ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

"Κοινωνική Μηχανική και Ασφάλεια Πληροφοριών"

Χρήστος Δ. Βασιλοκώστας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
Επιβλέπων
Γ. ΣΤΑΜΟΥΛΗΣ

Λαμία, 8 Νοεμβρίου έτος 2019

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

"Social Engineering and Information Security"

Christos D. Vasilokostas

Master thesis

G. Stamoulis

Lamia

8 November 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ
ΚΑΤΕΥΘΥΝΣΗ
«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»

“Κοινωνική Μηχανική και Ασφάλεια Πληροφοριών”

Χρήστος Δ. Βασιλοκώστας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων Καθηγητής

Γ. Σταμούλης

Λαμία, 8 Νοεμβρίου, έτος 2019

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ: Χρήστος Δ. Βασιλοκώστας

Ημερομηνία: 25/08/2019

Υπογραφή

“Κοινωνική Μηχανική και Ασφάλεια Πληροφοριών”

Χρήστος Δ. Βασιλοκώστας

Τριμελής Επιτροπή:

Γεώργιος Σταμούλης

Μαρία Κοζύρη

Δαδαλιάρης Αντώνιος

Επιστημονικός Σύμβουλος:

Ιωάννης Φιλλιπόπουλος

1. ΠΕΡΙΕΧΟΜΕΝΑ:

Σκοπός της Εργασίας 9
Εισαγωγικό Σημείωμα 9
1.1 Ορισμός Κοινωνικής Μηχανικής 10
1.2 Λειτουργία 11
1.3 Ποιός είναι ο social engineer 12
1.4 Παραδείγματα Κοινωνικής Μηχανικής. 13
1.5 Τεχνικές social engineer για να αποσπάσει πληροφορίες. 15
1.6 Ηλεκτρονικό Ψάρεμα ή Phishing. 16
1.7 Κακόβουλα Προγράμματα 21
1.9 Εργαλεία για την επίτευξη των στόχων του social engineer 25
1.10 Vishing 27
1.11 Κοινωνική Μηχανική και Μέσα Κοινωνικής Δικτύωσης 29
2.0 Τρόποι προστασίας κατά της κοινωνικής μηχανικής – ασφάλεια πληροφοριών 32
2.1 Εισαγωγή 32
2.2 Ανθρώπινος Παράγοντας 32
2.3 Άμυνα σε επιθέσεις κοινωνικής μηχανικής 34
2.4 Αντιμετώπιση επεισοδίου κοινωνικής μηχανικής 36
2.5 Τρόποι αντιμετώπισης Ηλεκτρονικού Ψαρέματος (phishing): 37
2.6 Χρήση Intrution Detected Systems (IDS) 40
2.7 Μια άλλη χρήση των μεθόδων Κοινωνικής Μηχανικής 41
ΕΠΙΛΟΓΟΣ 42
Βιβλιογραφία: 43

2. ΕΙΚΟΝΕΣ :

1. ΕΙΚΟΝΑ 1. Τι είναι κοινωνική Μηχανική 10
2. ΕΙΚΟΝΑ 2. Ποιός είναι ο social engineer 12
3. ΕΙΚΟΝΑ 3. Παραδείγματα κοινωνικής Μηχανικής 14
4. ΕΙΚΟΝΑ 4. Ηλεκτρονικό Ψάρεμα (Phishing).....16
5. ΕΙΚΟΝΑ 5. Ψάρεμα κωδικών..... 18
6. ΕΙΚΟΝΑ 6. Spear Phishing 20
7. ΕΙΚΟΝΑ 7. Trojan Horse-Worm..... 23
8. ΕΙΚΟΝΑ 8. Τηλεφωνικός διάλογος..... 24
9. ΕΙΚΟΝΑ 9. Vishing 28
10. ΕΙΚΟΝΑ 10. Μέσα κοινωνικής Δικτύωσης 29
11. ΕΙΚΟΝΑ 11. Malvertising..... 31
11. ΕΙΚΟΝΑ 12. Τρόποι Αντιμετώπισης Κοινωνικής Μηχανικής.....32
12. ΕΙΚΟΝΑ 13. Ανθρώπινος Παράγοντας..... 33
13. ΕΙΚΟΝΑ 14. Άμυνα σε επιθέσεις κοινωνικής μηχανικής 35
14. ΕΙΚΟΝΑ 15. IDS 40
15. ΕΙΚΟΝΑ 16. Η ασφάλεια είναι υπόθεση ισορροπιών. 42

Σκοπός της Εργασίας

Η χρήση των υπολογιστικών συστημάτων σε συνδιασμό με τις δυνατότητες του διαδικυακού ιστού, αποτελούν πλέον αναπόσπαστο και αναγκαίο κομμάτι της ζωής μας. Μέσα στα συστήματα αυτά αποθηκεύονται τεράστια δεδομένα (προσωπικά και επαγγελματικά) των οποίων η ασφάλεια και προστασία είναι μια απο τις σημαντικότερες υποθέσεις της σύγχρονης ζωής.

