαχνε το όνομα και τις υπόλοιπες πληροφορίες, στην συνέχεια έλεγε, “Το σύστημα έπεσε πάλι. Συγνώμη αστυνόμε, ο υπολογιστής μου έχει προβλήματα όλη την εβδομάδα. Θα μπορούσατε να καλέσετε και πάλι για να σας εξυπηρετήσει ένας άλλος υπάλληλος;”
Αυτό σίγουρα ήταν εκνευριστικό, για τον αστυνόμο, αλλά δεν κινούσε υποψίες. Στο μεταξύ, ο Eric είχε στην κατοχή του την ταυτότητα του αστυνόμου και μπορούσε να χρησιμοποιήσει αυτές τις πληροφορίες για πολλά πράγματα, αλλά κυρίως να αποκτήσει πληροφορίες από το Τμήμα Μηχανοκίνητων Οχημάτων.
Αφού συγκέντρωσε όλες τις πληροφορίες που ήθελε για λίγες ώρες στην συνέχεια ακύρωσε την προώθηση κλήσεων. Τώρα είχε μια μεγάλη λίστα πληροφοριών στην κατοχή του.
Για αρκετούς μήνες μετά το κόλπο αυτό, ο Eric μπορούσε εύκολα να συλλέξει στοιχεία από διάφορους αστυνομικούς, να ακυρώσει την προώθηση κλήσεων και μετά να χρησιμοποιήσει όλες τις πληροφορίες για να αποκτήσει αριθμούς από διπλώματα τα οποία στην συνέχεια μπορούσε να πουλήσει σε ιδιωτικούς ερευνητές ή άλλα άτομα τα οποία δεν τα ενδιέφερε πως έφτασε σε αυτές τις πληροφορίες.

Εφαρμογή Του Πλαισίου Αυτό-αξιολόγησης Στην Απάτη Στο Τμήμα Μηχανοκίνητων Οχημάτων

Ο Kevin προσδιόρισε κάποια πράγματα και συμπεριφορές του Eric που τον οδήγησαν στην επιτυχία, όπως το γεγονός ότι δεν φοβήθηκε ή ένοιωσε άβολα όταν μιλούσε με την αστυνομία αλλά και το γεγονός ότι βρήκε άκρη σε ένα γενικά άγνωστο περιβάλλον.

Το πρώτο βήμα για μία επιτυχημένη επίθεση κοινωνικής μηχανικής είναι η συγκέντρωση πληροφοριών. Σε αυτή την περίπτωση, ο Eric ήταν προετοιμασμένος πριν την επίθεση. Ήξερε αρκετά για το τηλεφωνικό σύστημα, τον τρόπο που λειτουργεί το Τμήμα Μηχανοκίνητων Οχημάτων και το γενικό πλαίσιο της διαδικασίας στην οποία ήθελε να διεισδύσει. Στις μέρες μας, μια τέτοια επίθεση είναι ακόμα ευκολότερη εξαιτίας του διαδικτύου που αποτελεί πραγματικό χρυσορυχείο πληροφοριών.

Αντιλαμβανόμαστε ότι η επιλογή ενός προσχήματος το οποίο μιμείται αυτό που γίνεται στην πραγματική ζωή, μπορεί να αυξήσει τις πιθανότητες επιτυχία μιας επίθεσης. Η δύναμη έγκειται στο γεγονός ότι το πρόσχημα είναι “ρεαλιστικό” και βοηθάει στην συλλογή των πληροφοριών αλλά και στην παραβίαση του στόχου.

Η εκμαίευση των πληροφοριών ή η ικανότητα δημιουργίας έξυπνων ερωτήσεων για την απόκτηση τους, αποτελεί σημαντικό κομμάτι μιας επιτυχημένης επίθεσης. Ο Eric εκμαίευσε τις πληροφορίες με μεγάλη επιδεξιότητα. Όταν μιλούσε στο τηλέφωνο με την αστυνομία, η μέθοδος εκμαίευσης που χρησιμοποίησε ο Eric ήταν η απόδειξη ότι ήταν αυτός που έλεγε ότι ήταν και ήξερε την “δουλειά” του καλά. Γνώριζε την τεχνική φρασεολογία και έκανε συνηθισμένες ερωτήσεις για τις οποίες περίμενε απαντήσεις. Στην πραγματικότητα, αν δεν έκανε αυτές τις ερωτήσεις, θα προκαλούσε περισσότερες υποψίες. Αυτή είναι η δύναμη μιας καλής τακτικής εκμαίευσης πληροφοριών.

Ο Eric γνώριζε ότι έπρεπε να αποκτήσει συγκεκριμένους τηλεφωνικούς αριθμούς για να εκτελέσει την επίθεση. Αντί να προσπαθήσει να εξηγήσει γιατί χρειαζόταν τις πληροφορίες, χρησιμοποίησε μια υποθετική πρόταση και έκανε ερωτήσεις που βασικά έλεγαν, “Τις δικαιούμαι αυτές τις απαντήσεις τώρα, επομένως απάντησε μου σε αυτό που σε ρωτάω.” Αυτό είναι ένα ακόμα παράδειγμα ισχυρής εκμαίευσης.

Οι περισσότερες επιτυχημένες επιθέσεις περιλαμβάνουν επίσης πολλά προσχήματα. Αυτή η περίπτωση δεν αποτελεί εξαίρεση. Ο Eric έπρεπε να δώσει δικαιολογίες, να κινήσει αρκετά γρανάζια για να πετύχει τους στόχους του. Όσο εντυπωσιακό και αν φαίνεται, ο Eric μιμήθηκε ένα όργανο επιβολής του νόμου, που αποτελεί παράνομη πράξη.

Από την ανάλυση της συμπεριφοράς του Eric σε αυτή την απάτη μπορούμε να διακρίνουμε την ψυχραιμία με την οποία έδρασε. Προσποιούμενος τον εκπρόσωπο του Τμήματος Μηχανοκίνητων Οχημάτων μπόρεσε να χρησιμοποιήσει την τεχνική της εκμαίευσης πληροφοριών σαν απόδειξη για την νομιμότητα των πράξεων του. Όταν χρησιμοποίησε το πρόσχημα της αστυνομίας, η συμπεριφορά του, η φωνή του και οι φράσεις που χρησιμοποίησε υποστήριζαν το πρόσχημα του. Οι δικαιολογίες του Eric ήταν ισχυρές και έκανε εξαιρετική δουλειά στο να κρατήσει την συνοχή τους, ιδιαίτερα όταν χρειάστηκε να υποδυθεί τον εκπρόσωπο του Τμήματος Μηχανοκίνητων Οχημάτων και να απαντήσει σε πραγματικές κλήσεις από την αστυνομία. Σε αρκετές περιπτώσεις θα μπορούσε να την έχει πατήσει, αλλά κατάφερε να μείνει συγκεντρωμένος.

Πολλές από τις τεχνικές που χρησιμοποιούνται για τις ψυχολογικές πλευρές της κοινωνικής μηχανικής, όπως σήματα με τα μάτια και εκφράσεις, δεν χρησιμοποιήθηκαν σε αυτή την επίθεση επειδή έγινε κυρίως μέσω τηλεφώνου.

Ο Eric φαίνεται ότι δεν αντιμετώπισε κανένα πρόβλημα στην δημιουργία καλής σχέσης με το θύμα. Ήταν πειστικός και άνετος, δεν φάνηκε να τον φοβίζει κάτι που θα μπορούσε να πάει στραβά, και μπόρεσε να χτίσει σχέση εμπιστοσύνης. Χρησιμοποί-

ησε την φωνή του και έκανε την συζήτηση με τέτοιο τρόπο που έδινε στον συνομιλητή του ένα καλό λόγο να τον εμπιστευτεί, χωρίς να τον αμφισβητεί.
Ο Eric χρησιμοποίησε επιτυχώς εντυπωσιακές τακτικές ανάκρισης και συζήτησης ακόμα και με εκπροσώπους του νόμου, οι οποίοι έχουν εμπειρία σε κάτι ανάλογο.
Επίσης, ο Eric ήταν εξαιρετικός στην ικανότητα εφαρμογής τακτικών επιρροής. Μία από τις πιο εμφανείς τακτικές επιρροής που χρησιμοποίησε ήταν όταν ζήτησε από τον αστυνομικό να καλέσει ξανά για να μιλήσει με κάποιον άλλο εκπρόσωπο του τμήματος. Αυτό που έκανε την τακτική επιτυχημένη, είναι ότι ο Eric "έδωσε" κάτι στον αστυνομικό πρώτα. Δηλαδή, "επιβεβαίωσε" τις πληροφορίες που χρειαζόταν ο αστυνομικός και όταν χρειάστηκε να δώσει την τελευταία πληροφορία, ο υπολογιστής "κόλλησε" . Με την εφαρμογή μερικών κανόνων επιρροής, ο Eric μπόρεσε εύκολα να γίνει πιστευτός στους αστυνομικούς.
Από τα ανωτέρω, κάποιος μπορεί να υποθέσει ότι ο Eric είτε εξάσκησε τις μεθόδους του, είτε έμαθε όλα όσα θα έπρεπε να ξέρει, για τα εσωτερικά συστήματα που χρησιμοποιήθηκαν στην επίθεση.
Σύμφωνα με τον Kevin Mitnick, ο Eric θα μπορούσε να λάβει μερικές ακόμα προφυλάξεις. Παραδείγματος χάριν, όταν απαντούσε στις κλήσεις του Τμήματος Μηχανοκίνητων Οχημάτων, να είχε βεβαιωθεί ότι είχε προωθήσει τον αριθμό μόνο όταν βρισκόταν στο "γραφείο" του. Θα έπρεπε να έχει ορίσει μια περιοχή για γραφείο, με ήχους από γραφείο και να είχε τον κατάλληλο εξοπλισμό έτσι ώστε να αποφύγει τον κίνδυνο να προδοθεί είτε από τη σερβιτόρα είτε από ένα φίλο του.
Επιπλέον, αν και ένα κινητό τηλέφωνο αποτελεί μια καλή λύση για την αποφυγή εντοπισμού, μια άλλη τεχνική είναι η προώθηση του αριθμού σε έναν αριθμό Google Voice ή Skype. Τίποτα δεν θα μπορούσε να χαλάσει το σχέδιο του εκτός από ένα αδύναμο, γεμάτο παρεμβολές σήμα.

2.2. Περίπτωση 2: Παράνομη Πρόσβαση στον Οργανισμό Κοινωνικής Ασφάλισης

Ο Keith Carter, ένας όχι και τόσο έντιμος ιδιωτικός ερευνητής, προσλήφθηκε να ερευνήσει στοιχεία για έναν άνδρα που έκρυβε χρήματα από τη σύζυγό του λίγο πριν χωρίσουν. Η γυναίκα είχε αρχικά χρηματοδοτήσει το εγχείρημα του άνδρα της, το οποίο εξελίχθηκε σε μια εταιρεία πολλών εκατομμυρίων.
Ενώ η διαδικασία του διαζυγίου ήταν σε εξέλιξη, οι δικηγόροι της γυναίκας προσπαθούσαν να ανακαλύψουν τα κρυφά περιουσιακά στοιχεία. Αυτή είναι μια πολύ ενδιαφέρουσα περίπτωση, επειδή η ιστορία ακολουθεί μια πολύ σκοτεινή μέθοδο για την συγκέντρωση πληροφοριών. Πρόκειται για μια επικίνδυνη απάτη.

Ο Στόχος
Ο στόχος ήταν να βρεθούν τα περιουσιακά στοιχεία του "Joe Johnson," χωρίς αυτός να αποτελεί τον πραγματικό στόχο της επίθεσης. Για την απόκτηση των πληροφοριών του Joe, ο ιδιωτικός ερευνητής, έπρεπε να αποκτήσει παράνομη πρόσβαση στον Οργανισμό Κοινωνικής Ασφάλισης.

Η Ιστορία
Ο Joe Johnson παντρεύτηκε μια πολύ πλούσια γυναίκα. Χρησιμοποίησε πολλές δεκάδες χιλιάδες δολάρια από τον λογαριασμό της για να ολοκληρώσει τις ιδέες του, οι οποίες εξελίχθηκαν σε ένα οργανισμό πολλών εκατομμυρίων δολαρίων.
Με το πέρασμα των χρόνων, η σχέση τους διαταράχθηκε και αποφάσισαν να χωρίσουν. Κατά την διάρκεια των διαδικασιών του διαζυγίου, η κυρία Johnson γνώριζε ότι της έκρυβε χρήματα που προσπαθούσε να τα αφήσει έξω από τον διακανονισμό του διαζυγίου.

Έτσι, προσέλαβε τον Keith, τον ιδιωτικό ερευνητή, ο οποίος δεν ήταν και πολύ έντιμος και δεν είχε αναστολές στο να ξεπεράσει τα όρια του νόμου για να αποκτήσει τις πληροφορίες που χρειαζόταν.
Καθώς ο Keith ανέλυε την υπόθεση, συνειδητοποίησε ότι ένα καλό σημείο για να ξεκινήσει ήταν ο Οργανισμός Κοινωνικής Ασφάλισης. Σκέφτηκε, ότι αν αποκτούσε πρόσβαση στα αρχεία του Joe, θα μπορούσε να ανακαλύψει διαφορές στα εισοδήματά του και τότε θα μπορούσε να επιτύχει την αποστολή του. Επιθυμούσε ελεύθερη επικοινωνία με τις τράπεζες που συνεργαζόταν ο Joe, τις επενδυτικές του εταιρείες καθώς και να έχει πρόσβαση στους offshore λογαριασμούς του, προσποιούμενος ότι είναι ο ίδιος ο Joe. Για να γίνει όμως αυτό εφικτό, χρειαζόταν αναλυτικά στοιχεία, και αυτός είναι ο λόγος που οδηγήθηκε στην απόφαση να αποκτήσει παράνομη πρόσβαση στον Οργανισμό Κοινωνικής Ασφάλισης.
Ο Keith άρχισε να συγκεντρώνει κάποιες βασικές πληροφορίες. Μπήκε στο διαδίκτυο και βρήκε έναν οδηγό που περιέγραφε τα εσωτερικά συστήματα του Οργανισμού Κοινωνικής Ασφάλισης αλλά και τον εσωτερικό κώδικα επικοινωνίας. Αφού τα μελέτησε και έχοντας εξοικειωθεί με την ορολογία, κάλεσε το γραφείο Κοινωνικής Ασφάλισης. Όταν συνδέθηκε με έναν εκπρόσωπο, του ζήτησε να τον συνδέσει με το γραφείο αιτήσεων. Η συζήτηση εξελίχθηκε κάπως έτσι:
“Γεια σας, είμαι ο Gregory Adams, γραφείο περιφέρειας 329. Ακούστε, προσπαθώ να επικοινωνήσω με τον υπάλληλο που διαχειρίζεται έναν λογαριασμό που τελειώνει σε 6363 και το τηλέφωνο που έχω είναι συνδεδεμένο με φαξ.”
“Α, αυτός είναι ο Συντονιστής 3, το τηλέφωνο είναι...”
Σε λίγα μόλις λεπτά, διέθετε τον εσωτερικό τηλεφωνικό αριθμό του γραφείου, ο οποίος δεν ήταν δημόσιος για το κοινό. Στη συνέχεια κάλεσε τον Συντονιστή 3, άλλαξε το πρόσχημα του προσπαθώντας να αποκτήσει χρήσιμες πληροφορίες για τον Joe. Την Πέμπτη το πρωί ο Keith είχε έτοιμο το σχέδιο του και κάλεσε τον Συντονιστή 3:
“Συντονιστής 3: Είμαι η May Linn Wang.”
“Δεσποινίς Wang, είμαι ο Arthur Arondale, από το γραφείο του Γενικού Επιθεωρητή. Μπορώ να σε λέω ‘May’;”
“Είναι ‘May Linn’,” του απάντησε.
“Ωραία, May Linn. Έχουμε έναν καινούριο υπάλληλο που δεν διαθέτει υπολογιστή ακόμα και τώρα έχει αναλάβει μια σημαντική δουλειά και χρησιμοποιεί τον δικό μου. Δουλεύουμε στην κυβέρνηση των Ηνωμένων Πολιτειών αλλά παρόλα αυτά, ο προϋπολογισμός δεν διαθέτει χρήματα για να αγοράσουμε έναν υπολογιστή για αυτό τον τύπο. Και σαν μην έφτανε αυτό, το αφεντικό μου νομίζει ότι αφήνω πίσω την δουλειά μου και δεν θέλει να ακούει δικαιολογίες, πιστεύω καταλαβαίνεις τι εννοώ, σωστά;”
“Καταλαβαίνω απόλυτα.”
“Μπορείς να με βοηθήσεις να κάνω μια γρήγορη αναζήτηση στο MCS;” Ρώτησε, χρησιμοποιώντας το όνομα του συστήματος το οποίο περιέχει στοιχεία όλων των φορολογούμενων.
“Φυσικά, τι χρειάζεστε;”
“Το πρώτο που πρέπει να μάθω είναι ένα “alphadent” για τον Joseph Johnson, με ημερομηνία γέννησης 7/4/69.” (“Alphadent” σημαίνει ότι ο υπολογιστής πρέπει να αναζητήσει ένα λογαριασμό αλφαβητικά με το όνομα του φορολογούμενου, το οποίο συμπληρώνεται με την ημερομηνία γέννησης.)
“Τι πρέπει να μάθετε;”
“Ποιος είναι ο αριθμός Κοινωνικής Ασφάλισης;”
Η May Linn τον έδωσε.
“Εντάξει, τώρα χρειάζομαι ένα “Numident” για τον αριθμό λογαριασμού.” (Το “Numident” είναι παρόμοιο με το “alphadent”, μόνο που είναι αριθμητική αναζήτηση αντί για αλφαβητική). Με τον τρόπο αυτό ζητούσε να του διαβάσει τα βασικά στοιχεία του φορολογούμενου και η May Linn του έδωσε τον τόπο γέννησης του φορολογούμενου, το όνομα της μητέρας του και το όνομα του πατέρα του.

Ο Keith στην συνέχεια ζήτησε ένα “DEQY” (συντομογραφία για λεπτομερές ερώτημα για έσοδα)
“Για ποια χρονιά;”
“Έτος 2001.”
Η May Linn είπε, “Το ποσό ήταν $190.286
“Κάποια άλλη πληρωμή;”
“Όχι.”
“Σε ευχαριστώ,” είπε ο Keith. “Ήσουν πολύ εξυπηρετική.”
Ο Keith στην συνέχεια κανόνισε να της τηλεφωνεί όποτε χρειαζόταν πληροφορίες και “δεν είχε πρόσβαση στο υπολογιστή του,” χρησιμοποιώντας ένα τρικ των κοινωνικών μηχανικών, οι οποίοι προσπαθούν να δημιουργήσουν ένα δέσιμο, ώστε να μπορούν να επικοινωνούν το ίδιο άτομο, αποφεύγοντας να επαναλαμβάνουν όλη την διαδικασία κάθε φορά.
“Όχι την επόμενη εβδομάδα,” του είπε, επειδή θα πήγαινε στο Kentucky για τον γάμο της αδερφής της. Μετά από αυτό θα μπορούσε να τον εξυπηρετήσει και πάλι.
Σε αυτό το σημείο φαίνεται ότι το παιχνίδι τελείωσε. Ο Keith είχε όλες τις πληροφορίες που ήθελε και μπορούσε πλέον να τηλεφωνεί στις τράπεζες. Μια καλά εκτελεσμένη και πραγματικά εντυπωσιακή επίθεση.

Εφαρμογή Του Πλαισίου Αυτό-αξιολόγησης Στην Απάτη Στον Οργανισμό Κοινωνικής Ασφάλισης

Ο Keith ξεκίνησε την επίθεση με την συγκέντρωση πληροφοριών αποδεικνύοντας πως η απόκτηση των πληροφοριών είναι πραγματικά η βάση για μια καλή επίθεση κοινωνικής μηχανικής— όσες περισσότερες, τόσο το καλύτερο.
Ο Keith αρχικά ανακάλυψε πολλές χρήσιμες πληροφορίες μέσω ενός διαδικτυακού εγχειριδίου για Προγραμματιστικές Λειτουργίες του Οργανισμού Κοινωνικής Ασφάλισης που περιείχε συντομογραφίες, οδηγίες αλλά και τι επιτρέπεται να πουν οι υπάλληλοι του σε ένα όργανο επιβολής του νόμου.
Οπλισμένος με αυτές τις πληροφορίες, ο Keith γνώριζε τι να ζητήσει και πώς, χωρίς να κινήσει υποψίες.
Αν και ο σύνδεσμος του έδωσε αρκετές πληροφορίες, αποφάσισε να προχωρήσει ένα βήμα παραπέρα, χρησιμοποιώντας το πρόσχημα ότι είναι υπάλληλος από το γραφείο του Γενικού Επιθεωρητή. Πραγματικά, σκέφτηκε αντισυμβατικά, χρησιμοποιώντας το τοπικό γραφείο για να αποκτήσει τους εσωτερικούς αριθμούς που χρειαζόταν για να ολοκληρώσει το σχέδιο του.
Ο Keith χρησιμοποίησε διαφορετικά προσχήματα με αριστοτεχνικό τρόπο. Μπόρεσε να αποκτήσει πολλές πληροφορίες που χρειαζόταν, χρησιμοποιώντας το διαδικτυακό εγχειρίδιο του Οργανισμού Κοινωνικής Ασφάλισης, έτσι ώστε να θέσει τις σωστές ερωτήσεις. Αυτό το εγχειρίδιο αποδείχτηκε ιδανικό για την εκμαίευση πληροφοριών. Χρησιμοποιώντας τις κατάλληλες λέξεις και ορολογία, ακουγόταν σαν πραγματικός εργαζόμενος. Χρησιμοποίησε πολλές τακτικές επιρροής, έτσι ώστε να βεβαιωθεί ότι ο στόχος ένοιωθε άνετα. Δημιούργησε καλή σχέση και έδειξε ότι είχε εξασκηθεί καλά στις τεχνικές αυτές.
Για παράδειγμα, συνδύασε την υποχρέωση και την αμοιβαιότητα με περίτεχνο τρόπο. Όταν μπόρεσε να πάρει με το μέρος του την May Linn, περιγράφοντας της την έλλειψη χρήσιμων εργαλείων και υποστήριξης από το γραφείο του, αυτή ένοιωσε υποχρεωμένη να τον βοηθήσει. Επίσης χρησιμοποίησε λέξεις κλειδιά και φράσεις, όπως το “το αφεντικό μου δεν είναι χαρούμενο μαζί μου,” το οποίο αποτελεί ένδειξη ότι έχει προβλήματα και η υπάλληλος του Οργανισμού Κοινωνικής Ασφάλισης, η May Linn, μπορεί να τον σώσει. Οι άνθρωποι νοιώθουν ότι έχουν την ηθική υποχρέωση να βοηθούν αυτούς που έχουν ανάγκη. Λίγοι θα απομακρυνθούν από κάποιον που έχει ανάγκη και η May Linn δεν μπόρεσε να το κάνει. Ένοιωσε υποχρεωμένη όχι μόνο να βοηθήσει αλλά και να ενημερώσει τον Keith για το προσωπικό της πρόγραμμα.