Σκοπός αυτής της εργασίας είναι η προβολή και ανάλυση της κοινωνικής μηχανικής, μιας σύγχρονης σχετικά «επιστήμης» που χρησιμοποείται ως τρόπος για την απόσπαση/ παραβίαση προσωπικών και εμπιστευτικών δεδομένων με την εφαρμογή διαφόρων τεχνικών, τις οποίες και θα αναπτύξω. Συνεπώς, θα εστιάσω στους τρόπους τους οποίους ο κοινωνικός μηχανικός ‘’μηχανεύεται’’ για να παγιδεύσει τα θύματα του, καθώς και τους τρόπους για την αντιμετώπιση αυτών.

Εισαγωγικό Σημείωμα

1. Ολοένα και περισσότερο, η ζωή μας συνδέεται και εξαρτάται σε μεγάλο βαθμό απο τα υπολογιστικά συστήματα και το διαδίκτυο. Τα μέσα κοινωνικής δικτύωσης έχουν καθιερωθεί στην ζωή μας ως μια νέα “μόδα” μέσα απο την οποία πραγματοποιείται η ενημέρωση, η διασκέδαση, η κοινωνικοποίηση, η προβολή του ατόμου καθώς και η αναγνώρισή του απο το υπόλοιπο κοινωνικό διαδυκτιακό σύνολο. Το αυτόβουλο ηλεκτρονικό φακέλωμα πλέον είναι γεγονός, φακέλωμα που δεν αφορά μόνο στα προσωπικά στοιχεία αλλά και στην προσωπικότητα του ατόμου. Αυτό όμως οδηγεί στην δημιουργία προβλημάτων ασφαλείας τόσο για την ιδιωτικότητα του ατόμου, όσο και στον επαγγελματικό του χώρο.

2. Πολλοί επαγγελματίες πάνω σε πληροφοριακά συστήματα (information Technology-IT) έχουν την λανθασμένη εντύπωση οτι έχουν κάνει τα συστήματα της εταιρείας τους άτρωτα σε επιθέσεις επειδή έχουν αναπτύξει κάποια τυποποιημένα προιόντα ασφαλείας όπως firewalls, IDS (Intrusion Detection Systems) καθώς και αυστηρές πολιτικές αυθεντικότητας και χρήσης των συστημάτων.

Είναι γεγονός οτι όσο οι τεχνικοί υπολογιστών αναπτύσουν ολοένα και πιο ασφαλή συστήματα, εξαλείφοντας τις τρωτότητες και τις αδυναμίες αυτών, τόσο πιο πολύ οι επιτιθέμενοι θα προσπαθούν να εκμεταλλευτούν τις αδυναμίες του ανθρώπινου παράγοντα για να εισχωρήσουν σε αυτά. Οι κοινωνικοί μηχανικοί ισχυρίζονται πως το να σπάσεις ένα ‘’ανθρώπινο firewall’’ είναι συνήθως πιο εύκολο απο το να σπάσεις ένα firewall δικτύου διότι απαιτεί μικρότερο κόστος, χρόνο και εμπεριέχει μικρότερο ρίσκο. Σε αυτήν την εργασία θα αναδείξω πόσο ευάλωτος μπορεί να γίνει ένας χρήστης υπολογιστών στην επίθεση ενός social engineer χρησιμοποιόντας την γνώση του περί υπολογιστών σε συνδιασμό με τις κοινωνικές του δεξιότητες, καθώς και θα αναλύσουμε τους τρόπους και τις τεχνικές αντιμετώπισης κατά των τεχνασμάτων της κοινωνικής μηχανικής σε συνδιασμό με την ασφάλεια των πληροφοριών.

3. Αξίζει να σημειωθεί οτι, παρόλο που η μέθοδος της κοινωνικής μηχανικής δεν είναι ευρέως γνωστή, οι ειδικοί ασφαλείας υπολογιστικών συστημάτων ανα τον κόσμο συμφωνούν οτι όσο τα συστήματα εξελίσσονται και γίνονται πιο “έξυπνα” και ασφαλή, η μέθοδος αυτή θα αποτελέσει τον μεγαλύτερο μελλοντικό κίνδυνο για τα συστήματα αυτά. Στην εργασία αυτή λοιπόν, θα προσπαθήσω να αναδείξω τους κινδύνους που απορρέουν απο την κοινωνική μηχανική καθώς και να αναπτύξω τρόπους αντιμετώπισης και συμβουλές ασφαλείας.

ΑΝΑΛΥΣΗ

Κεφάλαιο 1.0
Κοινωνική Μηχανική (Social Engineering)

1.1 Ορισμός Κοινωνικής Μηχανικής

1. Η κοινωνική μηχανική έχει κατά καιρούς ονομαστεί ως η «επιστήμη της εκμετάλλευσης του έμψυχου υλικού», «τέχνη της απάτης», «μυστικά της εξουσίας», «χειρισμός των κατωτέρων», «real politik», κ.ά…

ΕΙΚΟΝΑ 1. Τι είναι κοινωνική Μηχανική

2. Πρόσφατα, ο όρος κοινωνική μηχανική εκτός απο την ερμηνεία της ως “η τέχνη της εξουσίας’’ για την χειραγώγιση των κατωτέρων σε γνωστικό και μορφωτικό επίπεδο ανθρώπων, άρχισε να χρησιμοποείται ευρύτατα στους κύκλους των βιομηχανικών κατασκόπων και χάκερς και ως το σύνολο των τεχνικών/ μεθόδων εκείνων με τις οποίες οι επιτήδειοι μπορούν να εκμαιεύσουν σημαντικές πληροφορίες, και εν συνεχεία χρήματα, εκμεταλλεύομενοι την αφέλεια, την άγνοια ή την χαλαρότητα κάποιων ανθρώπων. Αν και η τελευταία ερμηνεία του όρου της κοινωνικής μηχανικής δεν συμπίπτει ακριβώς με την εξουσιαστική κοινωνική μηχανική, παρ’όλα αυτά και στις δύο περιπτώσεις ο σκοπός είναι η κοροϊδία και εξαπάτηση των ανυποψίαστων ανθρώπων.

3. Μια άλλη προσέγγιση της έννοιας της κοινωνικής μηχανικής είναι η εξής: **‘’Κοινωνική μηχανική** (Social engineering) είναι η πράξη της

προφορικής χειραγώγησης ατόμων με σκοπό την απόσπαση πληροφοριών. Αν και είναι παρόμοια με το τέχνασμα ή την απλή απάτη, ο όρος είναι κυρίως συνδεδεμένος με την εξαπάτηση ατόμων με σκοπό την απόσπαση εμπιστευτικών πληροφοριών που είναι απαραίτητες για την πρόσβαση σε κάποιο υπολογιστικό σύστημα. Συνήθως αυτός που την εφαρμόζει δεν έρχεται ποτέ πρόσωπο με πρόσωπο με το άτομο που εξαπατά ή παραπλανά. Παρόλο που ο όρος ίσως να μην είναι ακριβής ή επιτυχημένος έχει πλέον καθιερωθεί.'' [1]

4. Ο πρώην εγκληματίας υπολογιστών, βιομηχανικός κατάσκοπος και αργότερα σύμβουλος ασφαλείας πληροφορικών συστημάτων Κέβιν Μίτνικ, ένας απο τους πιο διάσημους Αμερικανούς χάκερς διέδωσε τον όρο «κοινωνική μηχανική», επισημαίνοντας ότι είναι πολύ ευκολότερο να ξεγελάσεις κάποιον να δώσει έναν κωδικό πρόσβασης για ένα σύστημα από το να προσπαθήσεις να τον σπάσεις. Γράφει στο βιβλίο του, ''Η τέχνη της απάτης'': «Οι κοινωνικοί μηχανικοί χρησιμοποιούν την επιρροή και την πειθώ τους για να εξαπατήσουν τα θύματα τους, είτε πείθοντάς τα ότι η ταυτότητα τους είναι άλλη απο την πραγματική, είτε οδηγώντας τα σε ανεπίτρεπτες πράξεις.....».

1.2 Πως Λειτουργεί

1. Ο Αμερικανός ηθοποιός, επιχειρηματίας και πολιτικός P.T. Barnum έμεινε γνωστός στην ιστορία λέγοντας την ρήση : «κάθε ένα λεπτό γεννιέται κι ένα κορόιδο». Αυτή η ρήση περιγράφει ακριβώς τις σκέψεις, τα συναισθήματα και τις συμπεριφορές των social engineers ως προς τους συνανθρώπους τους ή διαφορετικά ως προς τα μελλοντικά εν δυνάμει θύματα τους. Μια συνηθισμένη τακτική που χρησιμοποιούν οι social engineers είναι η ανοικοδόμιση εμπιστοσύνης, ο φόβος και η επιβολή της ιεραρχίας ως προς τους επιτιθέμενους[2].