Στο τέλος, ο Keith χρησιμοποίησε αρκετές ικανότητες οι οποίες δεν περιλαμβάνουν την προσωπική παρουσία του ατόμου που συμμετέχει. Είναι γεγονός ότι τα κυβερνητικά συστήματα λειτουργούν από άτομα που είναι ευάλωτα σε μεθόδους παράνομης πρόσβασης. Αυτό, βέβαια δεν αποτελεί επιχείρημα υπέρ της εφεύρεσης ρομποτικών ή υπολογιστικών συστημάτων για την εκτέλεση αυτών των εργασιών, απλά τονίζει το γεγονός ότι πολλά από αυτά τα συστήματα βασίζονται σε μεγάλο βαθμό σε άτομα που έχουν κάνει υπερωρίες, δεν έχουν πληρωθεί καλά ή δέχονται μεγάλη πίεση και η χειραγώγηση τους δεν είναι και πολύ δύσκολη δουλειά.
Η συγκεκριμένη επίθεση, δείχνει πόσο ευάλωτα είναι τα συστήματα πάνω στα οποία βασίζονται οι άνθρωποι.

2.3. Περίπτωση 3: Ο Διευθύνων Σύμβουλος με την υπέρμετρη αυτοπεποίθηση

Η επίθεση κοινωνικής μηχανικής σε διευθύνοντα σύμβουλο με υπέρμετρη αυτοπεποίθηση αποτελεί μια πολύ ενδιαφέρουσα περίπτωση επειδή το εν λόγω άτομο πίστευε ότι δεν μπορούσε να πέσει θύμα μιας τέτοιας προσπάθειας κοινωνικής μηχανικής για δύο λόγους: Πρώτον, δεν χρησιμοποιούσε ιδιαίτερα την τεχνολογία στην προσωπική του ζωή και δεύτερον, πίστευε ότι ήταν πολύ έξυπνος και προστατευμένος απέναντι σε κάτι που αποκαλούσε “ανόητα παιχνίδια.”

Ο Στόχος
Ο στόχος ήταν μια αρκετά μεγάλη εταιρεία εκτυπώσεων στις ΗΠΑ, η οποία είχε μπει στο στόχαστρο των ανταγωνιστών της .
Το Τμήμα IT και ασφάλειας συνειδητοποίησε ότι η εταιρεία είχε αδυναμίες και ενημέρωσε τον διευθύνοντα σύμβουλο ότι ήταν απαραίτητος ένας έλεγχος. Ο διευθύνων σύμβουλος υποστήριζε ότι η προσπάθεια να χακάρει κάποιος την εταιρεία του ήταν σχεδόν αδύνατη επειδή προστάτευε τα μυστικά του όσο καλύτερα μπορούσε. Ισχυριζόταν μάλιστα, ότι ούτε οι στενοί του συνεργάτες γνώριζαν πολλές λεπτομέρειες.
Ο Kevin έπρεπε να διεισδύσει στην εταιρεία και να αποκτήσει πρόσβαση στον server ώστε να συλλέξει τις απαραίτητες πληροφορίες. Η δυσκολία ήταν ότι οι κωδικοί του server ήταν αποθηκευμένοι στον προσωπικό υπολογιστή του διευθύνοντα συμβούλου και κανένας δεν είχε πρόσβαση σε αυτόν, ούτε το προσωπικό ασφαλείας, χωρίς την άδεια του.

Η Ιστορία
Ο διευθύνων σύμβουλος ήταν ενημερωμένος και περίμενε την προσπάθεια του Kevin, αυτό αποτελούσε μεγάλη πρόκληση για τον κοινωνικό μηχανικό.
Ο Kevin ξεκίνησε λοιπόν όπως κάθε φορά με την συλλογή πληροφοριών. Έκανε μια έρευνα για την εταιρεία χρησιμοποιώντας πηγές από το διαδίκτυο και άλλα εργαλεία. Με αυτό τον τρόπο μπόρεσε να συλλέξει πληροφορίες όπως η τοποθεσία των server, διευθύνσεις IP, διευθύνσεις e-mail, τηλεφωνικούς αριθμούς, ταχυδρομικούς κωδικούς, ονόματα και τίτλους υπαλλήλων και πολλά άλλα.
Φυσικά, κατέγραψε όλες αυτές τις πληροφορίες με τέτοιο τρόπο ώστε να μπορεί να τις χρησιμοποιήσει αργότερα. Κατά την διάρκεια της έρευνας παρατήρησε ότι η δομή του email ήταν συγκεκριμένη, όνομα.επώνυμο@εταιρεία.com. Δεν μπορούσε να εντοπίσει την διεύθυνση του e-mail του διευθύνοντα συμβούλου, αλλά πολλά άρθρα είχαν το όνομα του και τον τίτλο του (Charles Jones). Αυτή ήταν μια πληροφορία που ένας συνηθισμένος, χωρίς ιδιαίτερες γνώσεις χάκερ θα μπορούσε να αποκτήσει.
Χρησιμοποιώντας λοιπόν την μορφή όνομα.επώνυμο@εταιρεία, προσπάθησε να στείλει ένα e-mail, δίχως αποτέλεσμα. Στην αρχή απογοητεύτηκε, επειδή ήταν σίγου-

ρος ότι η μέθοδος του e-mail θα του έδινε αρκετές πληροφορίες. Στην συνέχεια αποφάσισε να χρησιμοποιήσει ένα ψευδώνυμο για τον Charles, και δοκίμασε το chuck.jones@εταιρεία.com. Η απόπειρα στέφθηκε με επιτυχία. Μόλις είχε αποκτήσει μια έγκυρη διεύθυνση e-mail.
Τώρα έπρεπε να εξακριβώσει ότι επρόκειτο για το email του διευθύνοντα συμβούλου και όχι κάποιου άλλου με το ίδιο όνομα. Αφιέρωσε χρόνο στο Google καθώς και στο Maltego, προσπαθώντας να συγκεντρώσει όσες περισσότερες πληροφορίες μπορούσε. Το Maltego ήταν ένα εξαιρετικό εργαλείο που επέτρεπε την αναζήτηση ενός domain για οποιαδήποτε αρχεία ήταν ορατά σε μια συνηθισμένη μηχανή αναζήτησης. Έκανε λοιπόν την αναζήτηση στο domain της εταιρείας και βρήκε πολλά αρχεία. Το Maltego προσέφερε τη δυνατότητα εκτός από την παροχή των ονομάτων και άλλων πληροφοριών σχετικά με ημερομηνίες, δημιουργούς και λοιπά στοιχεία των αρχείων. Η εκτέλεση αυτής της λειτουργίας του Maltego έδειξε ότι τα περισσότερα από αυτά τα αρχεία δημιουργήθηκαν από κάποιον “Chuck Jones” και το περιεχόμενο τους αναφερόταν σε αυτόν σαν τον διευθύνοντα σύμβουλο της εταιρείας.
Κατά την διάρκεια της αναζήτησης ένα συγκεκριμένο αρχείο με τίτλο InvoiceApril.xls τράβηξε την προσοχή του Kevin. Μόλις το άνοιξε ανακάλυψε ότι ήταν ένα τιμολόγιο από μια τοπική τράπεζα για ένα διαφημιστικό εγχείρημα στο οποίο συμμετείχε ο Chuck. Το όνομα της τράπεζας, η ημερομηνία και το ποσό περιλαμβάνονταν στο αρχείο εκτός από το συμβάν στο οποίο είχε συμμετάσχει η εταιρεία.
Κάνοντας μια γρήγορη αναζήτηση στην ιστοσελίδα της τράπεζας δεν κατάφερε να βρει περισσότερες πληροφορίες επειδή το συμβάν είχε γίνει έξι μήνες πριν και δεν βρισκόταν πλέον στην λίστα. Αποφάσισε να καλέσει έναν εκπρόσωπο του τμήματος μάρκετινγκ της τράπεζας:
“Γεια σας, είμαι ο Tom από την (Όνομα Εταιρείας). Προσπαθώ να οργανώσω τα βιβλία μας και βλέπω ένα τιμολόγιο από τον Απρίλιο αξίας $3.500 σαν πακέτο χρηματοδότησης. Δεν βλέπω το όνομα του συμβάντος μπορείτε να μου πείτε σας παρακαλώ τι αφορά αυτό το τιμολόγιο;”
“Βεβαίως, Tom,” απάντησε η υπάλληλος.
“Βλέπω ότι αποτελεί την ετήσια χρηματοδότηση της τράπεζας στο Ίδρυμα ενάντια στον παιδικό καρκίνο.”
“Ευχαριστώ πολύ, είμαι νέος εδώ και εκτιμώ την βοήθεια σου. Τα λέμε αργότερα.”
Άρχισε λοιπόν να σχεδιάζει μια πιθανή επίθεση συλλέγοντας όσα περισσότερα στοιχεία , πριν πραγματοποιήσει το τηλεφώνημα στο ίδρυμα.
Βρήκε αρκετά άρθρα στο διαδίκτυο για το συγκεκριμένο ίδρυμα καθώς και πολλές εταιρείες που το στήριζαν οικονομικά έτσι ώστε να κάνει έρευνες για την θεραπεία του καρκίνου.
Επίσης, όσο περισσότερο έψαχνε για τον διευθύνοντα σύμβουλο, τόσες περισσότερες πληροφορίες συγκέντρωνε. Βρήκε το όνομα των γονιών του, εικόνες των παιδιών του στο Facebook, την εκκλησία στην οποία πήγαινε όταν ζούσε κοντά στους γονείς του, μια κριτική που έγραψε για το αγαπημένο του εστιατόριο, την αγαπημένη του ομάδα, την αγαπημένη ομάδα του μεγαλύτερου γιου του, το πανεπιστήμιο που σπούδασε, σε ποιο σχολείο φοιτούν τα παιδιά του και πολλά άλλα. Θέλοντας να εξακριβώσει τον λόγο που η εταιρία χρηματοδοτούσε το ίδρυμα, έκανε ένα τηλεφώνημα στην διευθύντρια του τμήματος marketing της εταιρείας:
“Γεια σας, είμαι ο Tom από το XYZ. Το κατάστημα της First National Bank στην περιοχή με προσέλαβε για να τηλεφωνήσω σε όλους όσους συμμετείχαν στην χρηματοδότηση του Ιδρύματος ενάντια στον παιδικό καρκίνο για τον μήνα Απρίλιο και αναρωτιόμουν αν θα μπορούσα να σας απασχολήσω μερικά λεπτά για να μου πείτε την γνώμη σας;”
“Φυσικά,” είπε η Sue, η διευθύντρια του τμήματος marketing.
“Sue, πιστεύετε ότι η διαφήμιση που αποκομίσατε άξιζε τα χρήματα που πληρώσατε;”

“Λοιπόν, αυτό είναι κάτι που κάνουμε κάθε χρόνο και απασχολεί τον τύπο της περιοχής μας. Πιστεύω ότι δεν θα είχαμε πρόβλημα αν βλέπαμε περισσότερες παροχές.”
“Τέλεια, θα το σημειώσω. Κάθε χρόνο — ναι, το βλέπω ότι το κάνετε κάθε χρόνο. Αναρωτιέμαι, γιατί επιλέξατε αυτό το ίδρυμα όταν υπάρχουν τόσα πολλά διαθέσιμα?”
“Ξέρω ότι ο Chuck πάντα προτιμούσε αυτό. Είναι ο διευθύνων σύμβουλος και νομίζω ότι κάποιος στην οικογένεια του πάλεψε με τον καρκίνο.”
“Λυπάμαι που το ακούω αυτό. Δεν πιστεύω να είναι ένα από τα παιδιά του;”
“Όχι. Νομίζω ένας ανιψιός ή ξάδερφος του. Δεν το έχουμε συζητήσει ποτέ.”
“Λοιπόν, σίγουρα εκτιμούμε τη στήριξη και τις δωρεές σας.”
Τελείωσε με μερικές ακόμα ερωτήσεις και το άφησε έτσι, ευχαριστώντας την για τον χρόνο που του αφιέρωσε.
Πήρε τις πληροφορίες που ήθελε, δεν ήταν ένα από τα παιδιά του που είχε καρκίνο, αν και γνώριζε ότι αυτό δεν θα σταματούσε έναν κακόβουλο κοινωνικό μηχανικό να διαπράξει την επίθεση. Διαθέτοντάς όλες τις πληροφορίες, ήταν έτοιμος να σχεδιάσει την επίθεσή του.
Γνώριζε ότι ο Διευθύνων Σύμβουλος είχε καταγωγή από την Νέα Υόρκη και το αγαπημένο του εστιατόριο ήταν το Domingoes. Πήγαινε τα παιδιά του εκεί συχνά μετά από αγώνα των Mets και έτρωγαν. Μάλιστα είχε γράψει μερικές κριτικές για αυτό το μέρος και είχε σχολιάσει τρία αγαπημένα του πιάτα. Ήξερε επίσης ότι οι γονείς του ζούσαν ακόμα εκεί κοντά και τους επισκεπτόταν συχνά με βάση αυτά που έγραφε στο Facebook.
Σχεδίασε την επίθεση του ως ένα ίδρυμα που συγκεντρώνει χρήματα για έρευνα ενάντια στον καρκίνο. Επρόκειτο για ένα ίδρυμα της ευρύτερης περιοχής και έναντι μιας μικρής δωρεάς θα συμμετείχε σε μια κλήρωση. Το δώρο από την κλήρωση θα ήταν δύο εισιτήρια για ένα αγώνα των Mets και κουπόνια για τρία εστιατόρια, ένα εκ των οποίων ήταν το Domingoes.
Θα προσποιούταν ότι τηλεφωνούσε από την Νέα Υόρκη, αλλά ήταν σχετικά καινούριος εκεί και δεν ήξερε πολλά πράγματα, σε περίπτωση που τον ρωτούσε κάτι που δεν γνώριζε. Ο απώτερος σκοπός του ήταν να δεχτεί ο διευθύνων σύμβουλος ένα αρχείο PDF κακόβουλου περιεχομένου, που θα του προσέφερε κάλυψη ώστε να αποκτήσει πρόσβαση στον υπολογιστή του Charles. Αν δεν χρησιμοποιούσε μια έκδοση του Adobe που θα του επέτρεπε την πρόσβαση, θα έπρεπε να τον πείσει να κατεβάσει ένα αρχείο zip και να εκτελέσει ένα αρχείο EXE το οποίο θα είχε ενσωματωμένο το κακόβουλο λογισμικό.
Έκανε πρόβα την τηλεφωνική συνομιλία και το πρόσχημα του, δοκίμασε τα αρχεία PDF και EXE και είχε ανοιχτό το Google Maps για να εντοπίσει την τοποθεσία του Domingoes. Αφού ετοίμασε τον υπολογιστή του ώστε να είναι έτοιμος να λάβει την πληρωμή, πραγματοποίησε την κλήση.
Έκανε το τηλεφώνημα γύρω στις 4:00 μ.μ., επειδή έμαθε από την ιστοσελίδα της εταιρείας ότι το γραφείο κλείνει στις 4:30μμ. Επειδή δεν ήταν στην αρχική τηλεφωνική συνάντηση για το στήσιμο αυτού του ελέγχου, (ήταν ο συνέταιρος του Kevin), ο Διευθύνων Σύμβουλος δεν θα αναγνώριζε την φωνή του.
“Γεια σας, μήπως είναι διαθέσιμος ο Κύριος Charles Jones;”
“Φυσικά, μισό λεπτό.”
“Γεια σας, εδώ Chuck.”
“Γεια σας κύριε Jones, το όνομα μου είναι Tony και τηλεφωνώ από το Ινστιτούτο Ερευνών ενάντια στον καρκίνο. Διοργανώνουμε ένα ετήσιο έρανο στήριξης στην έρευνα που κάνουμε ενάντια στον καρκίνο που βασανίζει άνδρες, γυναίκες και παιδιά.”
“Σε παρακαλώ να με λες Chuck”.
Αυτό ήταν ένα καλό σημάδι επειδή δεν του είπε κάποια δικαιολογία ή προσπάθησε να κλείσει λέγοντας ότι ήταν απασχολημένος και από μόνος του έκανε την συζήτηση πιο φιλική.

“Σε ευχαριστώ Chuck. Διοργανώνουμε έναν έρανο από εταιρείες που στήριξαν στο παρελθόν ιδρύματα ενάντια στον καρκίνο και σας ζητάμε μια μικρή δωρεά της τάξης των $50–$150 δολαρίων. Το καλό είναι ότι όλοι όσοι βοηθήσουν θα μπουν σε μια κλήρωση για δύο μεγάλα βραβεία. Αν κερδίσεις, θα λάβεις δύο εισιτήρια για ένα παιχνίδι των Mets στην Νέα Υόρκη και ένα δωρεάν γεύμα για δύο σε ένα από τα τρία εξαιρετικά εστιατόρια που έχουμε επιλέξει. Θα υπάρξουν πέντε νικητές.”
“Αγώνας των Mets, αλήθεια;”
“Καταλαβαίνω, αν δεν σου αρέσει το βραβείο των Mets, ίσως σε ενδιαφέρουν τα εστιατόρια που είναι πολύ καλά.”
“Όχι, όχι, λατρεύω τους Mets, για αυτό το είπα. Ήταν επιφώνημα χαράς.”
“Σκέψου λοιπόν ότι όχι μόνο βοηθάς την έρευνα ενάντια στον καρκίνο αλλά μπορεί να κερδίσεις και εισιτήρια για ένα αγώνα και μετά μπορείς να φας στο Morton’s, το Basil’s, ή το Domingoes.”
“Το Domingoes! Πλάκα κάνεις! Το λατρεύω αυτό το μέρος.”
“Ναι, είναι εξαιρετικό. Πήγα εκεί τις προάλλες και έφαγα κοτόπουλο Portabella. Ήταν απίστευτο.” Αυτό ήταν το τρίτο πιο αγαπημένο πιάτο του Charles.
“Αν σου άρεσε αυτό, θα πρέπει να δοκιμάσεις και το Fra Diablo. Είναι το καλύτερο πιάτο εκεί. Το τρώω συνέχεια.”
“Θα πάω ξανά το Σαββατοκύριακο οπότε θα το δοκιμάσω. Σε ευχαριστώ για την συμβουλή. Ξέρω ότι είναι αργά. Τώρα δεν ζητάω χρήματα, δεν μπορώ να τα πάρω άλλωστε από το τηλέφωνο. Αυτό που μπορώ να κάνω είναι να σου στείλω ένα PDF. Εσύ μπορείς να το ελέγξεις με την ησυχία σου και αν ενδιαφέρεσαι μπορείς να μου στείλεις με email την επιταγή και την αίτηση.”
“Ναι, μπορείς να μου το στείλεις.”
“Ωραία, απλά μερικές ερωτήσεις. Ποιο είναι το e-mail σου;”
“chuck.jones@εταιρεία.com.”
“Αν μπορείς, άνοιξε το πρόγραμμα για PDF που διαθέτεις και πες μου ποια έκδοση χρησιμοποιείς, σε παρακαλώ.”
“Ένα λεπτό. Είναι η 8.04.”
“Τέλεια, δεν θέλω να σου στείλω μια έκδοση που δεν μπορείς να ανοίξεις. Ένα λεπτό μόνο να στο στείλω ενώ είμαστε στο τηλέφωνο – ωραία έφυγε.”
“Τέλεια, ευχαριστώ. Ελπίζω να κερδίσω. Λατρεύω αυτό το μέρος.”
“Το ξέρω, το φαγητό είναι εξαιρετικό. Πριν κλείσουμε, μπορείς να δεις αν πήρες το e-mail κα μπορείς να το ανοίξεις;”
“Φυσικά, θα κλείσουμε σε πέντε λεπτά, αλλά μπορώ να ελέγξω. Ναι είναι εδώ.”
Όταν άκουσε το διπλό κλικ, ο Kevin κοίταξε το BackTrack του υπολογιστή του και είδε τον συλλέκτη κακόβουλου λογισμικού, το Meterpreter , να ανταποκρίνεται. Το Meterpreter άλλαξε τη μορφή σε κάτι σαν Explorer.exe.
Ο Chuck τότε είπε, “Χμμ, είναι μια κενή οθόνη. Δεν κάνει τίποτα.”
“Αλήθεια; Αυτό είναι περίεργο. Για να δω.” Αυτό που έλεγχε ήταν να είχε πρόσβαση στον σκληρό δίσκο του και την ικανότητα να ανεβάσει ένα λογισμικό που θα μπορούσε να τρέξει αν έκλεινε ο υπολογιστής. Του είπε, “Λυπάμαι, δεν ξέρω τι έγινε. Μπορείς να μου δώσεις ένα λεπτό ή πρέπει να φύγεις;”
“Πρέπει να πάω την κούπα μου στην κουζίνα, οπότε θα αφήσω το τηλέφωνο ανοιχτό και θα επιστρέψω σε ένα λεπτό.”
“Τέλεια, ευχαριστώ.” Ήταν αυτό που χρειαζόταν για να βεβαιωθεί ότι είχε απεριόριστη και συνεχή πρόσβαση στον υπολογιστή του διευθύνοντα συμβούλου.
“Ήρθα.”
“Λοιπόν, Chuck, πραγματικά ντρέπομαι αλλά δεν ξέρω τι έγινε. Δεν θέλω να σε καθυστερώ, οπότε μπορούμε να κλείσουμε και θα στο στείλω όταν έχω ένα άλλο PDF. Μπορούμε να ξαναμιλήσουμε την Δευτέρα.”
“Εντάξει, κανένα πρόβλημα. Καλό σαββατοκύριακο.”
“Επίσης,Chuck.”

Κλείνοντας το τηλέφωνο προς μεγάλη του έκπληξη και χαρά ο υπολογιστής παρέμεινε ενεργός. Είχε τα πάντα σε έναν ασφαλή δίσκο που μόνο αυτός είχε πρόσβαση. Γρήγορα κατέβασε αυτά τα έγγραφα και μέσα σε λίγες ώρες είχε πρόσβαση στους server. Εκτύπωσε όλες τις εσωτερικές διαδικασίες.
Επικοινώνησαν τη Δευτέρα, αλλά όχι ως Tony από τον έρανο, αλλά ως ο σύμβουλος ασφαλείας που είχε στη διάθεσή του εκτυπωμένα τα “μυστικά”, τους κωδικούς και τις ηχογραφημένες κλήσεις που έγιναν σε Charles και το προσωπικό του .
Αυτή, η πρώτη συνάντηση μετά από μια επιτυχημένη επίθεση περιλαμβάνει πάντα το αρχικό σοκ του πελάτη αλλά και τον ισχυρισμό του ότι χρησιμοποιήθηκαν κακές τακτικές και εκμεταλλεύτηκαν προσωπικές του αδυναμίες. Εξηγώντας ότι οι χάκερ θα ακολουθήσουν τις ίδιες τακτικές, ο εκνευρισμός γίνεται φόβος και ο φόβος στην συνέχεια μετατρέπεται σε κατανόηση.

Εφαρμογή του Πλαισίου Αυτό-Αξιολόγησης στην Απάτη στον Διευθύνοντα Σύμβουλο με την Υπέρμετρη Αυτοπεποίθηση

Όπως πάντα, η συλλογή πληροφοριών είναι το κλειδί για οποιαδήποτε προσπάθεια κοινωνικής μηχανικής, και αυτή η ιστορία το αποδεικνύει περίτρανα. Η συλλογή πληροφοριών από πολλές πηγές (διαδίκτυο, Maltego, μέσα κοινωνικής δικτύωσης, κλπ.) είναι αυτό έκανε την επίθεση επιτυχημένη. Η έλλειψη πληροφοριών θα μπορούσε να οδηγήσει σε αποτυχία.
Η κατάλληλη και επαρκής πληροφόρηση κάνει την διαφορά, και αυτό περιλαμβάνει ακόμα και πληροφορίες που δεν αποδείχτηκαν χρήσιμες, όπως η εκκλησία, τα ονόματα των γονιών και των παιδιών του. Αυτά θα ήταν χρήσιμα σε περίπτωση που τα χρειαζόταν, αλλά αυτό που αποδείχτηκε πολύτιμο ήταν η δομή του email και ότι για τα αρχεία των server χρησιμοποιούσε το Maltego. Αυτό ήταν το κλειδί για να μπει στην επιχείρηση αυτή. Η οργάνωση των πληροφοριών είναι εξίσου σημαντική με την συλλογή και την χρήση τους.
Η σκέψη και η συμπεριφορά του συμβούλου σαν πραγματικού θύτη— αναφορικά με τον τρόπο αναζήτησης και εκμετάλλευσης των αδυναμιών και την επιθυμιών του στόχου— δεν αποτελεί το καλύτερο μέρος της δουλειάς, αλλά ως επαγγελματίας ελεγκτής πρέπει να προστατεύσει τον πελάτη και να του αποδείξει πόσο ευάλωτος είναι σε επιθέσεις. Όσες περισσότερες πληροφορίες συλλέγει τόσο ευκολότερο είναι να βρει αδυναμίες.
Η ανάπτυξη ρεαλιστικών προσχημάτων και θεμάτων, τα οποία θα έχουν μέγιστη επίδραση, συμβάλει επίσης στην επιτυχία της επίθεσης. Κάποιος θα πρέπει να βρει στοχευμένες ερωτήσεις και λέξεις κλειδιά που θα προσελκύσουν τον στόχο. Συλλέγοντας πολλές πληροφορίες, μπορεί να δημιουργηθεί ένα πλαίσιο που συμπεριλαμβάνει λέξεις κλειδιά και νευρο-γλωσσολογικές λέξεις, που μπορεί να χρησιμοποιηθεί στις τακτικές επιρροής του θύτη ώστε να διασφαλίσει την επιτυχία του.
Κάθε φορά έπρεπε να σχεδιάζει προσεκτικά το πρόσχημα, να μπαίνει στον κάθε χαρακτήρα και να τον μιμείται με επιτυχία. Αυτό, φυσικά, χρειαζόταν μεγάλη προετοιμασία για να βεβαιωθεί ότι το πρόσχημα θα γινόταν πιστευτό, θα κυλούσε ομαλά και θα είχε λογική. Επιπλέον, πριν την επίθεση, έπρεπε να διασφαλίσει ότι τα PDF δούλευαν και το εγχείρημα έβγαζε νόημα. Η σημασία της εξάσκησης δεν πρέπει να υποτιμηθεί. Η εξάσκηση επιτρέπει την εξακρίβωση των αποτελεσματικών τακτικών.
Όπως διαπίστωσε εκ των υστέρων ο Kevin, υπήρχαν μερικές βελτιώσεις στο σχέδιο του που θα έκαναν την επίθεση πολύ πιο αποτελεσματική. Καταρχήν, είναι πάντα ριψοκίνδυνο να βασίζεσαι σε ένα κακόβουλο PDF. Θα έπρεπε να έχει δημιουργήσει μια μικρή ιστοσελίδα που μιμείται μια πραγματική ιστοσελίδα έρευνας για τον καρκίνο, και φυσικά να είχε και το PDF εκεί. Τόσο η ιστοσελίδα αλλά και το PDF θα

μπορούσαν να είναι κακόβουλα. Αυτό θα διπλασίαζε τις πιθανότητες του για επιτυχία και θα του έδινε ένα εναλλακτικό σχέδιο σε περίπτωση που κάτι αποτύγχανε.
Ένα ακόμα ρίσκο που πήρε ήταν όταν ο Διευθύνων Σύμβουλος έπρεπε να αφήσει τον υπολογιστή του ανοικτό όταν θα έφευγε από το γραφείο. Αν δεν το έκανε, θα έπρεπε να περιμένει μέχρι την Δευτέρα για να προσπαθήσει για να αποκτήσει πρόσβαση. Για να παραμείνει ο διευθύνων σύμβουλος στον υπολογιστή του, έπρεπε να έχει ένα "πραγματικό PDF" με πληροφορίες τις οποίες θα μπορούσε να διαβάσει και το οποίο θα έστελνε, αφού λειτουργούσε το κακόβουλο PDF, για να εκμεταλλευτεί το μηχάνημα του.
Ο έλεγχος διήρκησε περίπου μια εβδομάδα ώστε να ερευνήσει, συγκεντρώσει και οργανώσει τις πληροφορίες, να κάνει εξάσκηση και τέλος να πραγματοποιήσει την επίθεση του. Σε μια εβδομάδα, τα μυστικά αυτής της εταιρείας θα μπορούσαν να πέσουν στα χέρια των ανταγωνιστών της ή σε κάποιο άλλο άτομο.

2.4. Περίπτωση 4 :Το Σκάνδαλο Στο Θεματικό Πάρκο

Η περίπτωση με το σκάνδαλο στο θεματικό πάρκο είναι αρκετά ενδιαφέρουσα εξαιτίας της φύσης της επιχείρησης και η επιτυχία μιας τέτοιας επίθεσης θα μπορούσε να δώσει στον κοινωνικό μηχανικό την πρόσβαση σε χιλιάδες αριθμούς πιστωτικών καρτών.

Ο Στόχος
Ο στόχος ήταν ένα θεματικό πάρκο το οποίο ανησυχούσε για πιθανή παράνομη διείσδυση σε ένα από τα συστήματα έκδοσης εισιτηρίων. Στο check in των πελατών, ο κάθε υπολογιστής περιείχε ένα σύνδεσμο προς τους server, τα στοιχεία των πελατών και τα οικονομικά αρχεία. Το πάρκο ήθελε να δει αν υπήρχε πιθανότητα να χρησιμοποιήσει κάποιος κακόβουλες μεθόδους και να εκμεταλλευτεί έναν υπάλληλο, ο οποίος άθελα του θα έδινε πληροφορίες τις οποίες θα μπορούσε ένας απατεώνας να εκμεταλλευτεί και να αποκτήσει πρόσβαση στο σύστημα.
Ο στόχος του Kevin δεν ήταν να δημιουργήσει πρόβλημα σε κάποιον υπάλληλο, ούτε να διεισδύσει στους υπολογιστές της επιχείρησης μέσω χακαρίσματος αλλά μέσω προσπαθειών κοινωνικής μηχανικής και μόνο.
Για να επιτύχει η προσπάθεια της επίθεσης, έπρεπε να κατανοήσει τις διαδικασίες του θεματικού πάρκου και τις μεθόδους που χρησιμοποιούσαν για να κάνουν check in στους πελάτες.

Η Ιστορία
Ο στόχος αυτής της συγκεκριμένης υπόθεσης δεν ήταν πολύ περίπλοκος. Έπρεπε απλά ο Kevin να ανακαλύψει αν οι υπάλληλοι στα ταμεία του πάρκου μπορούσαν να γίνουν θύματα κοινωνικής μηχανικής από πελάτες – θύτες. Για να το επιτύχει αυτό, έπρεπε να καταλάβει τον τρόπο λειτουργίας της επιχείρησης.
Έκανε μια περιήγηση στην ιστοσελίδα του πάρκου και χρησιμοποίησε το Maltego και το Google για να αναζητήσει άρθρα και άλλες πληροφορίες για τον εν λόγω οργανισμό. Επίσης έκανε μια έρευνα στις εγκαταστάσεις τους. Στην συνέχεια ακολούθησε όλη την διαδικασία που απαιτούνταν για την αγορά ενός εισιτηρίου από το γκισέ του ταμείου. Κατά την διάρκεια αυτής της διαδικασίας, ξεκίνησε μια σύντομη συζήτηση με έναν ταμία και προσπάθησε να παρατηρήσει την όλη διάταξη, τον υπολογιστή αλλά και άλλες πτυχές της περιοχής του "γραφείου".
Αυτή η περιοχή ήταν αυτό που του έδωσε μια πιο ξεκάθαρη εικόνα. Κατά την διάρκεια της συζήτησης, ανέφερε ότι ήταν από μια επαρχιακή πόλη με ένα τεράστιο όνομα. Όταν η υπάλληλος ρώτησε που ακριβώς, και της απάντησε, του έδωσε μια συνηθισμένη απόκριση:
"Που στο καλό είναι αυτό;"
"Έχετε πρόσβαση στο διαδίκτυο ;"

“Ναι, φυσικά.”
“Α, θα το λατρέψεις. Πήγαινε στο maps.google.com και πληκτρολόγησε τον ταχυδρομικό κωδικό 11111, και βάλε εμφάνιση από δορυφόρο. Κοίτα πόσο μικρή είναι η πόλη.”
“Θεέ μου, είναι πολύ μικρή. Δεν νομίζω ότι την έχω ξανακούσει ποτέ στο παρελθόν.”
Σε αυτό το σύντομο χρονικό διάστημα έμαθε τα ακόλουθα, την διάταξη του χώρου του ταμεία, πως οι υπάλληλοι ελέγχουν το πελάτη καθώς και ότι οι υπολογιστές έχουν πλήρη πρόσβαση στο διαδίκτυο.
Έτσι, επέστρεψε στην ιστοσελίδα του πάρκου και άρχισε την αναζήτηση του και πάλι υπό νέα διάσταση, γνωρίζοντας πια μέρος των διαδικασιών τους. Χρειαζόταν να βρει ένα τρόπο να μπει στον υπολογιστή τους και στο σύστημα τους. Το πρόσχημα του ήταν αρκετά λογικό. Ήταν ένας πατέρας που θα έφερνε την οικογένεια του στο πάρκο. Η ιστορία του ήταν ότι δεν το είχανε σχεδιάσει, αλλά όταν φτάσανε στο ξενοδοχείο έψαξαν στο διαδίκτυο τι μπορούσαν να κάνουν και βρήκαν μια καλή προσφορά για το πάρκο η οποία ίσχυε για κρατήσεις από το διαδίκτυο. Πλήρωσαν και μετά ανακαλύψαν ότι τα εισιτήρια έπρεπε να τυπωθούν για να σκαναριστούν. Ζήτησε από το ξενοδοχείο να τα εκτυπώσει αλλά ο εκτυπωτής δεν λειτουργούσε. Είχε ήδη πληρώσει και φοβόταν μην χάσει τα εισιτήρια έτσι τα εκτύπωσε σε PDF και στην συνέχεια τα έστειλε με e-mail στον εαυτό του.
Χρειαζόταν να κάνει ένα ακόμα βήμα πριν θέσει σε ισχύ το σχέδιο του. Έπρεπε να κάνει μια σύντομη τηλεφωνική κλήση:
“Γεια σας, πήρα το Θεματικό Πάρκο XYZ;”
“Ναι. Πως μπορώ να σας εξυπηρετήσω;”
“Γεια σας, το όνομα μου είναι Paul από την SecuriSoft. Προσφέρουμε μια δωρεάν δοκιμή του νέου λογισμικού μας για την ανάγνωση και εκτύπωση αρχείων PDF. Θα ήθελα να σας στείλω ένα URL για να το κατεβάσετε δωρεάν, υπάρχει πρόβλημα;”
“Δεν ξέρω αν μας ενδιαφέρει, αλλά μπορείτε να μας στείλετε κάποιες πληροφορίες.”
“Εντάξει. Μήπως ξέρετε ποια έκδοση του Adobe χρησιμοποιείτε;”
“Νομίζω είμαστε στην 8η ακόμα.”
“Εντάξει, θα σας στείλω μερικές πληροφορίες για να συγκρίνετε τα πακέτα σήμερα.”
Οπλισμένος με τις πληροφορίες για την έκδοση που χρησιμοποιούν, το μόνο που χρειαζόταν ήταν να δημιουργήσει ένα κακόβουλο λογισμικό, το οποίο θα ήταν ενσωματωμένο σε ένα PDF (το οποίο θα του έδινε πρόσβαση στον υπολογιστή τους, μόλις φυσικά άνοιγαν το PDF). Το ονόμασε Receipt.pdf, και μετά το έστειλε στον εαυτό του με e-mail.
Την επόμενη ημέρα, έφερε την οικογένεια του έτσι ώστε να συμμετέχει σε ένα μικρό πείραμα κοινωνικής μηχανικής. Ενώ έμεινε σε απόσταση, προσέγγισε την γυναίκα πίσω από το γκισέ και ξεκίνησε μια φιλική συζήτηση.
“Γεια, τι κάνεις... Tina;” είπε διαβάζοντας το καρτελάκι με το όνομα της.
“Καλά, πως μπορώ να βοηθήσω;” είπε με ένα φιλικό χαμόγελο.
“Κοίτα, αποφασίσαμε να περάσουμε ένα σαββατοκύριακο μακριά από την πόλη μας και μένουμε στο Hilton μαζί με την οικογένεια μου,” είπε, δείχνοντας την όμορφη οικογένεια του που στεκόταν λίγο πιο μακριά.
“Η κόρη μου είδε την διαφήμιση για το θεματικό σας πάρκο και μας παρακάλεσε να έρθουμε. Βρήκαμε μια καλή προσφορά για εισιτήρια στο διαδίκτυο...”
“Α, ναι την τιμή που ισχύει μόνο για το διαδίκτυο, μπορώ να έχω τα εισιτήρια σας;”
“Ναι, εδώ είναι που χρειάζομαι την βοήθεια σας, έτσι ώστε να μην πάρω το βραβείο του ‘Χειρότερου Μπαμπά της Χρονιάς’.” Είπε χαμογελώντας νευρικά ενώ αυτή γελούσε. Στην συνέχεια της εξήγησε.
“Tina, είδαμε αυτή την προσφορά με τη γυναίκα μου και είπαμε να εξοικονομήσουμε το 15% και αγοράσαμε τα εισιτήρια από τον υπολογιστή του ξενοδοχείου. Αλλά αφού ολοκλήρωσα την πληρωμή, δεν μπορούσα να τα εκτυπώσω επειδή ο εκτυπωτής δεν λειτουργούσε. Βέβαια, τα αποθήκευσα σε PDF και τα έστειλα με e-mail σε μένα. Ξέρω ότι αυτό που ζητάω είναι περίεργο αλλά μήπως θα μπορούσες να συνδεθείς στον

λογαριασμό του e-mail μου και να εκτυπώσεις για μένα;" Αυτός ο λογαριασμός ήταν σχεδιασμένος έτσι ώστε να έχει e-mails με τίτλο "Φωτογραφίες των παιδιών," "Επέτειος μαμάς και μπαμπά" κλπ.
Σίγουρα προβληματίστηκε αν έπρεπε να το κάνει και δεν ήταν σίγουρος αν η σιωπή της ήταν προς όφελος του ή θα έπρεπε να την πείσει και άλλο. Είπε, "Ξέρω ότι είναι περίεργο αυτό που ζητάω, αλλά το μικρό μου κοριτσάκι θέλει πολύ να μπει στο πάρκο και δεν μπορώ να της το αρνηθώ", δείχνοντας την κόρη του η οποία έκανε εξαιρετική δουλειά δείχνοντας χαριτωμένη και ανυπόμονη.
"Εντάξει, πώς να το κάνω;"
"Πήγαινε στο gmail.com, συνδέσου στο Paul1234@gmail.com και γράψε τον κωδικό B-E-S-M-A-R-T."
Μετά από λίγο, η Tina έκανε διπλό κλικ στο PDF του και βρέθηκε σε μια κενή οθόνη.
"Με κοροϊδεύεις; Το έγραψα λάθος; Σίγουρα θα πάρω το βραβείο του χειρότερου μπαμπά τώρα."
"Ξέρετε κάτι, κύριε; Τι θα λέγατε αν πληρώνατε το δικό σας εισιτήριο και της συζύγου σας και επέτρεπα στην κόρη σας να μπει δωρεάν σήμερα;"
"Αλήθεια; Αυτό είναι πολύ ευγενικό εκ μέρους σου." Με χαμόγελο έδωσε τα $50 και την ευχαρίστησε για την βοήθεια της και της ζήτησε να κάνει αποσύνδεση από τον λογαριασμό του.
Λίγο αργότερα, ο συνεργάτης του, του έστειλε μήνυμα και τον ενημέρωσε ότι "μπήκε" και "συγκέντρωσε" όλες τις πληροφορίες για την αναφορά. Αφού χαλάρωσαν για λίγες ώρες, έφυγαν από το πάρκο και τη Δευτέρα επέστρεψε στην δουλειά του για να συντάξει την αναφορά για την συνάντηση που είχαν προγραμματίσει.

Εφαρμογή του Πλαισίου Αυτό- Αξιολόγησης στην Απάτη στο Θεματικό Πάρκο
Η συγκέντρωση πληροφοριών, όπως φαίνεται σε αυτή την μελέτη περίπτωσης, δεν γίνεται πάντα από το διαδίκτυο αλλά μπορεί να γίνει και αυτοπροσώπως. Οι πιο σημαντικές πληροφορίες σε αυτή την περίπτωση, συγκεντρώθηκαν κατά την διάρκεια μιας επίσκεψης. Η αναζήτηση για το τι συστήματα χρησιμοποιούνταν, η προσπάθεια ανίχνευσης του τρόπου αντίδρασης του στόχου σε συγκεκριμένες ερωτήσεις, και η γνώση του πως δουλεύει το σύστημα έκδοσης εισιτηρίων αποτελούσαν σημαντικά στοιχεία για τη συγκέντρωση πληροφοριών.
Το καθοριστικό σημείο σε αυτή την συγκεκριμένη απάτη είναι ένα καλό πρόσχημα και ότι δεν έχει να κάνει μόνο με μια καλή μεταμφίεση και ένα ωραίο λόγο. Ένα καλό πρόσχημα είναι κάτι το οποίο μπορεί να βρεθεί χωρίς πολλή προσπάθεια.
Σε αυτό το σενάριο, ο Kevin μπόρεσε να μιλήσει και να υποκριθεί τον πατέρα καλά, αφού είναι και ο ίδιος πατέρας. Η ανησυχία του μην θεωρηθεί αποτυχημένος πατέρας φάνηκε αληθοφανής στον στόχο. Αυτό έκανε και όλη την συζήτηση πιο πιστευτή. Φυσικά, το να έχεις ένα γλυκό παιδάκι να περιμένει με ανυπομονησία το εισιτήριο βοήθησε και τον ίδιο καθώς και η ιστορία που σκαρφίστηκε για τον εκτυπωτή που χάλασε στο ξενοδοχείο.
Το πρόσχημα περιλαμβάνει την δημιουργία μιας πραγματικότητας η οποία θα χειραγωγήσει τα συναισθήματα και τις ενέργειες του στόχου με τον τρόπο που επιθυμεί ο θύτης. Οι άνθρωποι δεν το κάνουν αυτό συχνά με ένα απλό ψέμα. Ένας κοινωνικός μηχανικός πρέπει να "γίνει" ο χαρακτήρας του προσχήματος και αυτός είναι ο λόγος που δημιουργεί προσχήματα με τα οποία μπορεί εύκολα να ταυτιστεί κάποιος.
Το πρόσχημα του "δωρεάν λογισμικού σε μορφή PDF" είχε μεγάλο περιθώριο σφάλματος. Σαν πρόσχημα ήταν ισχυρό, αλλά μια γρήγορη απόρριψη θα σήμαινε μια καθυστέρηση μερικών ημερών μέχρι να γίνει η επόμενη επίθεση. Επίσης ήταν μια "τυχερή πρόβλεψη" ότι θα χρησιμοποιούνταν η ίδια έκδοση του Adobe σε όλη την εταιρεία και ο συγκεκριμένος ταμίας δεν είχε κάνει αναβάθμιση του Adobe στην πιο πρόσφατη έκδοση, κάτι που ουσιαστικά θα κατέστρεφε όλες τις προσπάθειές του.
Η χρήση λέξεων και φράσεων όπως, "Πραγματικά χρειάζομαι την βοήθεια σου..." αποτελεί ένα ισχυρό εργαλείο. Οι άνθρωποι από την φύση τους θέλουν να βοηθούν

ο ένας τον άλλον, ιδιαίτερα όταν τους ζητείται κάτι τέτοιο. Όταν τους ζητηθεί, εντελώς άγνωστα άτομα θα κάνουν ότι μπορούν για να βοηθήσουν φτάνοντας στο σημείο, όπως έγινε σε αυτή την περίπτωση, να ανοίξουν ένα αρχείο από τον λογαριασμό του email ενός άγνωστου ατόμου.
Μόλις έγινε η παραβίαση, το λογισμικό που αποθηκεύει όλες τις πληροφορίες από τις πιστωτικές κάρτες ήταν έτοιμο να εκτελέσει την επίθεση του. Η ικανότητα συλλογής δεδομένων με τόσο μικρή προσπάθεια θα μπορούσε να οδηγήσει το πάρκο σε τεράστιες απώλειες, μηνύσεις και κατακραυγή από την κοινή γνώμη.

2.5. Γιατί η μελέτη περιπτώσεων είναι σημαντική?