2. Η κοινωνική μηχανική στηρίζεται κυρίως στην ανθρώπινη περιέργεια, στην απληστία και στην άγνοια, καθόσον εκμεταλλεύεται την ανθρώπινη φύση και την ταυτόχρονη έλλειψη σωστής εκτίμησης / αξιολόγησης που έχουν οι πληροφορίες στην Κοινωνία της Πληροφορίας οδηγώντας στην έλλειψη προσοχής και διασφάλισης της πληροφορίας. Πολλοί θεωρούν ότι ένα καλό αντιϊκό ή ένα σωστά τοποθετημένο firewall μπορεί να τους προστατεύσει, αλλά αυτά δρουν μόνο για τους ευρέως γνωστούς ιούς και για τις ευρέως γνωστές τεχνικές και όχι για έναν ειδικά κατασκευασμένο "ιό". Πολλοί, επίσης, είτε λόγω ευπιστίας είτε λόγω ευγένειας δεν αρνούνται να δώσουν στοιχεία σε κάποιον που τους το ζητάει ευγενικά ή κάτω από δήθεν "πίεση".

3. Για παράδειγμα μπορούμε να πάρουμε τα σώματα ασφαλείας όπου το προσωπικό έχει εμποτιστεί με τις αρχές του σεβασμού ως προς την ιεραρχία και του βαθμού απο την πρώτη μέρα που κατατάγησαν στις αντίστοιχες σχολές εκπαίδευσης. Εφόσον τώρα ένας social engineer παρουσιαστεί μέσω τηλεφώνου ως ένας υψηλού βαθμού αξιωματικός, κατα

---

[1] ΧΑΚΕΡ ΕΠΙΘΕΣΗ ΚΑΙ ΑΜΥΝΑ, Γκιούρδας, 2η Έκδοση (2001),σελ. 555.

[2] http://osarena.net/koinoniki-mihaniki-ti-einai-i-shesi-tis-me-tin-tehnologia-social-engineer

πολύ αρχαιότερος απο το άτομο στον οποίο πρόκειται να μιλήσει, αυτομάτως το θύμα θα κρατήσει την στάση ¨Δεν ρωτάω και δεν αμφισβητώ ανωτέρους μου¨ ως ένδειξη σεβασμού, εκτίμησης και δέους στο πρόσωπο αυτού. Με άλλα λόγια, ο βαθμός σε κάποιο άτομο προσφέρει το προνόμοιο του να μη ελέγχεται και αμφισβητείται απο κάποιο άλλο άτομο κατώτερου βαθμού λόγω του σεβασμού προς την ιεραρχία και την εμπειρία του πρώτου. Με τον ίδιο τρόπο οι social engineers συνήθως κάνουν χρήση των εξουσιών μιας θέσεως, του βαθμού και της ιεραρχίας ως εργαλεία στις επιθέσεις τους κατά επιχειρήσεων, τραπεζών και κρατικών οργανισμών.

4. Ο άμεσος στόχος του social engineer δεν είναι πάντα η αποκάλυψη ενός κωδικού. Για κάποιον που θέλει να διεισδύσει σε ένα υπολογιστικό σύστημα πολλές φορές είναι αρκετή ακόμα και η απλή γνώση του αριθμού έκδοσης του λειτουργικού συστήματος ή άλλων προγραμμάτων που χρησιμοποιεί ο χρήστης. Με αυτές τις πληροφορίες μπορεί να μάθει αν υπάρχουν "πίσω πόρτες" (backdoors) στα προγράμματα και να τις αξιοποιήσει.

5. Άλλες πληροφορίες που μπορεί να συλλέξει κάποιος, και που πιθανά να του είναι χρήσιμες, όπως είναι οι ημερομηνίες γέννησης, τα ονόματα των παιδιών ενός γονέα, τα ονόματα των υπευθύνων για τη μηχανογράφηση κ.α. συλλέγονται είτε μέσω συνομιλίας είτε απο τα κοινωνικά δίκτυα και τις ιστοσελίδες της εταιρείας. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν αργότερα είτε σε απευθείας τηλεφωνική συνομιλία, είτε μέσω ηλεκτρονικού ταχυδρομείου, είτε τέλος σε άμεσα μηνύματα, για να πεισθεί ο συνομιλητής-θύμα ότι πρόκειται περί κάποιου γνωστού ή συναδέλφου και έτσι να του αποσπαστούν ακόμη περισσότερες πληροφορίες ή, ακόμα καλύτερα, κάποιον κωδικό πρόσβασης.