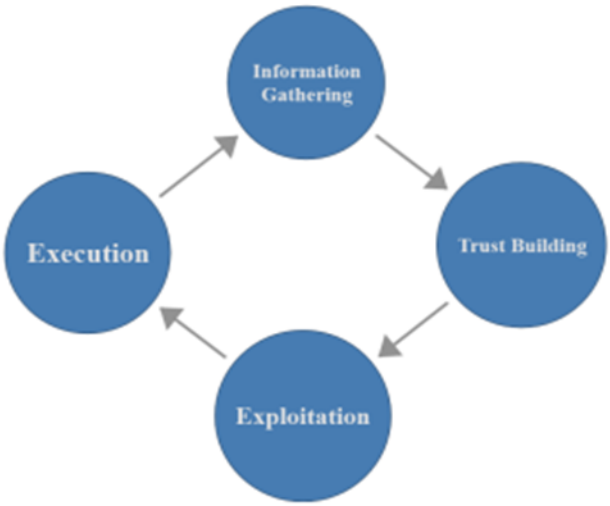
Αυτές οι μελέτες είναι απλά μερικές ιστορίες, και δεν αποτελούν τα πιο ακραία περιστατικά. Κάθε μέρα, κυβερνήσεις, εταιρείες δισεκατομμυρίων, υπηρεσίες αλλά και ολόκληρες χώρες πέφτουν θύματα κακόβουλων επιθέσεων κοινωνικής μηχανικής χωρίς αυτό να περιλαμβάνει τις προσωπικές ιστορίες απάτης και κλοπής προσωπικών στοιχείων αλλά και ληστείες που συμβαίνουν κάθε λεπτό.
Όσο στενάχωρη και αν είναι η ανάγνωση αυτών των ιστοριών, μπορεί να μας μάθει πολλά πράγματα. Ψυχολόγοι και γιατροί αναλύουν αμέτρητες ώρες συνεντεύξεις για να μάθουν τις εκφράσεις που χρησιμοποιούν οι άνθρωποι όταν νοιώθουν συγκεκριμένα συναισθήματα. Οι ειδικοί στην πειθώ εξετάζουν, αναλύουν και μελετούν ιστορίες θετικής και αρνητικής πειθούς. Αυτό τους βοηθάει να μάθουν τα κρυφά σημεία που επηρεάζουν τους ανθρώπους και να βλέπουν πως μπορούν να προστατέψουν τους πελάτες τους. Τα όργανα επιβολής του νόμου μελετούν αυτές τις ιστορίες σαν μέρος της καθημερινότητάς τους για να κατανοήσουν τι μπορεί να είναι ένα εγκληματικό χτύπημα. Οι ερευνητές εγκλημάτων αναλύουν και εξετάζουν κάθε πλευρά ενός κακόβουλου ατόμου, όπως το τι τρώει, πως επικοινωνεί με τους άλλους, τι σκέφτεται και τι τον κάνει να αντιδράσει. Όλες αυτές οι πληροφορίες τους βοηθούν να κατανοήσουν πλήρως το μυαλό ενός εγκληματία.
Αυτές οι ίδιες μέθοδοι χρησιμοποιούνται και από τους επαγγελματίες αναλυτές ανθρώπινης συμπεριφοράς να εντοπίσουν και να πιάσουν τους “κακούς.” Με τον ίδιο τρόπο, οι επαγγελματίες κοινωνικοί μηχανικοί μαθαίνουν πολλά, μελετώντας όχι μόνο τις δικές τους περιπτώσεις αλλά και περιπτώσεις κακόβουλων επιθέσεων που βρίσκουν στις ειδήσεις. Αναλύοντας αυτές τις μελέτες περιπτώσεων, ένας κοινωνικός μηχανικός μπορεί να δει τις αδυναμίες μιας ανθρώπινης ψυχής και να καταλάβει γιατί οι τακτικές στο πλαίσιο της κοινωνικής μηχανικής δουλεύουν τόσο εύκολα.
Τέλος, όλες αυτές οι προσπάθειες εκμετάλλευσης ήταν επιτυχείς επειδή οι άνθρωποι είναι από την φύση τους φτιαγμένοι έτσι ώστε να έχουν εμπιστοσύνη, να δείχνουν συμπόνια, κατανόηση και επιθυμία να βοηθήσουν τους συνανθρώπους τους. Αυτές φυσικά τις αξίες δεν πρέπει να τις χάσουμε καθώς ερχόμαστε σε επαφή με άλλους ανθρώπους στην καθημερινότητα μας. Παρόλα αυτά όμως, αυτές οι αξίες γίνονται προϊόν εκμετάλλευσης από κακόβουλος κοινωνικούς μηχανικούς. Σύμφωνα με τον Kevin Mitnick δεν πρέπει οι άνθρωποι να γίνουν σκληροί και χωρίς συναισθήματα και να συμπεριφέρονται σαν ρομπότ αλλά μας προτείνει να είμαστε ενημερωμένοι, εκπαιδευμένοι και προετοιμασμένοι ώστε να μείνουμε ασφαλείς από τις περισσότερες επιθέσεις κοινωνικής μηχανικής.

3. ΤΡΟΠΟΙ ΚΑΙ ΤΕΧΝΙΚΕΣ ΕΠΙΘΕΣΕΩΝ

Αντίθετα με τις παραδοσιακές επιθέσεις που είχαν στόχο τα πληροφορικά συστήματα χρηστών και οργανισμών, οι κοινωνικοί μηχανικοί έχουν στόχο τον ίδιο το χρήστη ή τον υπάλληλο μέσω των οποίων θα αποσπάσουν τους κωδικούς πρόσβασης των πληροφοριακών συστημάτων τους. Όπως είδαμε και στο κεφάλαιο 2, ο Kevin με διάφορες μεθόδους προσπαθούσε να δημιουργήσει σχέσεις εμπιστοσύνης, να λάβει γνώση των εσωτερικών διαδικασιών και της τεχνολογίας που χρησιμοποιούσαν οι στόχοι του ώστε να πετύχει η επίθεση του.

3.1. Στάδια επίθεσης

Οι επιθέσεις κοινωνικής μηχανικής περιλαμβάνουν τη χρήση διαφορετικών τεχνικών για την εξαγωγή προσωπικών στοιχείων και πληροφοριών από το θύμα. Ωστόσο, το μοτίβο της επίθεσης παραμένει το ίδιο. Η διαδικασία της επίθεσης περιλαμβάνει 4 στάδια: της συσσώρευσης συλλογής δεδομένων /έρευνας/πληροφόρησης, της δημιουργίας σχέσεων/εμπιστοσύνης, την εκμετάλλευση και τελικά εκτέλεση (Aldawood et al, 2020). Αυτά τα τέσσερα στάδια απεικονίζονται στο σχήμα 1.



Σχήμα 3.1: Στάδια επιθέσεων κοινωνικής μηχανικής

(Aldawood et al, 2020)

Η πρώτη φάση μιας επίθεσης κοινωνικής μηχανικής περιλαμβάνει την συγκέντρωση πληροφοριών σχετικά με τον στόχο. Αυτή είναι η πιο σημαντική φάση της επίθεσης. Τα επόμενα στάδια, καθώς και το αποτέλεσμα εξαρτώνται από τις πληροφορίες που αποκτήθηκαν σε αυτό το στάδιο. Είναι εξαιρετικής σημασίας το κατά πόσο ένα θύμα επιλέγεται τυχαία ή με βάση κάποιο συγκεκριμένο χαρακτηριστικό του. Αυτό μπορεί να αποτελέσει σημαντικό στοιχείο στην αντιμετώπιση μιας επίθεσης.

Μετά την ολοκλήρωση της ερευνητικής φάσης, ο εισβολέας επικεντρώνεται στην οικοδόμηση μιας σχέσης με το θύμα ώστε να κερδίσει την εμπιστοσύνη του. Το στάδιο εκμετάλλευσης περιλαμβάνει πειθώ και χειρισμό.

Τέλος, στην εκτελεστική φάση, ο εισβολέας εφαρμόζει την επίθεση για να αποκτήσει όλες τις απαιτούμενες πληροφορίες. Οι επιτιθέμενοι στη συνέχεια προσπαθούν να καθαρίσουν οποιοδήποτε στοιχεία που θα μπορούσαν να τους αποκαλύψουν σε οποιαδήποτε μελλοντική έρευνα**.**

Απαραίτητη προϋπόθεση για την αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής είναι ο εντοπισμός των αδύναμων σημείων του κάθε συστήματος που γίνεται στόχος,

ώστε να μπορούν να αναλυθούν με βάση τα στοιχεία που τα χαρακτηρίζουν, και να αναπτυχθούν οι αντίστοιχοι μηχανισμοί προστασίας (Aldawood et al, 2020).

3.2. Ανάπτυξη σχέσεων εμπιστοσύνης

Ο πρώτος στόχος είναι η δημιουργία σχέσης εμπιστοσύνης. Μόλις αναπτυχθεί αυτή η σχέση, ο κοινωνικός μηχανικός είναι σε θέση να λάβει τις ευαίσθητες πληροφορίες που αναζητά και να αποκτήσει πρόσβαση στο πληροφοριακό σύστημα του θύματος.
Ένας πεπειραμένος κοινωνικός μηχανικός θα εργαστεί σκληρά για να διατηρήσει μια φαινομενικά αθώα σχέση, όπως την εκμάθηση της γλώσσας της εταιρείας, ονόματα προσωπικού, ονόματα σημαντικών διακομιστών και εφαρμογές, αλλά και μια σειρά από άλλες πολύτιμες πληροφορίες.
Οι περισσότεροι άνθρωποι, ειδικά σε τμήματα όπως εξυπηρέτηση πελατών, γραφείο εξυπηρέτησης, βοηθοί επιχειρήσεων και γραμματείς προσπαθούν να βοηθήσουν όπου τους ζητηθεί. Αυτές οι θέσεις εργασίας παρέχουν συνεχώς υποστήριξη στους ανθρώπους και δεν είναι εύκολο να αμφισβητηθεί η εγκυρότητα της κάθε κλήσης.
Επίσης η σχέση εμπιστοσύνης είναι πιο εύκολο να αναπτυχθεί σε ένα μεγάλο οργανισμό συγκριτικά με ένα μικρότερο (Νάρη, 2005).

3.3. Παραπλανητικές σχέσεις

Ένα άλλο ψυχολογικό έναυσμα είναι η οικοδόμηση μιας σχέσης με σκοπό την εκμετάλλευση του άλλου. Ένας τρόπος για να πετύχει αυτό είναι η ανταλλαγή πληροφοριών και η συζήτηση για έναν κοινό εχθρό. Ο Kevin Mitnick στο βιβλίο του περιγράφει ότι η αγαπημένη του μέθοδος ήταν η εξαπάτηση ενός υπαλλήλου που ήδη τον είχε υποψιαστεί σε διαφορετικό όμως πλαίσιο.
Ο Mitnick δημιούργησε σχέση με τον εργαζόμενο – θύμα μέσω email μοιράζοντας πληροφορίες και τεχνολογία χωρίς να του ζητήσει οποιοδήποτε αντάλλαγμα. Βοήθησε να εξελιχθεί η σχέση μιλώντας αρνητικά για τον Kevin Mitnick που ο υπάλληλος δεν συνειδητοποιούσε ότι επρόκειτο για τον αποστολέα του email. Μετά τη δημιουργία της σχέσης αυτής, ο Kevin μπόρεσε να αποκτήσει όλες τις πληροφορίες σχετικά με το σύστημα του ενδιαφερόμενου στόχου.

3.4. Ανταπόδοση

Υπάρχει ένας κανόνας στις κοινωνικές αλληλεπιδράσεις όπου αν κάποιος μας δώσει κάτι ή μας υποσχεθεί, θα πρέπει να του το ανταποδώσουμε.
Αυτό τείνει να γίνει αληθινό ακόμα κι αν δεν ζητήθηκε δώρο ή ακόμα και αν το δώρο είναι πιο πολύτιμο από την αρχική εξυπηρέτηση. Το ψυχολογικό αυτό έναυσμα είναι γνωστό ως ανταπόδοση και χρησιμοποιείται αρκετά στις επιθέσεις.
Ο κοινωνικός μηχανικός εμφανίζεται ως ήρωας έτοιμος, πρόθυμος και ικανός να διορθώσει τα προβλήματα του στόχου. Ακόμη και προτού επιλυθεί το πρόβλημα, ο στόχος αισθάνεται χρέος απέναντί του.
Ένας άλλος τρόπος με τον οποίο μπορεί να χρησιμοποιηθεί η ανταπόδοση έχει αποδειχθεί από τα πειράματα συμπεριφοράς. Αυτά τα πειράματα δείχνουν ότι όταν δύο άτομα διαφωνούν, αν ο ένας υποχωρήσει σε κάποιο σημείο – όσο μικρό κι αν είναι – ο άλλος θα αισθανθεί υποχρεωμένος να υποχωρήσει επίσης. Για έναν κοινωνικό μηχανικό αυτό είναι αρκετά εύκολο.
Η ανταπόδοση παρατηρείται συνεχώς στο εταιρικό περιβάλλον. Ένας υπάλληλος θα βοηθήσει έναν άλλον με την προσδοκία ότι, τελικά η εύνοια θα επιστρέψει σε αυτόν. Είναι ένα άγραφο σύστημα ανταλλαγής που θεωρείται ανεκτίμητο αν κάποιος θέλει να θεωρείται επιτυχημένος. Ωστόσο, ο κοινωνικός μηχανικός εκμεταλλεύεται αυτό το σύστημα γιατί τα κίνητρά του είναι ανέντιμα και αναζητά κάτι που δεν πρέπει να δοθεί με κανένα κόστος.

Μία τεχνική που εφαρμόζει την ανταπόδοση είναι η αντίστροφη κοινωνική μηχανική. Ο επιτιθέμενος προκαλεί πρόβλημα στο δίκτυο ή στον υπολογιστή του θύματος και στη συνέχεια προσφέρεται να επιλύσει το πρόβλημα. Μόλις ο κοινωνικός μηχανικός επιλύσει το «πρόβλημα», θεωρείται ο ήρωας και έτσι έχει κερδίσει την εμπιστοσύνη του στόχου του. Για να λειτουργήσει η μέθοδος της αντίστροφης κοινωνικής μηχανικής, πρέπει ο θύτης να είναι σε θέση να μπει σε έναν υπολογιστή ή σύστημα εκ των προτέρων ή να στείλει ένα αρχείο για να προκαλέσει το «πρόβλημα». Αυτό απαιτεί αρκετή προετοιμασία για να προχωρήσει η έρευνα, αλλά στο τέλος το αποτέλεσμα να έχει θετικό πρόσημο (Μούρτος 2018).
Αυτή η μορφή επίθεσης περιλαμβάνει τα εξής στάδια:

- *Δολιοφθορά*: Σε αυτό το στάδιο ο κοινωνικός μηχανικός προκαλεί μια βλάβη στο σύστημα του θύματος ή τον πείθει προς πρόκειται για βλάβη.
- *Αυτοπροβολή*: Την κατάλληλη στιγμή, ο κοινωνικός μηχανικός παρουσιάζεται ως «από μηχανής Θεός» και καθησυχάζει το θύμα του πως έχει τη λύση για το πρόβλημα που έχει δημιουργηθεί.
- *Υποστήριξη* : Έχοντας κερδίσει την εμπιστοσύνη του θύματος ο κοινωνικός μηχανικός μπορεί να προχωρήσει στην επίλυση του “προβλήματος”. Αντίθετα το θύμα – χρήστης είναι σε θέση να αποκαλύψει όσον τον δυνατόν περισσότερες πληροφορίες και να προσφέρει στον θύτη πρόσβαση στα συστήματα ώστε να επιδιορθώσει το πρόβλημα.

3.5. Ταξινόμηση βάση του τρόπου προσέγγισης του στόχου

Οι επιθέσεις της κοινωνικής μηχανικής είναι πολυεπίπεδες και περιλαμβάνουν πολλά κοινωνικά, τεχνικά και φυσικά χαρακτηριστικά.

Κοινωνική προσέγγιση
Η κοινωνική προσέγγιση βασίζεται στην τέχνη της χειραγώγησης και της πειθούς και εξαρτάται από τη σχέση που αναπτύσσεται μεταξύ του στόχου και του επιτιθέμενου. Χρησιμοποιώντας ψυχολογικές δεξιότητες, οι στόχοι χειρίζονται με τέτοιο τρόπο ώστε να πεισθούν να αποκαλύψουν ευαίσθητες και εμπιστευτικές πληροφορίες. Σε τέτοιου είδους επιθέσεις, ο θύτης στηρίζεται σε κάποια βασικά χαρακτηριστικά την ανθρώπινης φύσης όπως για παράδειγμα την απληστία (Φραγκοπούλου, 2019).

3.5.1. Τεχνική προσέγγιση

Ως επίθεση τεχνικής προσέγγισης χαρακτηρίζεται η επίθεση η οποία γίνεται κυρίως μέσω του διαδικτύου και βασίζεται στη λήψη ευαίσθητων πληροφοριών χρησιμοποιώντας εξελιγμένα τεχνικά εργαλεία. Συνημμένα email, αναδυόμενα παράθυρα είναι μερικά από τα τεχνικά εργαλεία που χρησιμοποιούνται σε αυτή την τεχνική προσέγγισης. Οι θύτες τείνουν να στοχεύουν σε λιγότερο ασφαλείς ιστότοπους κοινωνικής δικτύωσης για να αποκτούν πρόσβαση με τους κωδικούς πρόσβασης. Πάρα πολλοί άνθρωποι συνηθίζουν να χρησιμοποιούν τον ίδιο κωδικό πρόσβασης για διαφορετικούς ιστότοπους το οποίο αποτελεί κλειδί για τους θύτες, ώστε να έχουν πρόσβαση σε προσωπικές πληροφορίες από ένα και μόνο κωδικό πρόσβασης.
Αξιοσημείωτο είναι πώς οι περισσότεροι άνθρωποι δεν γνωρίζουν πως παρέχουν προσωπικές πληροφορίες γενναιόδωρα σε ανθρώπους που πιθανόν να θέλουν να τους εκμεταλλευτούν. Εξαιρετικό μέσο για τη συλλογή προσωπικών δεδομένων αποτελούν τα μέσα κοινωνικής δικτύωσης. Ειδικά ένας χρήστης που έχει ανοιχτά τα προφίλ του στα μέσα κοινωνικής δικτύωσης αποτελεί εύκολο στόχο(Φραγκοπούλου, 2019).
Μέσω των μηχανών αναζήτησης μπορεί να βρεθούν πληροφορίες για επιχειρήσεις και οργανισμούς όπως για παράδειγμα τηλεφωνικοί αριθμοί, email, πληροφορίες για την οργανωτική δομή μιας επιχείρησης κλπ.

Με μια γρήγορη έρευνα σε λογαριασμούς μέσων κοινωνικής δικτύωσης των εταιρειών, μπορεί κάποιος να αποσπάσει στοιχεία για το προσωπικό, τους πελάτες, τους συνεργάτες καθώς και πληροφορίες για τα συστήματα που εφαρμόζουν. Όλες αυτές οι πληροφορίες μπορούν να παίξουν καταλυτικό ρόλο στην οργάνωση και την επιτυχία της επίθεσης (Μούρτος 2018).

Κοινωνικο-τεχνική
Προκειμένου μία επίθεση κοινωνικής μηχανικής να έχει θετικό αποτέλεσμα, επιλέγεται συχνά να χρησιμοποιείται ένας συνδυασμός διαφορετικών προσεγγίσεων. Η κοινωνική προσέγγιση θα βοηθήσει στην δημιουργία μιας σχέσης εμπιστοσύνης, ενώ η τεχνική προσέγγιση θα προσφέρει τον τρόπο για να αποκτηθεί η πρόσβαση σε ευαίσθητα προσωπικά στοιχεία. Η κοινωνικό-τεχνική αποτελεί ίσως την ισχυρότερη μορφή επίθεσης αφού παρέχει ένα συνδυασμό τύπων επιθέσεων. Baiting και Spear-phishing είναι κάποια είδη κοινωνικο-τεχνικών επιθέσεων.

3.5.2. Φυσική
Στην επίθεση φυσικής προσέγγισης, οι επιτιθέμενοι πραγματοποιούν κάποιου είδους φυσικής ενέργειας προκειμένου να συλλέξουν πληροφορίες. Σε αυτού του είδους την επίθεση ο θύτης δεν κρύβεται πίσω από την ανωνυμία ενός ηλεκτρονικού υπολογιστή. Ο εκβιασμός ή η κλοπή είναι τύποι φυσικής επίθεσης. Παραδείγματος χάριν, εάν ο θύτης αποκτήσει πρόσβαση στα γραφεία μίας εταιρείας και καταφέρει να συλλέξει πληροφορίες μέσω εγγράφων, σημειώσεων ή ξεκλείδωτων υπολογιστών μπορεί με βάση τα στοιχεία που συγκέντρωσε να σχεδιάσει μια πολύ επιτυχημένη επίθεση. Η Dumpster diving θεωρείται μια μορφή φυσικής επίθεσης.
Η Dumpster diving περιλαμβάνει την αναζήτηση σκουπιδιών αναζητώντας κάτι χρήσιμο. Αυτό γίνεται συχνά για να αποκαλυφθούν χρήσιμες πληροφορίες που μπορεί να βοηθήσουν ένα άτομο να αποκτήσει πρόσβαση σε ένα συγκεκριμένο δίκτυο. Έτσι, ενώ ο όρος μπορεί κυριολεκτικά να αναφέρεται στην αναζήτηση μέσα από σκουπίδια, χρησιμοποιείται συχνότερα στο πλαίσιο οποιασδήποτε μεθόδου (ειδικά φυσικών μεθόδων) με την οποία ένας κοινωνικός μηχανικός μπορεί να αναζητήσει πληροφορίες σχετικά με ένα δίκτυο υπολογιστών (https://www.techtarget.com/searchsecurity/definition/dumpster-diving).

3.6. Ταξινόμηση μέσω αλληλεπίδρασης προσώπων
Οι επιθέσεις αυτές βασίζονται στη χρήση ορισμένων αρχών συμπεριλαμβανομένων της ανεπάρκειας, της απόσπασης προσοχής, της εξουσίας, της περιέργειας, της προτίμησης και της ομοιότητας, της εξαπάτησης, της κοινωνική αποδοχής, του φόβου, της δέσμευσης, της ανεντιμότητας, της εμπιστοσύνης, της απληστίας, της πίεσης χρόνου, της φιλίας, της ευθύνης, και φυσικά της διάθεσης για βοήθεια.
Όλες αυτές οι αρχές επηρεάζουν τον στόχο και έτσι παρέχουν εύκολη πρόσβαση στις ιδιωτικές πληροφορίες. Οι τεχνικές προσωπικής αλληλεπίδρασης χρησιμοποιούνται στη φυσική, και μερικές φορές και στη κοινωνική και κοινωνικο-τεχνική κοινωνική μηχανικών επιθέσεων.
Σε όλες τις επιθέσεις που αφορούν στην αλληλεπίδραση, μετά την εκτέλεση της επίθεσης, οι θύτες σταματούν την επικοινωνία τους με το θύμα.