1.3 Ποιός είναι ο social engineer

1. Πολλοί άνθρωποι σχηματίζοντας την εικόνα ενός χάκερ στο μυαλό τους, έχουν την εντύπωση οτι είναι ένα άτομο απομακρυσμένο απο το υπόλοιπο κοινωνικό

ΕΙΚΟΝΑ 2. Ποιός είναι ο social engineer

σύνολο, αποξενωμένο, μοναχικό, ντροπαλό και εσωστρεφή, του οποίου η μοναδική ενασχόληση και συντροφιά είναι η οθόνη του υπολογιστή του. Ακόμη αναφέρονται για ένα άτομο με κοινωνική φοβία, το οποίο επικοινωνεί με τους συνανθρώπους του μόνο μέσω μυνημάτων απο τα μέσα κοινωνικής δικτύωσης, forums και τα emails και το οποίο άτομο έχει απεριόριστες και εξεζητημένες γνώσεις καθώς και δεξιότητες στον χειρισμό ενός υπολογιστικού συστήματος. Επιπλέον θεωρείται ένα άτομο με καταστροφικές τάσεις που μοναδικός του στόχος είναι η πρόκληση ‘’ηλεκτρονικών ζημιών” σε επιχειρήσεις, κυβερνητικούς οργανισμούς και εταιρείες με απώτερο σκοπό την αυτοεπιβεβαίωση ή και αναγνώριση απο τον κύκλο των υπολοίπων χάκερς, των δεξιοτήτων και δυνατοτήτων τους πάνω σε υπολογιστικά συστήματα και την ασφάλεια αυτών καθώς επίσης και την αποκόμιση χρημάτων με μή νόμιμα μέσα.

2. Και όντως αυτή η εντύπωση των περισσοτέρων ανθρώπων για το τι είναι χάκερ είναι ορθή, όμως στην περίπτωση ενός κοινωνικού μηχανικού, το άτομο αυτό ενώ κατέχει τις δεξιότητες ενός χάκερ, παράλληλα έχει αναπτύξει κοινωνικές ικανότητες και δεξιότητες σε τέτοιο βαθμό που να του παρέχουν την δυνατότητα της χειριστικής συμπεριφοράς ως προς τους συνανθρώπους του. Αυτό έχει ως συνέπεια την ευκολία με την οποία ένας κοινωνικός μηχανικός θα μπορεί να αναπτύξει με τα υποψήφια θύματα του, μια σχέση οικειότητας και εμπιστοσύνης, την οποία και θα εκμεταλλευτεί για την επίτευξη του δόλιου του σχεδίου.

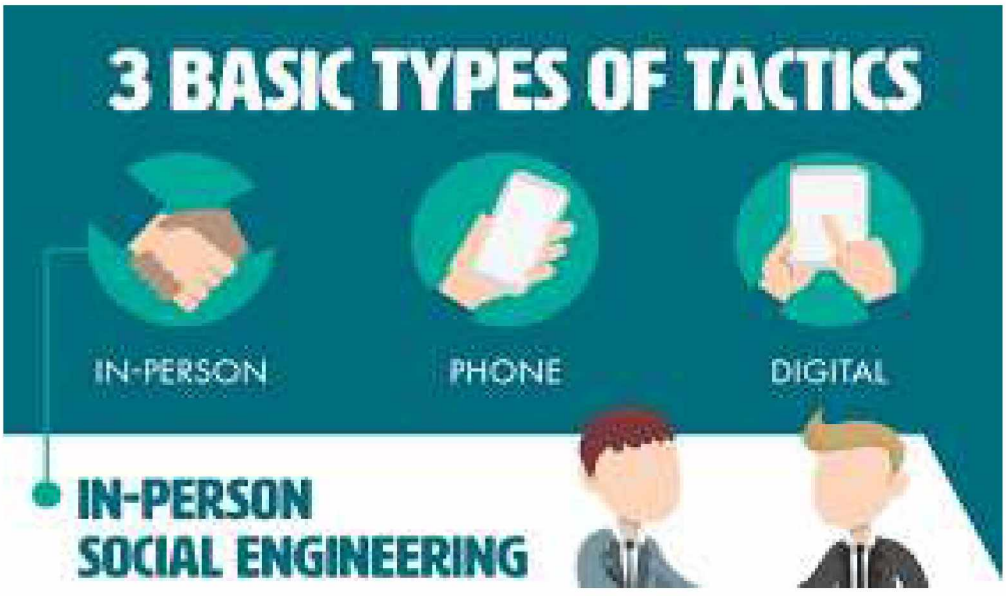
3. Συγκεκριμένα, ο κοινωνικός μηχανικός κατά την προσέγγιση του με το υποψήφιο θύμα συνήθως αναμένει συμπεριφορές υποψίας, καχυποψίας και αντίστασης. Για τον λόγο αυτό είναι πάντα προετοιμασμένος να μετατρέψει τα αισθήματα της αμφιβολίας και της δυσπιστίας, μέσω της συζήτησης και της πειθούς, σε εκείνα της ασφάλειας και της εμπιστοσύνης. Ένας καλός social engineer σχεδιάζει την επίθεση του με στρατηγική τέτοια όπως σε έναν αγώνα σκάκι, πάντα σκέφτεται την επόμενη κίνηση του προβλεποντας τις τυχόν ερωτήσεις του υποψηφίου θύματος και προετοιμάζεται για τις αντίστοιχες απαντήσεις.