3.6.1. Πλαστοπροσωπία
Αυτός ο τύπος προσωπικής αλληλεπίδρασης περιλαμβάνει την παρουσίαση και την προσποίηση προσωπικοτήτων και ταυτότητας άλλων προσώπων. Για να κερδίσουν πληροφορίες, οι θύτες εμφανίζονται ως άλλα άτομα και στη συνέχεια, αποκτούν πρόσβαση σε ασφαλείς, εμπιστευτικές και προσωπικές πληροφορίες. Μια κοινή περίπτωση πλαστοπροσωπίας είναι σε επίπεδο υποστήριξης. Οι εισβολείς σε αυτές τις

περιπτώσεις, καλούν άτομα και προσποιούνται ότι είναι από το τμήμα υποστήριξης με σκοπό την παροχή κάποιας βοήθειας και καταλήγουν να αποκτήσουν προσωπικές πληροφορίες.

3.6.2. Πρόφαση

Με το πρόσχημα της ανάγκης για άμεση επίλυση ενός προβλήματος, το θύμα αναγκάζεται να αποκαλύψει ορισμένες προσωπικές πληροφορίες. Το πρόβλημα είναι ένα ψεύτικο ζήτημα που πείθει το θύμα να επικοινωνήσει με τον κάποιον που είναι τελικά ο άνθρωπος που σχεδίασε την επίθεση. Η Reverse social engineering είναι ένα παράδειγμα αυτού του τύπου επίθεσης.

3.6.3. Tailgating

Σε αυτόν τον τύπο επίθεσης, ένας εισβολέας ακολουθώντας απλά ένα άτομο που έχει νόμιμη πρόσβαση σε μία συγκεκριμένη περιορισμένη περιοχή αποκτά πρόσβαση. Δηλαδή, χώροι στους ο οποίους απαιτείται έλεγχος ταυτότητας ή χρησιμοποιούνται κάρτες εισόδου. Παραδείγματος χάριν, το άτομο που έχει εξουσιοδοτημένη πρόσβαση σε μια εταιρία για λόγους ευγενείας θα κρατήσει τη πόρτα ανοιχτή για το άτομο-εισβολέα που βρίσκεται ακριβώς πίσω του εκείνη τη χρονική στιγμή. Επιπλέον, ο θύτης μπορεί να εισέλθει με παραποιημένα έγγραφα ή ταυτότητα.

Σχήμα 3.2 : Επίθεση Tailgating

(Φραγκοπούλου,2019)

3.6.4. Quid Pro Quo

Στη συγκεκριμένη περίπτωση οι θύτες τηλεφωνούν τυχαία σε οργανισμούς προσποιούμενοι τμήμα τεχνικής υποστήριξης και ότι είχαν κλήση από τον συγκεκριμένο οργανισμό. Οι επιτιθέμενοι προσποιούνται ότι ενεργούν ως ειδικοί πληροφορικής. Δυστυχώς, αυτή η τεχνική φαίνεται να είναι συχνά επιτυχής, επειδή οι εισβολείς βρίσκουν κάποιον που όντως αντιμετωπίζει πρόβλημα. Ο στόχος ευχαριστεί αυτόν που τον κάλεσε για να τον βοηθήσει με το πρόβλημα που αντιμετωπίζει. Ο τεχνικός θα ξεκινήσει την επίλυση του ζητήματος, αλλά θα προχωρήσει σε εκκίνηση κακόβουλου λογισμικού κατά τη διάρκεια της κλήσης.

3.7. Ταξινόμηση με αλληλεπίδραση προσώπων μέσω τεχνολογικών μέσων

Οι επιθέσεις που δεν περιλαμβάνουν την άμεση, φυσική παρουσία του θύτη εντάσσονται σε αυτή την κατηγορία. Αυτοί οι τύποι επιθέσεων εκτελούνται χρησιμοποιώντας υπολογιστή, κινητό, tablet ή οποιαδήποτε άλλη συσκευή συμβατή με το Διαδίκτυο.

Υπάρχουν διάφοροι μέθοδοι που όχι μόνο επηρεάζουν τους στόχους αλλά παρέχουν όλες τις απαιτούμενες πληροφορίες στους εισβολείς. Οι αλληλεπιδράσεις με βάση την τεχνολογία μπορούν να πραγματοποιηθούν μέσω email, ιστότοπων, κακόβουλων προγραμμάτων, κοινωνικών δικτύων και κινητών συσκευών. Οι επιθέσεις που γίνονται με χρήση κάποιου μέσου παρέχουν στον θύτη το πλεονέκτημα της ανωνυμίας. Ο θύτης χωρίς να αποκαλύψει την πραγματική του ταυτότητα μπορεί πάρα πολύ εύκολα να έρθει σε επαφή με χιλιάδες ανθρώπους καθημερινά, αυξάνοντας τις πιθανότητες κάποιος από αυτούς να πέσει θύμα της επίθεσής του, μειώνοντας ταυτόχρονα τις πιθανότητες να τον ανακαλύψουν, καθώς κρύβεται πίσω από την ανωνυμία των μέσων. Κάποια από τα μέσα που χρησιμοποιούνται:

3.7.1. Ηλεκτρονικό ταχυδρομείο

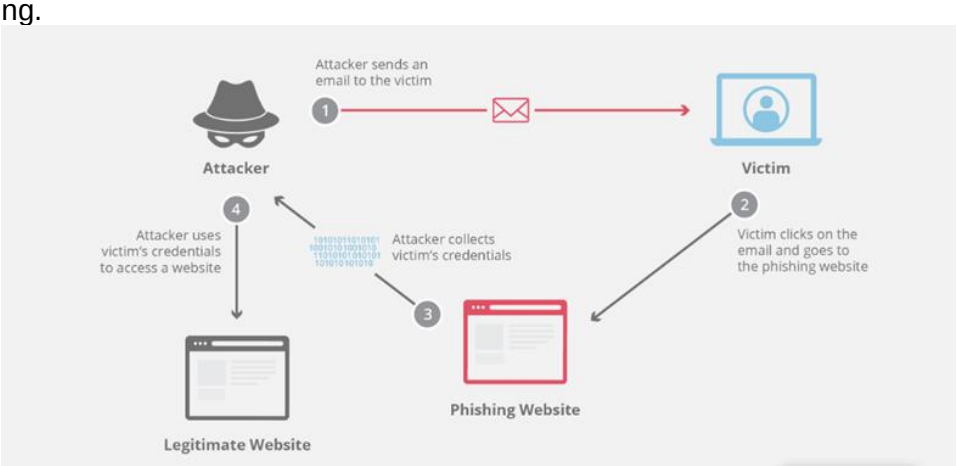
Οι επιθέσεις χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο ως μέσο επιρροής του στόχου.

3.7.1.1. Phishing

Το Phishing αποτελεί ίσως την πιο συνηθισμένη μορφή επίθεσης κοινωνικής μηχανής. Μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου ο θύτης, ο οποίος παρουσιάζεται ως ένα πρόσωπο πολύ αξιόπιστο, μέσω της αίσθησης επείγουσας ανάγκης, προσπαθεί να πείσει τον χρήστη να πατήσει ένα σύνδεσμο ή να κατεβάσει κάποιο λογισμικό. Μέσω αυτού μπορεί να συλλέξει προσωπικές πληροφορίες κωδικούς, προσωπικά δεδομένα ή να αποκτήσει πρόσβαση στο σύστημα του χρήστη και να το χειρίζεται εξ αποστάσεως.

Συνήθως ο θύτης αποστέλλει έναν μεγάλο αριθμό μηνυμάτων ηλεκτρονικού ταχυδρομείου σε τυχαίους παραλήπτες ελπίζοντας πώς όλο και περισσότεροι χρήστες θα πέσουν στην παγίδα του.

Τα μηνύματα ηλεκτρονικού ταχυδρομείου αυτά έχουν μορφή επίσημης αποστολής και περιλαμβάνουν συνήθως κάποιο σύνδεσμο σε κάποιον ιστότοπο μέσω του οποίου το θύμα καλείται να κάνει μια ενέργεια. Μόλις το θύμα πατήσει τον σύνδεσμο γίνεται η υποκλοπή των πληροφοριών. Το Phishing μέσω ηλεκτρονικού ταχυδρομείου μπορεί να κατηγοριοποιηθεί περαιτέρω σε spear-phishing, whaling, and clone-phishing.



Σχήμα 3.3: Επίθεση Phishing

(https://www.cloudflare.com/learning/access-management/phishing-attack/)

3.7.1.2. Spear-Phishing

Το spear-phishing θα μπορούσε εύκολα να συγχέεται με το phishing εξαιτίας της ομοιότητας να στοχεύουν σε χρήστες με σκοπό να κλέψουν προσωπικές πληροφορίες. Το phishing είναι ένας ευρύς όρος για οποιαδήποτε προσπάθεια παραπλάνησης των θυμάτων με σκοπό την απόκτηση προσωπικών δεδομένων τους, συμπεριλαμβανομένων κωδικών πρόσβασης, ονόματα χρηστών και pin πιστωτικών καρτών για κακόβουλους σκοπούς.

Από την άλλη πλευρά, οι spear-phishing επιθέσεις στοχεύουν σε ένα μεμονωμένο άτομο. Τα μηνύματα είναι συνήθως προσαρμοσμένα ώστε να απευθύνονται αποκλειστικά σε αυτό το θύμα. Τα μηνύματα μοιάζουν να προέρχονται από έναν φορέα με τον οποίο ο χρήστης είναι εξοικειωμένος.

Μετά από ενδελεχή έρευνα και συσσώρευση πληροφοριών, ο εισβολέας στέλνει αυτά τα συγκεκριμένα μηνύματα ηλεκτρονικού ταχυδρομείου στο χρήστη για να αποκτήσει τις απόρρητες πληροφορίες.

3.7.1.3. Whaling

Whaling είναι ένας τύπος κοινωνικής μηχανικής που στοχεύει συγκεκριμένα σε έναν οργανισμό συμπεριλαμβανομένων των ιδιοκτητών επιχειρήσεων και των υψηλόβαθμων υπαλλήλων (CEO, CFO, κλπ). Οι στόχοι δεν έχουν επιλεχθεί τυχαία σε αυτόν τον τύπο επίθεσης. Ο εισβολέας θα προσπαθήσει να αποκτήσει πρόσβαση σε πληροφορίες, συστήματα και συσκευές των υψηλών στελεχών μέσω διαφόρων τεχνικών κοινωνικής μηχανικής.

Αρχικά, γίνονται προσπάθειες για τη συλλογή πληροφοριών σχετικά με τον στόχο και στη συνέχεια μέσω των φιλικών σχέσεων που δημιουργούνται αναπτύσσεται και μια σχέση εμπιστοσύνης μεταξύ θύτη και θύματος. Αφού προκύψουν όλες οι πληροφορίες, όπως στοιχεία τραπεζικών συναλλαγών ή προσωπικά στοιχεία, οι θύτες μπορούν να τα επεξεργαστούν.

3.7.2. Ιστότοπος (Website)

Οι επιτιθέμενοι χρησιμοποιούν τον ιστότοπο ως μέσο επίθεσης

3.7.2.1. Website Phishing

Ο θύτης προσπαθεί να κλέψει τον κωδικό πρόσβασης του λογαριασμού ή άλλες εμπιστευτικές πληροφορίες του χρήστη προσποιούμενος ότι πρόκειται για έναν νόμιμο ιστότοπο.

Πληκτρολογώντας ακόμα και εσφαλμένα μια URL διεύθυνση, μπορεί κάποιος να οδηγηθεί σε έναν Website Phishing. Ο εισβολέας στοχεύει άτομα με τη δημιουργία ενός Website Phishing που έχει σχεδόν την ίδια ορθογραφία με έναν γνωστό ιστότοπο.

Ο εισβολέας πείθει τους χρήστες ότι πρόκειται για έναν νόμιμο και ασφαλές ιστότοπο και ο στόχος είναι να κλέψει τον κωδικό πρόσβασης του λογαριασμού των χρηστών ή άλλες εμπιστευτικές πληροφορίες. Η πρόσβαση σε αυτούς τους Website Phishing, οδηγεί σε απόκτηση όλων των στοιχείων αξιοπιστίας από τον εισβολέα.

3.7.3. Κακόβουλο λογισμικό

Αποτελεί μια από τις βασικές μεθόδους που χρησιμοποιούν οι κοινωνικοί μηχανικοί και πολλές φορές σε συνδυασμό με άλλες επιθέσεις κοινωνικής μηχανικής. Συγκεκριμένα αφορά την εξαπάτηση των θυμάτων μέσω ενός Phishing email ώστε το θύμα – παραλήπτης να κατεβάσει ένα κακόβουλο αρχείο στον υπολογιστή του, το οποίο όταν θα το ανοίξει θα δημιουργήσει ένα back-door το οποίο θα μπορέσει να χρησιμοποιηθεί από τον θύτη. Το κακόβουλο λογισμικό επιτρέπει στον επιτιθέμενο την πρόσβαση στον υπολογιστή του θύματος οποιαδήποτε στιγμή θελήσει να “επιτεθεί” (Μούρτος, 2018)

Οι επιθέσεις κοινωνικής μηχανικής που βασίζονται σε κακόβουλα λογισμικά είναι:

3.7.3.1. Spyware

Το λογισμικό υποκλοπής spyware είναι ένας τύπος κακόβουλου λογισμικού, το οποίο κρύβεται σε ψηφιακές συσκευές με σκοπό την παρακολούθηση των δραστηριοτήτων των χρηστών και την πρόσβαση σε ιδιωτικές και εμπιστευτικές πληροφορίες. Επιθέσεις που προκαλούνται από το spyware έχουν ως αποτέλεσμα τη λήψη ευαίσθητων πληροφοριών ατόμων χωρίς τη συγκατάθεσή τους. Ως αποτέλεσμα αυτού του τύπου επίθεσης, ένα ειδικό λογισμικό εγκαθίσταται συνήθως στις συσκευές των θυμάτων και οδηγεί στην απόκτηση προσωπικών στοιχείων, κωδικών πρόσβασης και άλλα προσωπικών δεδομένων.

3.7.3.2. Δόλωμα

Το δόλωμα είναι μια επίθεση κοινωνικής μηχανικής που βασίζεται σε χρήση κακόβουλου λογισμικού, βασικά σε ένα Trojan Horse, το οποίο χρησιμοποιεί φυσικά μέσα. Το κακόβουλο λογισμικό, αποθηκεύεται σε μια συσκευή αποθήκευσης (π.χ. USB) με μια ελκυστική ετικέτα. Στη συνέχεια οι επιτιθέμενοι αφήνουν τη μολυσμένη συσκευή στο χώρο εργασίας, ώστε να μπορεί να χρησιμοποιηθεί από το θύμα. Το θύμα, περιέργως, εισάγει τη συσκευή αποθήκευσης και ενεργοποιεί ακούσια την επίθεση.

Μόλις η επίθεση είναι ενεργοποιημένη οι εμπιστευτικές πληροφορίες έχουν πρόσβαση από τον εισβολέα λόγω της κακόβουλης παρουσίας λογισμικού στη συσκευή. Οι πιο συνηθισμένες συσκευές που χρησιμοποιούνται για δόλωμα είναι USB ή CD-ROM.

3.7.3.3. Ransomware

Το Ransomware είναι ένας κοινός τύπος επίθεσης κοινωνικής μηχανικής, στο οποίο ένα εγκατεστημένο κακόβουλο λογισμικό σε μια συσκευή του θύματος, δεν επιτρέπει την πρόσβαση στο σύστημα πληροφοριών έως ότου καταβληθεί κάποιο αντίτιμο. Αυτή η εγκατάσταση οδηγεί σε πλήρη κρυπτογράφηση των δεδομένων του χρήστη με αποτέλεσμα το κλείδωμα της συσκευής στις περισσότερες περιπτώσεις. Το αντίτιμο απαιτείται κυρίως με τη μορφή bitcoin για αποκρυπτογράφηση των αρχείων. Κανονικά το λογισμικό Ransomware εξαπλώνεται με την επίσκεψη σε ιστότοπους και την απάντηση σε μηνύματα phishing. Το Ransomware μπορεί να είναι πολύ επιβλαβές σε οργανισμούς και σε μεμονωμένα πρόσωπα.

3.7.3.4. Rootkits

Τα Rootkits είναι προγράμματα και σε ορισμένες περιπτώσεις, μια ομάδα εργαλείων λογισμικού, που χρησιμοποιούνται για την ενεργοποίηση των απομακρυσμένων ελέγχων πρόσβασης για τη διαχείριση ενός υπολογιστή ή συστημάτων πληροφοριών από απόσταση.

Αυτή η πρόσβαση χρησιμοποιείται συνήθως νόμιμα για την παροχή απομακρυσμένης υποστήριξης τελικού χρήστη για την επίλυση προβλημάτων πληροφορικής. Ωστόσο, σε πολλές περιπτώσεις, τα περισσότερα rootkits αποκτούν παράνομη πρόσβαση σε συστήματα πληροφοριών του θύματος για την εκκίνηση κακόβουλου λογισμικού.

Αυτό το κακόβουλο λογισμικό περιλαμβάνει ransomware, ιούς, keyloggers, προγράμματα και πολλούς άλλους τύπους κακόβουλου λογισμικού για χρήση του συστήματος του θύματος για άλλες επιθέσεις δικτύου.

Στην πραγματικότητα, γενικά, τα rootkits μπορούν να σταματήσουν το μηχανισμό ανίχνευσης κακόβουλου λογισμικού από λογισμικό προστασίας τελικού σημείου. Εν συντομία, ένας εισβολέας χρησιμοποιεί μια εργαλειοθήκη για να χειρίζεται το βασικό σύστημα της συσκευής του στόχου. Το κύριο πρόβλημα εδώ είναι ότι ο στόχος δεν μπορεί να αναγνωρίσει αυτόν τον τύπο επίθεσης καθώς το σύστημα προστασίας από ιούς είναι απενεργοποιημένο στη διαδικασία εφαρμογής της επίθεσης.

3.7.3.5. Trojans

Trojan είναι ένα επιβλαβές κομμάτι λογισμικού που εμφανίζεται και φαίνεται να είναι νόμιμο. Τα άτομα συνήθως χειραγωγούνται από τους εισβολείς να φορτώσουν και να εκτελέσουν στο δικό τους πληροφοριακό συστήματα το λογισμικό αυτό. Το πρόβλημα είναι ότι μετά την ενεργοποίηση ενός trojan , μπορεί να επιτευχθεί οποιοσδήποτε αριθμός επιθέσεων στο θύμα.

Η ενεργοποίηση αυτής της επίθεσης μπορεί να προκαλέσει ενόχληση στον χρήστη ανοίγοντας πολλά παράθυρα και μπορεί να προκαλέσει μεγάλες ζημιές, όπως διαγραφή αρχείων. Άνοιγμα συνημμένου από phishing, email καθώς και η λήψη ενός αρχείου από το Διαδίκτυο μπορούν να βοηθήσουν τη διάδοση.

3.7.4. Κοινωνικά δίκτυα

3.7.4.1. Κακόβουλοι σύνδεσμοι

Οι κακόβουλες επιθέσεις συνδέσμων περιλαμβάνουν την αποστολή κακόβουλων διευθύνσεων URL προς το θύμα, ώστε το κλικ στον σύνδεσμο να τον κατευθύνει στον μολυσμένο ιστότοπο. Αυτός ο σύνδεσμος είτε αποστέλλεται από πλαστοπροσωπία μιας αξιόπιστης αρχής ή άλλων ψευδών προφίλ σε κοινωνικά δίκτυα.

3.7.4.2. Ψεύτικες ομάδες

Οι ιστότοποι κοινωνικής δικτύωσης όπως το Facebook και το Instagram δεν κάνουν επαλήθευση ταυτότητας στο διαδίκτυο και εκτός σύνδεσης. Έτσι, οι εισβολείς μπορούν να δημιουργήσουν μια ψεύτικη ομάδα σε αυτούς τους ιστότοπους κοινωνικής δικτύωσης προκειμένου να προσελκύσουν τη συμμετοχή των θυμάτων.

3.7.4.3. Ψηφιακή πλαστοπροσωπία

Οι επιθέσεις ψηφιακής πλαστοπροσωπίας των κοινωνικών μέσων περιλαμβάνουν την παρουσίαση του εισβολέα ως κάποια αξιόπιστη αρχή ή πρόσωπο. Οι επιτιθέμενοι τείνουν να πλαστογραφούν την ταυτότητά τους με πλαστογράφηση ή την ταυτότητα άλλων χρηστών.

3.7.4.4. Ψεύτικα προφίλ

Τα κοινωνικά μέσα έγιναν πρόσφατα το μέσο σύνδεσης χρηστών. Ωστόσο, έγινε μια εύκολη πηγή για τους εισβολείς να έχουν πρόσβαση στα προσωπικά στοιχεία των ανθρώπων. Επιπλέον, επιτρέπει στους εισβολείς να πλαστογραφήσουν ταυτότητες φίλων των χρηστών ώστε να κερδίσουν την εμπιστοσύνη τους και να μπορέσουν να συνδεθούν μαζί τους ώστε να τους εξαπατήσουν σε μεταγενέστερο στάδιο. Facebook, Twitter, LinkedIn, Instagram και το Google είναι τα περισσότερο κοινά κοινωνικά μέσα όπου υπάρχουν ψεύτικες ταυτότητες από εισβολείς.

3.7.5. Τεχνάσματα

Οι επιθέσεις κοινωνικής μηχανικής που βασίζονται σε τεχνάσματα είναι :

3.7.5.1. Host File Poisoning

Ένα αρχείο κεντρικού υπολογιστή συνήθως περιέχει domain name και την IP τους διεύθυνση. Μόλις ένας χρήστης ζητήσει μια διεύθυνση URL, μετατρέπεται αρχικά σε μια διεύθυνση IP προτού μεταδοθεί μέσω του Διαδικτύου.

Το poisoning είναι να αλλάξει τις υπάρχουσες εγγραφές του ιστότοπου στο αρχείο του κεντρικού υπολογιστή έτσι ώστε ο πελάτης να μεταφερθεί σε έναν ιστότοπο απάτης όπου του ζητούνται προσωπικά δεδομένα.

3.7.5.2. Secure Socket Layer (SSL)

Αυτές οι επιθέσεις κοινωνικής μηχανικής πραγματοποιούνται μέσω μη αξιόπιστων και πλαστών ιστότοπων. Σε τέτοιες περιπτώσεις, οι αρχικοί ιστότοποι συχνά μοιάζουν με ιστότοπους phishing. Η κύρια διαφορά εδώ είναι ότι οι ψεύτικες σελίδες δεν χρησιμοποιούν πιστοποιητικά SSL ενώ SSL πιστοποιητικά χρησιμοποιούνται από έναν χειριστή για να διασφαλίσει ότι αυτές οι πληροφορίες μεταδίδονται μέσω προστατευμένων καναλιών μεταξύ προγράμματος περιήγησης και του server/διακομιστή. Από την άλλη πλευρά, οι πλαστοί ιστότοποι δεν χρησιμοποιούν SSL επικοινωνίες βάσει πιστοποιητικών. Έλλειψη ασφαλούς χρήσης πρότυπων.

Στις περισσότερες περιπτώσεις, αφού ληφθούν όλοι οι απαραίτητοι έλεγχοι ταυτότητας, ψεύτικες ιστοσελίδες ενδέχεται να ανακατευθύνουν τους χρήστες στους πρωτότυπους ιστότοπους με πιστοποιητικά SSL για να τους ξεγελάσει.

3.7.5.3. Domain Name Server (DNS)

Όταν ένας εισβολέας εκμεταλλεύεται τους υπάρχοντες περιορισμούς στο DNS για ανακατεύθυνση της εισερχόμενης γνήσιας κυκλοφορίας δεδομένων σε ψεύτικες ιστοσελίδες, η διαδικασία ονομάζεται δηλητηρίαση DNS. Κάθε φορά που το πρόγραμμα περιήγησης ενός χρήστη ζητά ένα όνομα domain name, το αίτημα αποστέλλεται συνήθως στο διακομιστή DNS για την αντίστοιχη διεύθυνση IP. Οι εισβολείς μπορούν να δημιουργήσουν ένα ψεύτικο DNS διακομιστή ή αναθεωρήσουν τον υπάρχοντα πίνακα διακομιστών. Τότε αλλάζουν τη διεύθυνση IP στο πραγματικό όνομα domain. Μόλις το DNS δηλητηριάζεται με ψευδείς καταχωρήσεις, οι πελάτες προωθούνται αμέσως σε πλαστογραφημένες σελίδες.

3.7.5.4. Phishing μέσω μηχανών αναζήτησης

Σύμφωνα με το phishing που βασίζεται στη μηχανή αναζήτησης, οι ψευδείς ιστότοποι είναι φτιαγμένοι με ελκυστικές διαφημίσεις. Αυτές οι ιστοσελίδες φαίνονται παρόμοιες με άλλους γνήσιους ιστότοπους υπηρεσιών με πρόθεση για πρόσβαση σε ιδιωτικές και εμπιστευτικές πληροφορίες.

3.7.6. Κινητές συσκευές

Οι επιθέσεις κοινωνικής μηχανικής βασίζονται σε κινητές συσκευές:

3.7.6.1. Αποστολή SMS

Το SMS fishing είναι μια μορφή επίθεσης μέσω κινητού στην οποία ο εισβολέας στέλνει ψεύτικα δοκιμαστικά μηνύματα στον στόχο. Αυτό θα μπορούσε να στοχεύει ότι το μήνυμα προέρχεται από αξιόπιστη οντότητα όπως τράπεζες ή οποιοδήποτε άλλο πάροχο υπηρεσιών. Μερικές φορές περιλαμβάνει επίσης τη λήψη ενός συνημμένου με αποτέλεσμα οι εισβολείς να έχουν πλήρη πρόσβαση στο κινητό τηλέφωνο του στόχου.

3.7.6.2. Εφαρμογές για κινητά

Η εγκατάσταση ή η περιήγηση σε εφαρμογές που βασίζονται σε κινητές συσκευές θα μπορούσαν να οδηγήσουν σε επιθέσεις κοινωνικής μηχανικής. Οι μολυσμένες από κακόβουλο λογισμικό εφαρμογές είναι διαθέσιμες παντού στον Ιστό και η εγκατάσταση αυτών σε smartphones οδηγεί τους εισβολείς να έχουν πρόσβαση σε προσωπικές και ιδιωτικές πληροφορίες.

3.7.6.3. Notification Attacks

Ο εισβολέας σε αυτόν τον τύπο επιθέσεων δημιουργεί ψευδείς ειδοποιήσεις και παράθυρα που είναι πανομοιότυπα των αληθινών ειδοποιήσεων και παραθύρων. Έτσι,

τα προσωπικά στοιχεία προκύπτουν μέσω της συμπλήρωσης των πληροφοριών σχετικά με τα αναδυόμενα παράθυρα ειδοποιήσεων.

3.7.6.4. Voice over Internet Protocol (VoIP) Phishing

Το VoIP είναι πρωτόκολλο επικοινωνίας στο οποίο η φωνή μετάδοσης μέσω του Διαδικτύου, για παράδειγμα μέσω μιας εφαρμογής Voice Over IP (VOIP) αλλά και μέσω του δικτύου κινητής τηλεφωνίας. Οι εισβολείς εισβάλλουν σε ένα χρήστη πληροφοριακών συστημάτων που χρησιμοποιούν VoIP για κλοπή προσωπικών πληροφοριών.

3.7.6.5. Phishing Vishing

Στις επιθέσεις vishing ο θύτης χρησιμοποιεί το δίκτυο κινητής τηλεφωνίας ή το VOIP με σκοπό την απόκτηση ευαίσθητων πληροφοριών από το θύμα. Η συγκεκριμένη επίθεση είναι ανάλογη του phishing ή του SMSishing, με τη διαφορά ότι ως μέσο μετάδοσης πληροφορίας χρησιμοποιείται η φωνή μέσω τηλεφώνου. Χαρακτηριστικό παράδειγμα επίθεσης vishing είναι όταν το θύμα δέχεται ένα τηλεφώνημα και ακούει ένα αυτοματοποιημένο, προ ηχογραφημένο μήνυμα που του υποδεικνύει να καλέσει σε έναν αριθμό για να επιβεβαιώσει τα στοιχεία της τραπέζης του. Όταν το θύμα καλέσει την τράπεζα, έχει στηθεί ένα IVR (Interactive Voice Response) σύστημα το οποίο δίνει στο θύμα έναν αριθμό επιλογών. Ανεξάρτητα από το ποια επιλογή θα επιλέξει το θύμα, θα ακούσει μια φωνή να του ζητά να πληκτρολογήσει τον αριθμό του τραπεζικού του λογαριασμού και τον κωδικό του. Αφού το θύμα τα πληκτρολογήσει, η σύνδεση ανακατευθύνεται στην τράπεζα ή διακόπτεται και ο θύτης έχει πλέον τα στοιχεία του θύματος. Οι εισβολείς αυτού του τύπου ψαρέματος χρησιμοποιούν τις φωνητικές συνομιλίες με σκοπό τη μεταχείριση του στόχου και αποκτώντας πρόσβαση σε ιδιωτικές πληροφορίες.

4. ΤΕΧΝΙΚΕΣ ΑΜΥΝΑΣ

Στο κεφάλαιο αυτό θα ασχοληθούμε με τα μέτρα που πρέπει να λαμβάνουμε ώστε να αντιμετωπίζουμε τις επιθέσεις κοινωνικής μηχανικής. Αναλύοντας τους τρόπους άμυνας θα δούμε ότι δεν υπάρχει κάποιος ολοκληρωτικά αποτελεσματικός τρόπος προστασίας απέναντι σε τέτοιους είδους επιθέσεις.

Οι κλασικοί μηχανισμοί ασφαλείας πληροφοριακών συστημάτων όπως firewalls, antivirus, θεωρούνται τα πιο διαδεδομένα προϊόντα προστασίας. Τα προϊόντα όμως αυτά αποδεικνύονται όλο και λιγότερο αποτελεσματικά ενάντια στην νέα γενιά επιθέσεων. Οι κοινωνικοί μηχανικοί ανακαλύπτουν ευάλωτα σημεία στους μηχανισμούς αυτούς και εφαρμόζουν μεθόδους με τις οποίες τους παρακάμπτουν (Νάρη, 2005).

Είναι προφανές ότι ανεξάρτητα από το πόσο τεχνολογικά ασφαλές είναι ένα δίκτυο, το ανθρώπινο στοιχείο θα να είναι πάντα ένα ευάλωτο σημείο. Συχνά οι άνθρωποι, είτε λόγω ευπιστίας είτε λόγω ευγένειας δεν αρνούνται να δώσουν εμπιστευτικά στοιχεία σε κάποιον που τους το ζητάει ευγενικά ή κάτω από δήθεν “πίεση”.

Αυτό που έχει αποδειχθεί αποτελεσματικό ως ένα βαθμό, δεν είναι η εξάλειψη της εμφάνισής μιας επίθεσης, αλλά η προσπάθεια μείωσης της πιθανότητας να ολοκληρωθεί μια επίθεση επιτυχημένα.

Με δεδομένο τη μη δυνατότητα εξάλειψης των επιθέσεων κοινωνικής μηχανικής, τα μέτρα που λαμβάνονται έχουν στόχο τις ανθρώπινες αδυναμίες που είναι αδύνατον να προβλεφθούν (Βάββας, 2010).

Το ποσοστό επιτυχίας καθώς και ο αριθμός των επιθέσεων αυξάνεται σταθερά λόγω του υψηλού επιπέδου ανωνυμίας που προσφέρεται μέσω των επιθέσεων κοινωνικής μηχανικής.

4.1. Πολιτική ασφάλειας

Δεν μπορείς να οικοδομήσεις κάτι όμορφο και σταθερό πάνω σε αδύναμα θεμέλια. Η βάση της προστασίας των οργανισμών απέναντι στις επιθέσεις κοινωνικής μηχανικής είναι η πολιτική της ασφάλειας.

Η πολιτική ασφάλειας των πληροφοριακών συστημάτων ορίζει το σύνολο των διαδικασιών και των κανόνων που πρέπει να λαμβάνει ένας οργανισμός για την προστασία των πληροφοριακών συστημάτων του. Πρόκειται για έγγραφο που περιγράφει τους ρόλους και τις αρμοδιότητες των υπαλλήλων καθώς και τους κανόνες, τις οδηγίες, τις διαδικασίες που πρέπει να ακολουθούνται ώστε να εφαρμόζονται τα μέτρα προστασίας (Σταματινός, 2015). Η πολιτική προστασίας έχει δεσμευτικό χαρακτήρα, είναι υποχρεωτική για όλους και μπορεί να διαφέρει από οργανισμό σε οργανισμό.

Καθοδηγεί για το τι δεν είναι αναμενόμενο και δίνει τρόπους προσαρμογής ώστε να εξακολουθεί το σύστημα να μένει σταθερό ανάλογα με το εξωτερικό περιβάλλον και με τις μεταβαλλόμενες ανάγκες.

Η κοινωνική μηχανική βοηθά τους χρήστες να αισθάνονται σαν να μην έχουν άλλη επιλογή εκτός από το να αντιστέκονται στις πιέσεις κακόβουλων ανθρώπων. Η απόφαση για το αν θα δοθεί μια πληροφορία δεν λαμβάνεται από τους υπαλλήλους αλλά από αυτούς που έχουν την απαραίτητη γνώση να κρίνουν τη σοβαρότητα της πληροφορίας.

Η πολιτική ασφάλειας πληροφοριακών συστημάτων πρέπει να απευθύνεται σε τομείς όπως: ο έλεγχος και η έγκριση πρόσβασης στις πληροφορίες, οι αλλαγές κωδικού πρόσβασης, η ρύθμιση λογαριασμών, η τακτική εκπαίδευση των υπαλλήλων (Μούρτος, 2018).

4.2. Ευαισθητοποίηση και εκπαίδευση

Η ευαισθητοποίηση και η εκπαίδευση θεωρείται η πρώτη γραμμή άμυνας για την αποτελεσματική αντιμετώπιση επιθέσεων κοινωνικής μηχανικής. Σε κάθε εργαζόμενο ο οργανισμός θα πρέπει να παρέχει βασική εκπαίδευση σε θέματα ασφαλείας πληροφοριακών συστημάτων σε τακτά χρονικά διαστήματα (Μούρτος, 2018).

Η ευαισθητοποίηση σε θέματα που αφορούν τις κυβερνοεπιθέσεις, τις αδυναμίες τους καθώς και τις επιπτώσεις τους στην κοινωνία είναι πλέον απαραίτητη. Βοηθά τους χρήστες να μάθουν να προστατεύονται από κινδύνους και να γνωρίζουν τον τρόπο που θα πρέπει να συμπεριφέρονται στον κόσμο του διαδικτύου. Είναι μια συνεχής διαδικασία που εξελίσσεται με το χρόνο ως προς τον τρόπο και τις μεθόδους που χρησιμοποιούνται ανάλογα το χρήστη και τον οργανισμό. Οι μέθοδοι μπορεί να αφορούν διάφορες παρουσιάσεις, εγχειρίδια, εκδηλώσεις- σεμινάρια με παραδείγματα πρόσφατες επιθέσεις, πραγματικά περιστατικά, νέους κινδύνους, νέες οδηγίες και κανονισμούς, πολιτικές κλπ. (Αποστόλου, 2014).

Η εκπαίδευση διδάσκει στους υπαλλήλους βασικές αρχές ασφάλειας δεδομένων και τους βοηθά να αναγνωρίζουν και να αμύνονται αποτελεσματικά στις επιθέσεις κοινωνικής μηχανικής (www.tylercybersecurity.com/blog/how-to-defend-your-organization-against-social-engineering-attacks)

Οι εργαζόμενοι θα πρέπει να γνωρίζουν ότι αρχικά ένας κοινωνικός μηχανικός θα προσπαθήσει να αναπτύξει μια σχέση εμπιστοσύνης την οποία στην συνέχεια θα εκμεταλλευτεί, ώστε να αποσπάσει πολύτιμες πληροφορίες. (Μούρτος, 2018).

4.2.1. Ευαισθητοποίηση και εκπαίδευση υπαλλήλων

Κάθε εργαζόμενος θα πρέπει να έχει γνώση των αρμοδιοτήτων του και της ευθύνης που του αναλογεί απέναντι σε θέματα επιθέσεων. Θα πρέπει να γνωρίζει ότι απαγορεύεται η δημοσίευση και η μετάδοση πληροφοριών χωρίς εξουσιοδότηση. Επιπλέον θα πρέπει να αναφέρει οποιαδήποτε ύποπτη συμπεριφορά. Σημεία που πρέπει να δίνεται βάση από τους χρήστες:

- Τι έχει αξία;

Οι περισσότεροι άνθρωποι δεν δίνουν σημασία στα δεδομένα μέχρι τη στιγμή της καταστροφής του πληροφοριακού συστήματος. Θα πρέπει να συλλογιστούν τι θα έκαναν αν έχαναν την πρόσβαση στον ηλεκτρονικό τους υπολογιστή. Αυτό είναι ένα καλό έναυσμα για να αρχίσει να καταλαβαίνει ένας χρήστης το νόημα και την χρησιμότητα της κάθε πληροφορίας.

- Οι φίλοι μπορεί και να μην είναι πάντα φίλοι

Οι χρήστες θα πρέπει να κατανοήσουν ότι, κάποιος δείχνει ευγενικός και φιλικός απέναντί τους δε σημαίνει ότι έχει πάντα καλές προθέσεις και μπορούν να του εμπιστευτούν ευαίσθητες πληροφορίες επαγγελματικών θεμάτων.

Οι σχέσεις που δημιουργούνται στο εργασιακό περιβάλλον με εξωτερικούς συνεργάτες δεν δίνουν το δικαίωμα για ερωτήματα ευαίσθητων πληροφοριών. Οι χρήστες δε θα πρέπει να ξεχνάνε ότι οι κοινωνικοί μηχανικοί δεν θα επιτεθούν άμεσα, αλλά μετά από ένα εύλογο διάστημα έχοντας αποκτήσει πρώτα την εμπιστοσύνη των θυμάτων τους. Όσο πιο υψηλό το επίπεδο ασφαλείας σύμφωνα με την πολιτική του κάθε οργανισμού, τόσο πιο πολλά εμπόδια θα πρέπει να ξεπεράσουν οι επιτιθέμενοι για να κερδίσουν στο τέλος την εμπιστοσύνη των χρηστών.

- Οι κωδικοί πρόσβασης είναι προσωπικοί

Οι κωδικοί πρόσβασης δεν θα ζητηθούν ποτέ άμεσα από τους κοινωνικούς μηχανικούς. Θα δημιουργήσουν τις συνθήκες ώστε να φαίνεται πολύ λογικό και αναγκαίο στους εργαζόμενους να δώσουν τους κωδικούς σε κάποιο ξένο άτομο χωρίς να σκεφτούν τις συνέπειες αυτής της πράξης

- Με ποικίλους τρόπους μπορεί να γίνει η υποκλοπή των κωδικών πρόσβασης

Οι σελίδες κακόβουλου περιεχομένου μπορούν να υποσχεθούν την διεκδίκηση σπουδαίων και ακριβών δώρων με μοναδικό κόστος την εγγραφή του χρήστη, κάτι που μοιάζει αθώο. Πολλές φορές όμως οι χρήστες χρησιμοποιούν τους ιδίους κωδικούς σε εταιρικούς και προσωπικούς λογαριασμούς, με αποτέλεσμα εύκολα κάποιος να μπορέσει να αποσπάσει κωδικούς που πιθανά να του δώσουν πρόσβαση σε περισσότερους του ενός λογαριασμούς (Μούρτος, 2018).

4.3. Φυσική ασφάλεια

Για να διασφαλίζεται η πρόσβαση μόνο από άτομα με εξουσιοδότηση σε συγκεκριμένα τμήματα του οργανισμού, θα πρέπει να υπάρχει ο κατάλληλος μηχανισμός ελέγχου πρόσβασης. Κάθε υπάλληλος ανάλογα με τη θέση του θα πρέπει να έχει σαφή οδηγία για τα όρια της πρόσβασης που διαθέτει, με τα όρια να αυξάνονται όσο αυξάνεται η σημαντικότητα του χώρου (server room, λογιστήριο, αποθήκες κτλ.).
Οι διακρίσεις ανάμεσα στους χώρους θα πρέπει να συνδυάζονται με χρήση τεχνολογικών μέσων όπως για παράδειγμα η χρήση μαγνητικής κάρτας και οι περιοχές ύψιστης σημασίας θα πρέπει να διαθέτουν επιπλέον μέτρα προστασίας. Επίσης, θα πρέπει διασφαλίζεται ο συνεχής έλεγχος όλων των φυσικών σημείων εισόδου και εξόδου (κάμερες ασφαλείας).
Εκτός της διαχείρισης των υπαλλήλων σημαντική είναι και η διαχείριση των επισκεπτών. Πολλές φορές, στο πλαίσιο λειτουργίας μιας εταιρείας θα πρέπει να αποκτήσουν πρόσβαση στις εγκαταστάσεις και άτομα που δεν ανήκουν στο προσωπικό της εταιρείας όπως πελάτες, εξωτερικοί συνεργάτες, τεχνικοί συντήρησης, συνεργεία καθαρισμού κ.α. Θα πρέπει λοιπόν σε αυτές τις περιπτώσεις να τηρείται ένα πρωτόκολλο το οποίο θα ορίζει τον τρόπο εισόδου καθώς τις επιτρεπόμενες κινήσεις των επισκεπτών. Επιπλέον συστήνεται η συνοδεία από υπάλληλο και η τήρηση βιβλίου επισκεπτών ώστε να υπάρχει η δυνατότητα ιχνηλάτισης (Μούρτος, 2018).

4.4. Έλεγχος ιστορικού υπαλλήλων

Οι κοινωνικοί μηχανικοί θέλοντας να επιτύχουν το στόχο τους θα χρησιμοποιήσουν κάθε δυνατό μέσο και πολλές φορές φθάνουν στο σημείο να επιζητήσουν θέση εργασίας στον οργανισμό που έχουν σκοπό να επιτεθούν. Για το λόγο αυτό, οι εταιρίες στο πλαίσιο προστασίας απέναντι σε επιθέσεις κοινωνικής μηχανικής θα πρέπει να ελέγχουν το ιστορικό ενός ατόμου που θέλουν να προσλάβουν. Η διαδικασία ελέγχου θα πρέπει να είναι συνεχής ακόμα και μετά την πρόσληψη και ανεξαρτήτου του χρόνου εργασίας. Όπως ήδη έχουμε αναφέρει ο κοινωνικός μηχανικός δεν επιτίθεται άμεσα αλλά εκμεταλλεύεται τον χρόνο προς όφελός του. Ο έλεγχος ξεκινά πριν δοθεί έγκριση για την πρόσληψη και περιέχει (Μπλέτσας, 2015):

- Έλεγχος ιατρικού ιστορικού
- Έλεγχος ποινικού μητρώου
- Επιβεβαίωση προσωπικών στοιχείων
- Έλεγχος εγκυρότητας πιστοποιητικών σπουδών- Μελέτη διαθέσιμων συστατικών επιστολών

4.5. Διακοπή πρόσβασης

Αμέσως, μετά τη λήξη συνεργασίας ή την οικειοθελή αποχώρηση ενός υπαλλήλου, είναι απαραίτητο η εταιρία να προβεί σε διακοπή πρόσβασης των ατόμων αυτών από οποιαδήποτε πληροφορία αφορά τον οργανισμό, είτε αφορά πρόσβαση στις εγκαταστάσεις (κατάργηση μαγνητικής κάρτας), είτε πρόσβαση στο δίκτυο, κατάργηση email, κωδικών, κλπ.
Στην περίπτωση της απόλυσης, η διακοπή γίνεται τη στιγμή της ανακοίνωσής της απόφασης της εταιρίας, ενώ σε κάποια αρχεία η δυνατότητα πρόσβασης μπορεί να έχει σταματήσει το προηγούμενο χρονικό διάστημα.

Αν κάποιος εργαζόμενος αιτηθεί άδεια μεγάλου διαστήματος, η εταιρία θα πρέπει να κλειδώσει τον λογαριασμό και να παύσει την πρόσβαση του, ώστε να αποφευχθεί κάποιο περιστατικό για όσο διάστημα αυτός απουσιάζει και να μην του δοθεί η δυνατότητα να εκμεταλλευτεί αυτό το κενό για να συλλέξει πληροφορίες ώστε να οργανώσει μια πιθανή επίθεση (Μπλέτσας, 2015).

4.6. Ασφάλεια Δικτύων

Η ασφάλεια του δικτύου, τόσο από εξωτερικές όσο και από εσωτερικές απειλές, αποτελεί υψηλή προτεραιότητα για κάθε εταιρία. Αδυναμία εφαρμογής αποτελεσματικών μέτρων προστασίας εγκυμονεί διάφορους κινδύνους όπως είναι η μόλυνση από κακόβουλο λογισμικό ή η αλλοίωση περιεχομένου ιστοσελίδας. Επιπρόσθετα εάν τα πρωτόκολλα επικοινωνίας έχουν ελλιπή προστασία, ο κοινωνικός μηχανικός μπορεί να υποκλέψει εμπιστευτικά δεδομένα και κωδικούς πρόσβασης που μεταδίδονται εντός του δικτύου.