Ως αποτέλεσμα, ένας social engineer δύναται να αποσπάσει οποιαδήποτε πληροφορία χρησιμοποιόντας ως εργαλείο του την ‘’in-person’’ επικοινωνία, και αργότερα κάνοντας χρήση την πληροφορία αυτή μαζί με άλλες αποκτηθέντες απο άλλους έτερους τρόπους (που θα αναλυθούν παράκατω) θα την χρησιμοποιήσει για να αποσπάσει εμπιστευτικά προσωπικά δεδομένα ή εκείνους τους κωδικούς που απαιτούνται για να «ξεκλειδώσει» κάποιον λογαριασμό.

1.4 Παραδείγματα Κοινωνικής Μηχανικής.

1. Ένας social engineer αφού πρώτα έχει κάνει την έρευνα του και έχει εντοπίσει την εταιρεία-στόχο που τον ενδιαφέρει, φροντίζει να ενημερωθεί για το δομικό της πλαίσιο (οργανόγραμμα Διοίκησης), τον τρόπο λειτουργίας της και την ειδική ορολογία-φρασεολογία (γνωστή ως αργκό) που χρησιμοποιείται απο τα στελέχη της. Αφού έχει συγκεντρώσει όλες αυτές τις πληροφορίες στα χέρια του, ο κοινωνικός μηχανικός περνάει στο επόμενο βήμα. Το βήμα αυτό είναι να καλέσει στο τηλεφωνικό κέντρο της εταιρείας και προσποιούμενος κάποιον υπάλληλο της εταιρείας αυτής να ζητήσει απο την

άλλη άκρη της γραμμής να τον ενημερώσει για τον τηλεφωνικό αριθμό του τεχνικού τμήματος υπολογιστών (computer room – IT department) καθόσον όπως ισχυρίζεται, υπάρχει ένα πρόβλημα με το υπολογιστικό του σύστημα και απαιτείται η συνδρομή του διαχειριστή (administrator). Χρησιμοποιώντας το τηλεφωνικό νούμερο καθώς και το όνομα του διαχειριστή ή οτιδήποτε άλλες πληροφορίες έχει εκμαιεύσει απο την προηγούμενη συνομιλία του, καλεί στο computer room και ζητά να συνομιλήσει με τον διαχειριστή. "Απο εδώ και πέρα ξεδιπλώνονται οι κοινωνικές δεξιότητες του social engineer. Εάν ο διαχειριστής απουσιάζει, κάτι που είναι σύνηθες για αυτήν την θέση λόγω φόρτου εργασίας, και απαντήσει στο τηλέφωνο κάποιος απο το βοηθητικό προσωπικό, τότε ο social engineer ζητάει να μάθει που βρίσκεται ο διαχειριστής καθώς και ποιά είναι τα στοιχεία του συνομιλούντος (όνομα και ιδιότητα), προσποιούμενος κάποιον συνάδελφο απο άλλο τμήμα της ίδιας εταιρείας, ο οποίος αντιμετώπιζει κάποιο πολύ σοβαρό πρόβλημα και που αναζητά άμεσα λύση. Κλείνει το τηλέφωνο και ξανακαλεί, προσποιούμενος τώρα τον διαχειριστή και ζητάει απο τον υπάλληλο που συνομίλησε προηγουμένος, τον οποίο καλεί και με το μικρό του όνομα (αφού το έχει μαθει μέσω της προηγούμενης συνομιλίας), να πληκτρολογήσει κάποιες εντολές και να αλλάξει ένα password, συμφώνως των οδηγιών που του μεταβιβάζει. Σε αυτό το παράδειγμα φαίνεται ένας απλός τρόπος με τον οποίο ο social engineer μπορεί να παραβιάσει την ιδιωτικότητα ενός υπολογιστή μιας εταιρείας, συνεπώς και να αποκτήσει όλες εκείνες τις πληροφορίες και αρχεία που αυτό περιέχει για να πετύχει τον δόλιο σκοπό του."[3]



ΕΙΚΟΝΑ 3. Παραδείγματα κοινωνικής Μηχανικής

2. Στο πρώτο παράδειγμα είδαμε λίγο απλουστευμένα πως ένας social engineer λειτουργεί και στήνει την απάτη του μέσα σε σύντομο χρονικό διάστημα μέσω τριών (3) τηλεφωνικών κλήσεων σε συγκεκριμένα γραφεία μιας εταιρείας. Το παράδειγμα αυτό δόθηκε για να κατανοήσουμε τις μεθόδους που