Για την προστασία των δικτύων θα πρέπει οι υπεύθυνοι διαχείρισης να :

- ✓ Αναπτύσσουν διαδικασίες που να περιγράφουν σκοπό, πεδίο εφαρμογής, ρόλους, αρμοδιότητες σχετικά με τη προστασία των δικτύων
- ✓ Διαχωρίζουν το εσωτερικό δίκτυο σε διακριτά υπό-δίκτυα με βάση το επίπεδο κρισιμότητας και ευαισθησίας των τμημάτων της εταιρίας
- ✓ Ενημερώνονται για τις τελευταίες εξελίξεις της τεχνολογίας τόσο σε θέματα άμυνας όσο και σε θέματα τρόπων επιθέσεων
- ✓ Εκτελούν τακτικές δοκιμές ελέγχου τρωτών σημείων των συστημάτων με σκοπό τη συνεχή βελτίωση τους (υπουργείου ψηφιακής διακυβέρνησης,2021).

4.7. Προστασία δεδομένων και Ανταλλαγή πληροφοριών

Η προστασία των πληροφοριακών συστημάτων και των προσωπικών δεδομένων θα πρέπει να καλύπτεται με νομοθετικές ρυθμίσεις τόσο σε εθνικό όσο και παγκόσμιο επίπεδο. Επίσης, η ανταλλαγή πληροφοριών μεταξύ επιχειρήσεων βοηθά στην ενημέρωση, βελτίωση και ανάπτυξη μεθόδων προστασίας από επιθέσεις κοινωνικής μηχανικής.

4.8. Εγκατάσταση Λογισμικού στους Εταιρικούς Υπολογιστές

Μέτρο προστασίας απέναντι σε επιθέσεις μέσω κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου ή κακόβουλου συνδέσμου ή συνημμένου αρχείου αποτελούν προϊόντα λογισμικού τα οποία ένας οργανισμός ή μια επιχείρηση οφείλει να παρέχει στους εργαζομένους της. Με τη χρήση αυτών προστίθεται ένα ακόμη μέτρο προστασίας (Φραγκοπούλου, 2019).

4.9. Εντοπισμός αδυναμιών

Οι οργανισμοί πρέπει ανά τακτά χρονικά διαστήματα να κάνουν ελέγχους για να ανακαλύψουν τυχόν αδυναμίες του πληροφοριακού τους συστήματος. Στους ελέγχους χρησιμοποιούνται εργαλεία και τεχνικές που θα χρησιμοποιούνταν σε περιπτώσεις πραγματικής επίθεσης. Για όλες αυτές τις ενέργειες ενημερώνονται οι υπάλληλοι ώστε να έχουν γνώση της πραγματικότητας. Το αποτέλεσμα είναι μεγαλύτερη προστασία σε πιθανή επίθεση (Νάρη, 2005).

4.10. Άμεση Αντίδραση

Σε περίπτωση επίθεσης κοινωνικής μηχανικής θα πρέπει να υπάρχει άμεση αντίδραση ώστε να συλλεχθούν όσο το δυνατόν γρηγορότερα όλα τα στοιχεία σχετικά με την επίθεση. Αν ο επιτιθέμενος καταφέρει να αποκρύψει την επίθεση, μπορεί η εταιρία να γίνει στόχος διαδοχικών επιθέσεων, με απρόβλεπτες συνέπειες. Ανάλογα με

τον οργανισμό υπάρχει και το αντίστοιχο σχέδιο μηχανισμού άμεσης αντίδρασης (Νάρη, 2005).

4.11. Αντιμετώπιση περιστατικού κοινωνικής μηχανικής

Η ανίχνευση και η αντιμετώπιση επιθέσεων κοινωνικής μηχανικής αποτελεί ζωτικής σημασίας ικανότητα για έναν οργανισμό. Κάθε επιχείρηση θα πρέπει να σχεδιάσει και να διαθέτει ένα σχέδιο αντιμετώπισης κοινωνικής επίθεσης ώστε να μπορεί να συνεχίσει να είναι λειτουργική και να προσφέρει αδιάλειπτα τις υπηρεσίες της. Το σχέδιο αντιμετώπισης διαφέρει από οργανισμό σε οργανισμό βάση της πολιτικής ασφάλειας που εφαρμόζει (υπουργείου ψηφιακής διακυβέρνησης,2021).
Το πρώτο και βασικό κομμάτι του σχεδίου αντιμετώπισης είναι η πληροφόρηση των εργαζομένων για το τι ενέργειες πρέπει να κάνουν και ποιους πρέπει να ενημερώσουν (Μπλέτσας,2015).
Η μη αποτελεσματική διαχείριση μιας επίθεσης μπορεί να επιφέρει σοβαρές επιπτώσεις όπως:

- ✓ **Αδυναμία περιορισμού της ζημιάς**: έλλειψη ικανότητας αναγνώρισης ότι πραγματοποιείται ή ότι έχει ήδη λάβει χώρα επίθεση μπορεί να οδηγήσει σε διακοπή λειτουργίας συστημάτων, σοβαρή οικονομική ζημία καθώς και έλλειψη εμπιστοσύνης των πελατών προς τον οργανισμό
- ✓ **Διαδοχικές διαταραχές λειτουργίας**: αδυναμία ολοκληρωτικής αντιμετώπισης μιας επίθεσης, θέτει στόχο και αφήνει εκτεθειμένη την επιχείρηση σε νέες επιθέσεις
- ✓ **Οικονομικές και διοικητικές κυρώσεις**: ο οργανισμός που έπεσε θύμα μιας επίθεσης μπορεί να δεχθεί σημαντικές κυρώσεις όταν μετά την επίθεση προκύψουν αποκλίσεις και μη συμμορφώσεις από νομικές και κανονιστικές διατάξεις

4.12. Κατάρτιση μέσω εκπαιδευτικών προγραμμάτων

Η προστασία και η ασφάλεια από επιθέσεις είναι ένα ζήτημα που εξελίσσεται διαρκώς και χρειάζεται συνεχή εκπαίδευση και κατάρτιση. Μέσα από τα προγράμματα επιτυγχάνεται:

- ✓ Η βελτίωση των δυνατοτήτων των ανθρώπων που ασχολούνται με θέματα ασφάλειας πληροφοριών
- ✓ Παρότρυνση φοιτητών για συμμετοχή, εκπαίδευση και μελέτη του τομέα της ασφάλειας
- ✓ Αύξηση των μαθημάτων ασφαλείας πληροφοριακών συστημάτων σε πανεπιστημιακά προγράμματα σπουδών, όχι μόνο σε τμήματα με παρεμφερές αντικείμενο, αλλά σε οποιαδήποτε επαγγελματική ειδικότητα που χρειάζεται γνώσεις λόγω της θέσης που μπορεί να αποκτήσει σε έναν οργανισμό (Αποστόλου, 2014)

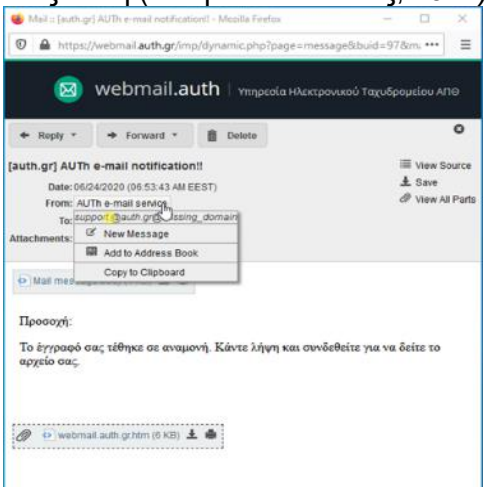
4.13. Τεχνικές πρόληψης για περιπτώσεις προσωπικών επιθέσεων

Σύμφωνα με τους Mosin et al. (2010):

- Πρέπει να είμαστε παρατηρητικοί ως προς το περιεχόμενο ενός e-mail που λαμβάνουμε σχετικά με επείγοντα αιτήματα που αφορούν προσωπικές πληροφορίες οικονομικών θεμάτων ή απειλές διακοπής διαδικτυακών λογαριασμών
- Το email θα πρέπει να είναι ψηφιακά υπογεγραμμένο διότι δεν μπορούμε διαφορετικά να είμαστε σίγουροι για τη γνησιότητά του
- Στην επικεφαλίδα του αποστολέα μπορούμε να αναγνωρίσουμε ότι η ηλεκτρονική του διεύθυνση προέρχεται από ένα δημόσιο πάροχο και όχι από εταιρική διεύθυνση. Εξαιρούνται οι περιπτώσεις στις οποίες ο επιτιθέμενος

έχει ήδη παραβιάσει κάποιους εταιρικούς λογαριασμούς και μέσω αυτών στέλνει τα κακόβουλα μηνύματα

- Πρέπει να δίνεται ιδιαίτερη προσοχή στα συνημμένα αρχεία που πολλές φορές περιέχουν τα ηλεκτρονικά μηνύματα καθώς μπορεί να πρόκειται για κακόβουλο λογισμικό
- Πληροφορίες όπως όνομα χρήστη, κωδικός πρόσβασης, αριθμοί πιστωτικών καρτών δεν θα ζητηθούν ποτέ από τράπεζες και γενικά νόμιμους οργανισμούς
- Τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου συνήθως δεν είναι εξατομικευμένα εν αντιθέσει με τα έγκυρα μηνύματα τραπεζών
- Θα πρέπει πάντα να χρησιμοποιούνται ασφαλείς ισότοποι κατά την υποβολή οποιασδήποτε ευαίσθητης προσωπικής πληροφορίας μέσω του προγράμματος περιήγησής σας στο Web. Η διεύθυνση URL πρέπει να ξεκινά με https:// αντί για http://
- Απαραίτητη είναι η συχνή αλλαγή κωδικών πρόσβασης
- Χρειάζεται τακτικός έλεγχος των κινήσεων των τραπεζικών λογαριασμών ώστε να αποδεικνύεται η νομιμότητα των συναλλαγών
- Η αναγνώριση της γνησιότητας ενός ιστότοπου δεν επιτυγχάνεται κοιτάζοντας απλά τη γενική μορφή του
- Εάν δεν γνωρίζουμε τον αποστολέα, καλό θα είναι να αποφεύγουμε να κατεβάζουμε συνημμένα αρχεία από τέτοια email (Φραγκοπούλου, 2019)
- Ένα κακόβουλο ηλεκτρονικό μήνυμα μπορεί να ελεγχθεί από συντακτικά και ορθογραφικά λάθη. Κατά κύριο λόγο χρησιμοποιείται η Αγγλική γλώσσα, η οποία για πολλούς δεν είναι η μητρική, με αποτέλεσμα να καταγράφονται πολλά τέτοιου είδους λάθη (Αναγνωστόπουλος, 2021)



Σχήμα 4.1 :Παραπλανητικό μήνυμα ηλεκτρονικού ταχυδρομείου
(https://it.auth.gr/el/phishing-email)

4.14. Απομακρυσμένη εργασία

Η εμφάνιση της πανδημίας του κορωνοϊού, οδήγησε μεγάλο ποσοστό εργαζομένων ιδιωτικών και δημοσίων οργανισμών, στην εφαρμογή της απομακρυσμένης εργασίας. Ένα μοντέλο που φαίνεται ότι θα συνεχίσει να εφαρμόζεται και μετά το τέλος της πανδημίας. Μέτρα προστασίας πρέπει να λάβουν τόσο οι φορείς όσο και οι ίδιοι οι εργαζόμενοι.

Σύμφωνα με το Εγχειρίδιο Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης (2021), οι φορείς πρέπει να:

- ✓ Αναπτύξουν πολιτική απομακρυσμένης εργασίας, που θα περιγράφει σκοπό, αρμοδιότητες, ευθύνες και μέτρα προστασίας
- ✓ Ενημερώσουν (update) τον δικτυακό εξοπλισμό με τις πιο πρόσφατες επιδιορθώσεις λογισμικού και ρυθμίσεις ασφάλειας
- ✓ Δημιουργήσουν ισχυρούς κωδικούς πρόσβασης για όλες τις συνδέσεις προς το δίκτυο του οργανισμού

Οι εργαζόμενοι με τη σειρά τους θα πρέπει να :

- ✓ Εφαρμόσουν ισχυρούς κωδικούς πρόσβασης για την πρόσβαση στο δίκτυό τους
- ✓ Χρησιμοποιούν διαφορετικό κωδικό πρόσβασης για κάθε λογαριασμό προσωπικό η υπηρεσιακό που διαθέτουν
- ✓ Μην επιλέγουν αποθήκευση κωδικών πρόσβασης
- ✓ Μην ανοίγουν συνημμένα αρχεία από ύποπτα email
- ✓ Να επαληθεύουν τους αποστολείς των email (π.χ. μέσω τηλεφώνων)
- ✓ Μην αναρτούν το σύνδεσμο της τηλεδιάσκεψης σε δημόσια διαθέσιμο ιστότοπο. Πρέπει η αποστολή του συνδέσμου και των κωδικών να αποστέλλονται απευθείας στους αποδέκτες

Συμπερασματικά, είναι εύκολο να εφαρμοστούν διαδικασίες προστασίας από επιθέσεις κοινωνικών μηχανικών. Ωστόσο, είναι πολύ δύσκολο να καταφέρει ένας ολόκληρος οργανισμός να λειτουργεί, να πράττει και να αξιολογεί με τον ίδιο τρόπο τις καταστάσεις.

5. ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΓΙΑ ΤΗΝ ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ

Τα στατιστικά στοιχεία δείχνουν ότι η χρήση της κοινωνικής μηχανικής αποτελεί έναν αποτελεσματικό τρόπο εξαπάτησης των ανθρώπων. Οι κοινωνικοί μηχανικοί εύκολα μπορούν να αποκτήσουν πρόσβαση σε δεδομένα και στη συνέχεια να εξαπολύσουν επιθέσεις μεγάλης κλίμακας.
Στη συνέχεια θα αναφέρουμε στατιστικά στοιχεία που δείχνουν τον εκπληκτικό αντίκτυπο που έχει η κοινωνική μηχανική παγκοσμίως.

5.1. Γενικά στατιστικά στοιχεία Κοινωνικής Μηχανικής

- Μια επίθεση ransomware είναι επιτυχής κάθε 11 δευτερόλεπτα
- Υπάρχουν 75 φορές περισσότεροι ιστότοποι phishing από ιστότοπους κακόβουλου λογισμικού
- Το 21% όλων των αρχείων δεν προστατεύεται με κανέναν τρόπο
- Το 25% των οργανισμών διαθέτει αυτόνομο τμήμα ασφαλείας
- Το 51% των μικρών επιχειρήσεων δηλώνουν ότι δεν διαθέτουν προϋπολογισμό για την ασφάλεια στον κυβερνοχώρο
- Το 4% του κακόβουλου λογισμικού που αποστέλλεται σε μικρές επιχειρήσεις παραδίδεται μέσω email
- Το 69% των μικρών επιχειρήσεων δεν εφαρμόζουν αυστηρά τις πολιτικές κωδικών πρόσβασης
- Το 16% των μικρών επιχειρήσεων δηλώνουν ότι είχαν αναθεωρήσει τη στάση τους στον κυβερνοχώρο μόνο αφού δέχθηκαν επίθεση
- Τα αρχεία υγείας των ασθενών μπορούν να πουληθούν έως και 363 $ στη μαύρη αγορά, που είναι περισσότερα για οποιαδήποτε πληροφορία από άλλες βιομηχανίες
- Το 41% των πελατών θα σταματούσαν τις συναλλαγές με μια επιχείρηση που έχει πέσει θύμα επίθεσης ransomware
- Το 75% των εταιρειών παγκοσμίως ήταν θύματα phishing το 2020
- Με 241.342 επιτυχημένα περιστατικά , το phishing ήταν το πιο κοινό έγκλημα στον κυβερνοχώρο το 2020 στις ΗΠΑ
- Το 2019 το κόστος ανά παραβιασμένη εγγραφή ήταν 150 $ κατά μέσο όρο.
- Η κυβέρνηση των ΗΠΑ διέθεσε σχεδόν 19 δισεκατομμύρια δολάρια για την ασφάλεια στον κυβερνοχώρο μέσα στο 2021
- Οι μισές από όλες τις παραβιάσεις δεδομένων παγκοσμίως θα συμβαίνουν στις Ηνωμένες Πολιτείες έως το 2023
- Το 2019 οι παραβιάσεις προκάλεσαν κύκλο εργασιών πελατών 3,9%
- Οι προσπάθειες κοινωνικής μηχανικής αυξήθηκαν περισσότερο από 500% από το πρώτο έως το δεύτερο τρίμηνο του 2018
- Ο αριθμός των περιστατικών παραβίασης ανά τύπο:
  - Κλοπή ταυτότητας – 65%
  - Πρόσβαση στον λογαριασμό – 17%
  - Οικονομική πρόσβαση – 13%
  - Ενόχληση – 4%
  - Υπαρξιακά δεδομένα – 1%
- Ο αριθμός των περιστατικών παραβίασης ανά πηγή:
  - Κακόβουλο εξωτερικό άτομο – 56%
  - Τυχαία απώλεια – 34%
  - Κακόβουλο μυστικό – 7%
  - Άγνωστο – 1%
- Αριθμοί ρεκόρ που παραβιάστηκαν από τον κλάδο το 2018:
  - Μέσα κοινωνικής δικτύωσης: 2,5 δισεκατομμύρια αρχεία, ή 56%

- Κυβέρνηση: 1,2 δισεκατομμύρια αρχεία, ή 27%
- Άλλοι κλάδοι: 380 εκατομμύρια δίσκοι, ή 8%
- Λιανικό εμπόριο: 186 εκατομμύρια δίσκοι, ή 4%
- Τεχνολογία: 171 εκατομμύρια δίσκοι, ή 4%

5.2. Πρόσφατα στατιστικά στοιχεία κοινωνικής μηχανικής

- Οι επιθέσεις στον κυβερνοχώρο χρησιμοποιούν κοινωνική μηχανική σε ποσοστό 98%.

Πολλοί υπάλληλοι δεν μπορούν να εντοπίσουν απειλές κοινωνικής μηχανικής και εν αγνοία τους "ανοίγουν τις πόρτες" στους εγκληματίες του κυβερνοχώρου που κλέβουν χρήματα, αποκτούν πρόσβαση σε δεδομένα και να αμαυρώνουν τη φήμη τους.
Βεβαίως υπάρχουν και υπάλληλοι (21% αν λάβουμε υπόψη τόσο τους νυν όσο και τους πρώην υπαλλήλους) που μπορεί να εφαρμόσουν ή να έχουν εφαρμόσει επίθεση κοινωνικής μηχανικής για οικονομικό πλεονέκτημα, για εκδίκηση, από περιέργεια ή για διασκέδαση.

- Πάνω από το 70% των παραβιάσεων προσωπικών δεδομένων οφείλονται σε κοινωνική μηχανική.

Είναι πιο εύκολο να ξεγελάσεις τους ανθρώπους παρά να διεισδύσεις σε ένα ασφαλές σύστημα υπολογιστή, επομένως δεν αποτελεί έκπληξη το γεγονός ότι περίπου το 70% έως 90% της διείσδυσης δεδομένων οφείλεται σε επιθέσεις phishing και κοινωνικής μηχανικής.
Οι εγκληματίες του κυβερνοχώρου μπορούν να στοχεύσουν οποιοδήποτε άτομο ή εταιρεία, αν και οι στατιστικές δείχνουν ότι τα ιδρύματα υγειονομικής περίθαλψης, οι κυβερνητικές υπηρεσίες και τα πανεπιστήμια είναι οι προτιμώμενοι στόχοι για απάτες κοινωνικής μηχανικής λόγω του όγκου των πληροφοριών που αποθηκεύουν.

- Υπάρχουν περισσότεροι από δύο εκατομμύρια ιστότοποι phishing.

Από τις 17 Ιανουαρίου 2021, η ισχυρή μηχανή αναζήτησης, η Google κατέγραψε 2.145.013 ιστότοποι phishing.
Αυτό που συμβαίνει είναι ότι οι μηχανικοί τροφοδοτούν συνεχώς το Dark Web με τα δεδομένα που κλέβουν, τα οποία στη συνέχεια χρησιμεύουν ως εργαλεία για περαιτέρω επιθέσεις στον κυβερνοχώρο.
Μόλις το 2020, οι κοινωνικοί μηχανικοί πρόσθεσαν περίπου 22 εκατομμύρια νέα αρχεία στο Dark Web.

- Το 96% των επιθέσεων phishing χρησιμοποιούν ως μέσο το ηλεκτρονικό ταχυδρομείο.

Αν και ο αριθμός των ιστότοπων phishing είναι εκπληκτικός, τα πιο πρόσφατα στατιστικά στοιχεία κοινωνικής μηχανικής αποκαλύπτουν ότι μόνο το 3% των επιθέσεων phishing πραγματοποιούνται μέσω ιστότοπου και το 1% μέσω τηλεφώνου (είτε vishing είτε smishing).
Ένα email που αναφέρεται σε μια κατάσταση έκτακτης ανάγκης οδηγεί άμεσα στην αποκάλυψη ευαίσθητων πληροφοριών.
Οι πιο συνηθισμένες λέξεις που χρησιμοποιούνται από τους εγκληματίες του κυβερνοχώρου στα μηνύματα ηλεκτρονικού ταχυδρομείου είναι : επείγον, αίτημα, σημαντικό, πληρωμή και προσοχή.

- Το 18% των θυμάτων phishing χάνει χρήματα.

Φαίνεται ότι τα χρήματα δεν είναι το κύριο κίνητρο για τους εγκληματίες του κυβερνοχώρου, παρά μόνο οι πληροφορίες που αποσπούν.
Μετά από μια επιτυχημένη επίθεση phishing, το 60% των εταιρειών αναφέρει χαμένα δεδομένα, το 52% δηλώνει παραβιασμένα διαπιστευτήρια και το 29% παραπονιέται για μόλυνση από κακόβουλο λογισμικό, το οποίο καταλήγει να προκαλεί βλάβη σε ολόκληρο το δίκτυο υπολογιστών της εταιρείας.

Οι εταιρείες ξοδεύουν εκατομμύρια δολάρια για να προστατεύσουν τους ίδιους και τους πελάτες τους από παραβιάσεις δεδομένων, αλλά φαίνεται ότι οι μέθοδοι που χρησιμοποιούν δεν επιφέρουν κάποιο αποτέλεσμα εκτός κι αν προχωρήσουν σε εκπαίδευση των υπαλλήλων τους.
Η κοινωνική μηχανική είναι ένα φλέγον ζήτημα που εκμεταλλεύεται τη φυσική τάση των ανθρώπων να εμπιστεύονται τους άλλους και να τους αποκαλύπτουν ευαίσθητες πληροφορίες με αποτέλεσμα να εξαπατώνται.

- ❖ Ο μέσος οργανισμός αντιμετωπίζει 700 απειλές κοινωνικής μηχανικής ετησίως.

Μέσα σε ένα χρόνο, οι επιτιθέμενοι έστειλαν 12 εκατομμύρια μηνύματα ηλεκτρονικού ψαρέματος (spear-phishing) σε τρία εκατομμύρια γραμματοκιβώτια, επηρεάζοντας 17.000 οργανισμούς. Αυτό σημαίνει ότι 46,5 εταιρείες λαμβάνουν κατά μέσο όρο δύο email ηλεκτρονικού ψαρέματος (spear-phishing) κάθε ημέρα.