[3] Ασφάλεια της πληροφορίας, Ανδρέας Σουρής, Δημήτρη Πατσός, Νίκος Γρηγοριάδης, έκδοση 1η, 2004, Εκδόσεις Νέων Τεχνολογιών, σελ 44

μηχανεύεται ο social engineer, διότι στην πραγματικότητα οι επαγγελματίες επιτήδιοι συλλέγουν τις πληροφορίες κομμάτι, κομμάτι και σε βάθος χρόνου, εισχωρόντας βαθύτερα και με μεγάλη λεπτομέρεια στα ενδότερα, εκμαιεύοντας πληροφορίες για το πως λειτουργεί ένας οργανισμός/ εταιρεία/ τράπεζα. Για παράδειγμα, το χακάρισμα της RSA, μια απο της παγκόσμιες κορυφαίες εταιρείες ασφαλείας Η/Υ στον κόσμο. Η εταιρία RSA "χτυπήθηκε" με μεθόδους κοινωνικής μηχανικής, δηλαδή ο social engineer μηχανεύτηκε τρόπους για την πρόσβαση στις υποδομές των αρχείων της εταιρείας υποκλέπτοντας στοιχεία ταυτότητας και ασφαλείας Η/Υ σαράντα χιλιάδων επιχειρήσεων (πελατών της RSA).

Το πρώτο βήμα της επίθεσης ήταν η αποστολή ενός ή δύο ταυτόχρονων emails ηλεκτρονικού ψαρέματος σε δύο απο τα σχετικά χαμηλόβαθμα στελέχη της εταιρίας. Το θέμα των emails ήταν «Recruiting 2011», ενώ τα μυνήματα είχαν ως συννημένο, ένα αρχείο Excel που περιείχε κακόβουλο λογισμικό. Παρ΄όλο που το αρχείο καταχωρήθηκε αυτομάτως στα junk files, ο ένας απο τους δύο υπαλλήλους το ανέσυρε απο εκεί και το άνοιξε, με συνέπεια να τρέξει το κακόβουλο λογισμικό και να μολύνει τον υπολογιστή του. Προγενέστερα της αποστολής των emails είχε προηγηθεί η έρευνα του social engineer στα μέσα κοινωνικής δικτύωσης όπως το LinkedIn έτσι ώστε ο επιτιθέμενος να είχε εντοπίσει τα ονόματα και την θέση που κατείχαν στην εταιρεία τα θύματα του, και αναζητώντας άλλα στοιχεία από άλλους υπαλλήλους της εταιρείας ο social engineer μπόρεσε να «μαντέψει» τις διευθύνσεις των emails των υπολοίπων, χρησιμοποιόντας ένα μοτίβο της μορφής όπως fisrt.last@rsa.com.

Οταν το κακόβουλο λογισμικό εγκαταστάθηκε στον Η/Υ του υπαλλήλου, ο social engineer ψάχνοντας τα αποθηκευμένα αρχεία καθώς και έχοντας πρόσβαση στα εσωτερικά RSA web sites, μπορούσε να συλλέξει στοιχεία για να παγιδεύσει υψηλότερα υστάμενα στελέχη. Συνεχίζοντας την "στοχοποίηση" του σε βάθος χρόνου και αναρηχώντας όλο και πιο πολύ ψηλά στο οργανόγραμμα της ιεραρχείας της εταιρείας, ο social engineer τελικά έφτασε στον υψηλότερο στόχο του και υπέκλεψε τις πληροφορίες που αναζητούσε για να επιτύχει τον σκοπό του.[4]

1.5 Τεχνικές social engineer για να αποσπάσει πληροφορίες.

1. Σύμφωνα με τον Μίτνικ [5]: «..ένας social engineer μπορεί να στείλει έναν ιό ή Δούρειο Ίππο ως συννημμένο αρχείο σε ένα email, να ανακαλύψει τα πλήκτρα που πάτησε το θύμα-χρήστης χρησιμοποιόντας διαθέσιμα προγράμματα, να αφήσει μια δισκέτα ή ένα cd με επιβλαβή κώδικα (malicious software) στον χώρο εργασίας του θύματος, να χρησιμοποιήσει ψεύτικα pop-up παράθυρα ζητώντας να κάνει log on ή να συνδεθεί με το δικτυακό του password, να στείλει δωρεάν λογισμικό για να το εγκαταστήσει το θύμα...».

2. Η κοινωνική μηχανική μπορεί να χωριστεί στις ακόλουθες τρεις κατηγορίες:

---

[4] https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/
[5] The art of Human hacking, christofer Hanargy, John Wiley & Sons, 29 Νοε 2010.