- ❖ Το 45% των υπαλλήλων ηλικίας 25-38 ετών δεν γνωρίζει τι είναι το phishing.

Οι στατιστικές κοινωνικής μηχανικής ανά ηλικία δείχνουν ότι όσο μεγαλύτεροι είναι οι εργαζόμενοι, τόσο πιο εξοικειωμένοι είναι με το αντικείμενο.
Το 65% των εργαζομένων άνω των 39 μπορεί να ορίσει σωστά την έννοια phishing.
Ωστόσο, το αντίθετο ισχύει για το vishing, όπου το 34% των εργαζομένων στην ηλικιακή ομάδα 18-22 ετών γνωρίζει την επίθεση αυτή, ενώ στα άτομα άνω των 55 ετών το ποσοστό μειώνεται στο 20%.

- ❖ Το 43% των εργαζομένων στον τομέα της πληροφορικής έπεσαν θύματα επιθέσεων κοινωνικής μηχανικής το 2020.

Ωστόσο, οι πιο συνηθισμένοι στόχοι δεν είναι ούτε οι διευθύνοντες σύμβουλοι ούτε οι υπάλληλοι των τμημάτων πληροφοριακών συστημάτων.
Το 80% των απειλών έχουν στόχο τους εργαζόμενους που δεν έχουν οικονομικό ή εκτελεστικό ρόλο.

- ❖ Περίπου το 30% των εργαζομένων αποτυγχάνει σε ένα τεστ phishing.

Το ποσοστό PPP (Phish-Prene Percentage) ποικίλλει ανάλογα με τον κλάδο, αλλά μπορούμε να θεωρήσουμε έναν μέσο όρο παγκοσμίως που αγγίζει το 31,4%.
Εάν το αναλύσουμε κατά μέγεθος οργανισμού, οι τομείς που κινδυνεύουν περισσότερο είναι τα μικρά κέντρα υγειονομικής περίθαλψης και τα φαρμακευτικά προϊόντα (34% PPP), οι μεσαίες εγκαταστάσεις φιλοξενίας (42,3% PPP) και οι μεγάλοι ενεργειακοί οργανισμοί (52,4% PPP).
Οι εκστρατείες ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο και την κοινωνική μηχανική μείωσαν το ποσοστό αποτυχίας από 30% σε 5% περίπου.

- ❖ Μόνο το 27% των εταιρειών παρέχει εκπαίδευση ευαισθητοποίησης σε θέματα κοινωνικής μηχανικής.

Οι επιχειρήσεις παγκοσμίως ξοδεύουν εκατομμύρια σε τεχνολογίες ασφάλειας, αλλά δεν αφιερώνουν χρόνο για να εκπαιδεύσουν τους υπαλλήλους σχετικά με την κοινωνική μηχανική και τις παραβιάσεις δεδομένων.
Τα τελευταία στατιστικά λένε ότι περίπου το 43% των εργαζομένων δεν λαμβάνουν τακτικά εκπαίδευση για την ασφάλεια των δεδομένων και είναι ανησυχητικό ότι ένα 8% δεν έχει λάβει ποτέ καμία εκπαίδευση.

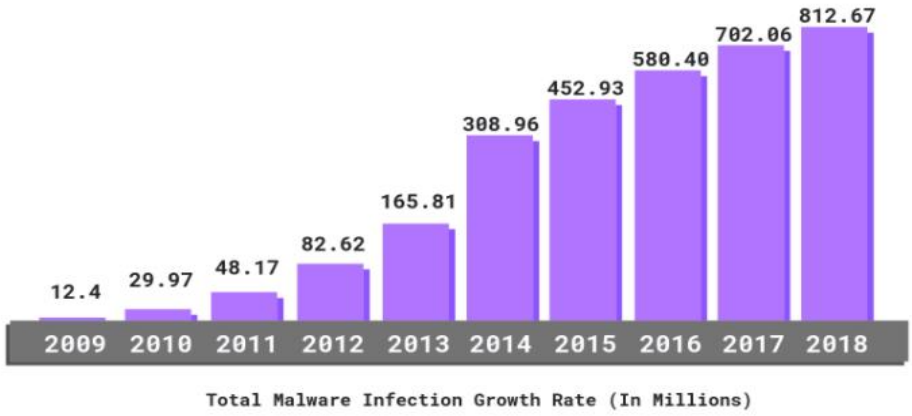
5.3. Στατιστική για Phishing

- Το 56% των υπευθύνων λήψης αποφάσεων πληροφορικής λένε ότι οι στοχευμένες επιθέσεις phishing είναι η κορυφαία απειλή για την ασφάλεια τους
- Το 30% των μηνυμάτων ηλεκτρονικού ψαρέματος ανοίγονται από στοχευμένους χρήστες και το 12% αυτών των χρηστών κάνουν κλικ στο κακόβουλο συνημμένο ή σύνδεσμο
- Μόνο το 3% των στοχευμένων χρηστών αναφέρει κακόβουλα email στη διοίκηση

- Ο συμβιβασμός διαπιστευτηρίων αυξήθηκε κατά 70% το τελευταίο έτος σε σχέση με το 2017 ενώ έχει αυξηθεί κατά 280% από το 2016
- Το 50% των ιστότοπων phishing χρησιμοποιούν πλέον https
- Τα πλαστά τιμολόγια είναι η πρώτη κίνηση για τη διανομή κακόβουλου λογισμικού
    - Λογαριασμός / τιμολόγιο 15,9%
    - Αποτυχία παράδοσης email 15,3%
    - Νομική / επιβολή νόμου 13,2%
    - Σαρωμένο έγγραφο 11,5%
    - Παράδοση πακέτου 3,9%
- Οι πιο συνηθισμένοι τύποι κακόβουλων συνημμένων:
    - Office 38%
    - Αρχείο 37%
    - PDF 14%
    - Άλλο Ext 6%
    - Δυαδικά 4%
    - XML/HTML/JS 1%
- Ο όγκος της απάτης μέσω email που λαμβάνουν οι οργανισμοί έχει αυξηθεί κατά 8% από έτος σε έτος
- Το 66% του κακόβουλου λογισμικού εγκαθίσταται μέσω κακόβουλων συνημμένων email

5.4. Στατιστικά για κακόβουλο λογισμικό

Συνεχόμενη αύξηση των επιθέσεων κακόβουλου λογισμικού καταγράφεται τα τελευταία δέκα χρόνια όπως παρουσιάζεται στο γράφημα που ακολουθεί:



Σχήμα 5.1 : Ρυθμός αύξησης επιθέσεων
(*Αναγνωστόπουλος 2020)*

- Το 92% του κακόβουλου λογισμικού παραδίδεται μέσω email
- Οι νέες παραλλαγές κακόβολου λογισμικού σε κινητά οδήγησαν σε αύξηση αυτών των επιθέσεων κατά 54% το 2018
- Περισσότεροι από 250.000 μοναδικοί χρήστες δέχθηκαν επίθεση από εφαρμογή κακόβουλου λογισμικού (Trojan-Banker.AndroidOS.Asacub)
- Το 98% του κακόβουλου λογισμικού για κινητά στοχεύει σε συσκευές Android
- Κατά τη διάρκεια του τελευταίου έτους, καταγράφηκε αύξηση κατά 165% στο MacOS Malware
- Το κακόβουλο λογισμικό εξακολουθεί να είναι το προτιμώμενο μοντέλο επίθεσης, το οποίο χρησιμοποιήθηκε σε ποσοστό 71,14% τους τελευταίους 12 μήνες

- Τα Trojans αποτελούν το 51,45% όλων των κακόβουλων προγραμμάτων
- 7 στα 10 ωφέλιμα φορτία κακόβουλου λογισμικού ήταν ransomware
- Κάθε μέρα παράγονται 230.000 νέα δείγματα κακόβουλου λογισμικού και υπάρχει πρόβλεψη ότι η αύξηση αυτή θα συνεχιστεί
- Το κακόβουλο λογισμικό και οι επιθέσεις που βασίζονται στον ιστό είναι οι δύο πιο δαπανηροί τύποι επιθέσεων — οι εταιρείες ξόδεψαν κατά μέσο όρο 2,4 εκατομμύρια δολάρια για την προστασία τους
- Πάνω από 18 εκατομμύρια ιστότοποι μολύνονταν κάθε εβδομάδα το 2021 με κακόβουλο λογισμικό
- Το 34% των επιχειρήσεων που χτυπήθηκαν με κακόβουλο λογισμικό χρειάστηκε μία εβδομάδα ή περισσότερο για να ανακτήσουν την πρόσβαση στα δεδομένα τους

5.5. Στατιστικά Ransomware

- Οι επιθέσεις ransomware παγκοσμίως αυξήθηκαν κατά 350% το 2018.
- Το 2021, οι επιθέσεις ransomware εκτιμάται ότι κόστιζαν περίπου 6 τρισεκατομμύρια δολάρια ετησίως
- Σε ερώτηση 582 επαγγελματιών ασφάλειας πληροφοριών το 50% θεωρεί ότι ο οργανισμός τους δεν είναι έτοιμος να αποκρούσει μια επίθεση ransomware
- Το Ransomware κοστίζει στις επιχειρήσεις περισσότερα από 75 δισεκατομμύρια δολάρια ετησίως
- Η Ατλάντα έχει ξοδέψει περισσότερα από 5 εκατομμύρια δολάρια για την ανοικοδόμηση του δικτύου υπολογιστών της, μετά την επίθεση ransomware SamSam που δέχτηκε τον Μάρτιο του 2018
- Το μέσο κόστος μιας επίθεσης ransomware σε επιχειρήσεις ήταν 133.000 $
- Οι επιχειρήσεις έχασαν περίπου 8.500 $ την ώρα λόγω του χρόνου διακοπής λειτουργίας που προκλήθηκε από ransomware
- Το 25% των στελεχών επιχειρήσεων θα ήταν πρόθυμο να πληρώσει μεταξύ 20.000 και 50.000 $ για να αποκτήσει ξανά πρόσβαση σε κρυπτογραφημένα δεδομένα
- Το 40% των θυμάτων ransomware πλήρωσαν τα λύτρα
- Πάνω από το 50% των λύτρων καταβλήθηκαν με bitcoin το 2018
- Το 10% των απαιτήσεων για λύτρα είναι πάνω από 5.000 $
- Από τους 1.100 επαγγελματίες πληροφορικής που συμμετείχαν στην έρευνα, το 90% είχε πελάτες που υπέστησαν επιθέσεις ransomware το 2020
- Το 40% είχε πελάτες που υποβλήθηκαν σε τουλάχιστον 6 επιθέσεις ransomware
- Ένας νέος οργανισμός έπεσε θύμα ransomware κάθε 14 δευτερόλεπτα το 2019 και κάθε 11 δευτερόλεπτα έως το τέλος του 2021

5.6. Το κόστος της ασφάλειας στον κυβερνοχώρο

- Το 2017,το κόστος του εγκλήματος στον κυβερνοχώρο επιταχύνθηκε με τους οργανισμούς να ξοδεύουν σχεδόν 23% περισσότερο συγκριτικά με το 2016 — κατά μέσο όρο περίπου 11,7 εκατομμύρια δολάρια
- Μέχρι το 2025, οι αναλυτές πληροφορικής προβλέπουν δαπάνες για ασφάλεια κυβερνοχώρου πολύ πάνω από 1 τρισεκατομμύριο δολάρια
- Το μέσο κόστος μιας επίθεσης κακόβουλου λογισμικού σε μια εταιρεία είναι 2,4 εκατομμύρια δολάρια
- Το μέσο κόστος χρονικά μιας επίθεσης κακόβουλου λογισμικού είναι 50 ημέρες
- Από το 2016 έως το 2017 σημειώθηκε αύξηση 22,7% στο κόστος της ασφάλειας στον κυβερνοχώρο

- Το μέσο παγκόσμιο κόστος του εγκλήματος στον κυβερνοχώρο αυξήθηκε πάνω από 27% το 2017
- Το πιο ακριβό στοιχείο μιας κυβερνοεπίθεσης είναι η απώλεια πληροφοριών, η οποία αντιπροσωπεύει το 43% του κόστους
- Η ζημιά που σχετίζεται με το έγκλημα στον κυβερνοχώρο άγγιξε τα 6 τρισεκατομμύρια δολάρια ετησίως το 2021

5.7. Πρόσφατες επιθέσεις στον κυβερνοχώρο και παραβιάσεις

Καθώς η παραβίαση προσωπικών δεδομένων γίνεται όλο και πιο διαδεδομένη στην εποχή που ζούμε, έτσι πρέπει να κατανοήσουμε και τις σύγχρονες επιθέσεις στον κυβερνοχώρο. Ας δούμε κάποιες από τις επιθέσεις που πραγματοποιήθηκαν μέσα στο 2021.

- Η Kaseya που διευθύνει έως και 1500 εταιρείες, υπέστη επίθεση με ransomware με τα λύτρα να αγγίζουν το ποσό των 70 εκατομμυρίων δολαρίων
- Η Saudi Aramco αντιμετώπισε επίθεση παραβίασης ευαίσθητων προσωπικών δεδομένων των υπαλλήλων της καθώς και σημαντικών εγγράφων της εταιρείας με τα λύτρα να ανέρχονται στα 50 εκατομμύρια δολάρια
- Η παραβίαση δεδομένων της εφαρμογής μεταφοράς αρχείων Accellion (FTA) επηρέασε περισσότερες από 100 εταιρείες, οργανισμούς, πανεπιστήμια και κυβερνητικούς φορείς σε όλο τον κόσμο
- Το Pulse Secure VPN Zero-Day έγινε αντικείμενο εκμετάλλευσης με αποτέλεσμα την παραβίαση αρκετών εταιρειών και κυβερνητικών οργανισμών στις Ηνωμένες Πολιτείες και την Ευρώπη

Κάποιες από τις επιθέσεις που πραγματοποιήθηκαν το 2020

- Η αλυσίδα ξενοδοχείων Marriott αποκάλυψε επίθεση που επηρέασε τα δεδομένα περισσότερων από 5,2 εκατομμυρίων επισκεπτών ξενοδοχείων που χρησιμοποίησαν την εφαρμογή επιβράβευσης της εταιρείας τους
- Η MGM Resorts υπέστη μαζική παραβίαση δεδομένων με αποτέλεσμα τη διαρροή 142 εκατομμυρίων προσωπικών δεδομένων των επισκεπτών του ξενοδοχείου
- 500.000 κλεμμένοι κωδικοί πρόσβασης Zoom διαθέσιμοι προς πώληση στο Dark web
- Το Magellan Health επλήγη από επίθεση ransomware με παραβίαση δεδομένων 365.000 ασθενών

5.8. Στατιστικά Στοιχεία Κυβερνοεπιθέσεων στην περίοδο εμφάνισης του Κορωνοϊού

Λόγω της επιδημίας του COVID-19 , έχει προκύψει μια άνοδος σε εξελιγμένα συστήματα ηλεκτρονικού "ψαρέματος" από εγκληματίες του κυβερνοχώρου . Οι κακόβουλοι παράγοντες παρουσιάζονται ως εκπρόσωποι του Κέντρου Ελέγχου και Πρόληψης Νοσημάτων (CDC) ή του Παγκόσμιου Οργανισμού Υγείας (ΠΟΥ).

- Το έγκλημα στον κυβερνοχώρο αυξήθηκε κατά 600% λόγω της πανδημίας COVID-19
- Η απόσπαση της προσοχής προκάλεσε το 47% των εργαζομένων να υποκύψουν σε απάτες phishing κατά τη διάρκεια της πανδημίας
- Ο COVID-19 επηρέασε επίσης την ικανότητα των εταιρειών να αντιμετωπίζουν απειλές για την ασφάλεια στον κυβερνοχώρο. Μια πρόσφατη μελέτη δείχνει ότι το 56% των τμημάτων πληροφορικής αναφέρουν αύξηση του χρόνου απόκρισής τους σε κυβερνοεπιθέσεις

- Το 42% των επιχειρήσεων δηλώνουν απροετοίμαστες να αποκρούσουν τις επιθέσεις στον κυβερνοχώρο που στοχεύουν απομακρυσμένους εργαζόμενους
- Οι επιθέσεις κατά των τραπεζών παρουσίασαν αύξηση των επιθέσεων κατά 238%
- Το 27% των επιθέσεων είχαν ως στόχο την υγειονομική περίθαλψη και τις τράπεζες
- Από τον Ιανουάριο μέχρι τον Απρίλιο του 2020 καταγράφηκε αύξηση 630% των επιθέσεων μέσω cloud
- Οι επιθέσεις phishing αυξήθηκαν από το Φεβρουάριο του 200 κατά 600%.
- Το 10% των επιθέσεων phishing από τον Ιανουάριο μέχρι το Μάρτιο αφορούσε την Apple
- Τον Μάρτιο αυξήθηκαν κατά 148% οι επιθέσεις Ransomware
- Το πρώτο τρίμηνο του 2020, πραγματοποιήθηκαν 394.000 επιθέσεις σε βρετανικές εταιρείες, μία αύξηση 30%
- Κατά τη διάρκεια της καραντίνας πενταπλασιάστηκαν οι επιθέσεις που είχαν στόχο τους εργαζόμενους που βρίσκονταν σπίτι τους (τηλεργασία)
- Κατά 66% αυξήθηκαν οι επισκέψεις των μηχανικών σε φόρουμ και ιστότοπους τον Μάρτιο 2020
- Σε σύγκριση με το τελευταίο τρίμηνο του 2019, η μέση πληρωμή ransomware έφτασε τα 111.605$, αύξηση 33%
- 200 τραπεζικές εφαρμογές έγιναν στόχο ενός Trojan EventBot που ανακαλύφθηκε το Μάρτιο του 2020

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι επιθέσεις κοινωνικής μηχανικής αυξάνονται συνεχώς και δυνητικά γίνονται πιο καταστροφικές καθώς αυξάνεται η εξάρτησή μας από την τεχνολογία.
Η ασφάλεια γύρω από τις πληροφορίες βελτιώνεται συνεχώς, όμως ο άνθρωπος εξακολουθεί να είναι ο αδύναμος κρίκος καθώς είναι επιρρεπής σε τεχνικές χειραγώγησης. Η καλλιέργεια μιας κουλτούρας εστιασμένης στην ασφάλεια είναι το κλειδί για την μείωση του ανθρώπινου λάθους. Εάν ο άνθρωπος διδαχθεί πώς να εντοπίζει και να ανταποκρίνεται σωστά σε απειλές στον κυβερνοχώρο, η πλειονότητα των περιστατικών παραβίασης δεδομένων μπορεί να αποφευχθεί.
Η εκπαίδευση, η κατάρτιση και η ευαισθητοποίηση είναι οι πιο σημαντικοί τρόποι αντιμετώπισης της κοινωνικής μηχανικής. Οι χρήστες που κατανοούν τι είναι η κοινωνική μηχανική και πώς λειτουργεί μπορούν να αποφύγουν πιο αποτελεσματικά τις επιθέσεις κοινωνικής μηχανικής.
Οι οργανισμοί πρέπει να ορίζουν διαδικασίες σχετικά με τη προστασία των πληροφοριακών συστημάτων τους και να επενδύσουν σε εκπαιδεύσεις ευαισθητοποίησης κοινωνικής μηχανικής για να εξοπλίσουν τους υπαλλήλους τους, ώστε να μπορούν να αντέξουν επιθέσεις κοινωνικής μηχανικής.
Σύμφωνα με τον Kevin Mitnick η Κοινωνική Μηχανική είναι μία αληθινή μορφή τέχνης…ας την απολαύσουμε.

7. ΒΙΒΛΙΟΓΡΑΦΙΑ

- Ελληνική βιβλιογραφία

  - Αναγνωστόπουλος, Β. (2021). Κοινωνική Μηχανική (Social Engineering): Τεχνικές χειραγώγησης ατόμων για την απόσπαση πληροφορίας μέσω υπολογιστικών συστημάτων.
  - Αποστόλου, Μ. Χ. (2014). *Συγκριτική ανάλυση της κατάστασης κυβερνοασφάλειας των χωρών-μελών της ΕΕ* (Master's thesis).
  - Βάββας, Ι. (2010). Τεχνικές Social Engineering για την παραβίαση προσωπικών δεδομένων.
  - Βλάχου Δ., Ζαμπατή Μ., Κοντραφούρη Χ. (2020). Πανεπιστήμιο Πειραιά. *Η επίδραση των κυβερνοεπιθέσεων στη μετεξέλιξη της κυβερνοασφάλειας*: Η περιπτωσιολογική μελέτη της Εσθονίας
  - Μούρτος, Θ. (2020). *Η θεωρία του social engineering: εργαλεία τεχνικές και τρόποι άμυνας κατά των επιθέσεων phishing* (Master's thesis, Πανεπιστήμιο Πειραιώς).
  - Μπλέτσας, Ι. (2015). Κοινωνική μηχανική και ασφάλεια ηλεκτρονικών υπολογιστών.
  - Νάρη, Ε. (2005). *Συστήματα ανίχνευσης εισβολέων* (Bachelor's thesis).
  - Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ, 2020
  - Σταματινός, Μ. (2015). Πολιτικές ασφάλειας πληροφοριακών συστημάτων.
  - Φραγκοπούλου, Β. (2019). Επιθέσεις κοινωνικής μηχανικής σε κοινωνικά δίκτυα: παρούσα κατάσταση, ταξινόμηση επιθέσεων και μέθοδοι προστασίας

- Αγγλική βιβλιογραφία

  - Aldawood, H., & Skinner, G. (2020). An advanced taxonomy for social engineering attacks. *International Journal of Computer Applications*, *177*(30), 1-11.
  - Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.

- Ιστοσελίδες

- https://www.imperva.com/learn/application-security/social-engineering-attack,2022

- https://el.wikipedia.org/wiki/%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1, 2022

- https://www.philenews.com/koinonia/eidiseis/article/1025005/kampanaki-ga-kybernoasfaleia-dechomaste-epitheseis,2022

- https://www.philenews.com/eidiseis/paraskinio/article/934790,2022

- https://www.eset.com/gr/social-engineering-business/,2022

- https://el.wikipedia.org/wiki/%CE%A3%CE%BA%CE%AC%CE%BD%CE%B4%CE%B1%CE%BB%CE%BF_%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD_Facebook-Cambridge_Analytica,2022
- http://vr.arch.uth.gr/VR-Arch/PDF/VR-01_Cyberspace.pdf,2022

- https://el.wikipedia.org/wiki/%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%87%CF%8E%CF%81%CE%BF%CF%82,2022

- https://www.cloudflare.com/learning/access-management/phishing-attack/,2022

- https://www.techtarget.com/searchsecurity/definition/dumpster-diving