α. Στην πρώτη κατηγορία η απάτη επιτελείται βασιζόμενη στην γνώση πληροφοριακών συστημάτων. Ο social engineer παραπλανά τον χρήστη-θύμα κάνοντας τον να πιστεύει οτι αλληλεπιδρά με ένα αυθεντικό πρόγραμμα υπολογιστή και έτσι να του παρέξει εμπιστευτικές προσωπικές πληροφορίες.

β. Στην δεύτερη κατηγορία η απάτη επιτελείται βασιζόμενη στις κοινωνικές δεξιότητες του social engineer, ο οποίος εκμεταλλεύεται την άγνοια του θύματος και την κοινωνική και αλτρουϊστική φύση του ανθρώπου να βοηθά τον συνάνθρωπο του όταν αυτός αντιμετωπίζει προβλήματα.

γ. Στην τρίτη κατηγορία η απάτη επιτυγχάνεται με τον συνδιασμό της γνώσης πάνω σε πληροφοριακά συστήματα και την χρήση των κοινωνικών δεξιοτήτων.

Στην πρώτη κατηγορία ανήκουν οι απάτες με την χρήση των ηλεκτρονικών διευθύνσεων (emails):

Ηλεκτρονικό Ψάρεμα ή Phishing.

ΕΙΚΟΝΑ 4. Ηλεκτρονικό Ψάρεμα (Phishing)

α. Το ηλεκτρονικό ψάρεμα γνωστό ως phishing (αποτελεί παραφθορά της λέξης fishing λόγω της χρήσης και στις δύο περιπτώσεις «δολώματος» για να παγιδευτεί το θύμα) αποτελείται απο πέντε (5) στάδια:

(1). Σχεδιασμός. Ο phisher ερευνά και εντοπίζει τον υποψήφιο στόχο του (επιχείρηση, οργανισμός, τράπεζα) και καθορίζει τον τρόπο με τον οποίο θα εντοπίσει και θα υποκλέψει τις ηλεκτρονικές διευθύνσεις των ατόμων εκείνων που θα γίνουν ακούσια τα μέσα πληροφόρησης και κατ'επέκταση τα εργαλεία του για την επίτευξη του σκοπού του.

(2). Εγκατάσταση. Ο phisher αρχίζει να εγκαθιστά τις τεχνικές του για την παράδοση των emails - δολωμάτων και την συλλογή δεδομένων.

(3). Επίθεση. Αποστολή “παγιδευμένων” emails με διεύθυνση αποστολέα μια αξιόπιστη πηγή (χρήση τεχνικών spoofing) και συννημένο λίνκ με χρήση ψεύτικης αλλά αληθοφανούς ιστοσελίδας.

(4). Συλλογή πληροφοριών. Ο phisher καταγράφει τις πληροφορίες που έχει υποκλέψει απο τα ψεύτικα sites.

(5) Εκτέλεση Απάτης. Ο phisher επεξεργάζεται και χρησιμοποιεί όλες αυτές τις πληροφορίες που έχει συλλέξει για να πραγματοποιήσει την σχεδιασμένη του απάτη.

β. Αναλυτικά, κατά την διαδικασία του phishing ένας επιτήδειος κοινωνικός μηχανικός, ή αλλιώς στην περίπτωση αυτή ένας phisher, στέλνει συνήθως ένα email στο υποψήφιο θύμα του ως μια επίσημη ειδοποίηση. Στην ειδοποίηση αυτή, ως διεύθυνση αποστολέα εμφανίζεται μια διεύθυνση που φαινομενικά είναι ασφαλής και αξιόπιστη γιατί μπορεί να παραπέμπει σε κάποια νόμιμη, γνωστή και ευηπόληπτη εταιρεία (τράπεζα, εταιρεία πιστωτικής κάρτας ή εταιρεία ηλεκτρονικού εμπορίου) ή κάποιο επώνυμο/ αξιόπιστο φυσικό πρόσωπο. Εν συνεχεία, το περιεχόμενο του μυνήματος παροτρύνει/ κατευθύνει τον παραλήπτη να ανοίξει ένα συνημμένο λινκ με σκοπό δήθεν να ενημερώσει τις προσωπικές του πληροφορίες, συνήθως με το πρόσχημα οτι είναι επείγουσα ανάγκη για "επιβεβαίωση της ταυτότητάς του", λόγω του οτι ο λογαριασμός του έχει δεχθεί επίθεση από hackers ή οτι έχει λήξει και πρέπει να ενημερωθεί άμεσα ώστε να μην κλειδωθεί για λόγους ασφαλείας. Όμως, το λίνκ αυτό οδηγεί σε κάποιον ψεύτικο αλλά αληθοφανή ιστότοπο κατασκευασμένο απο τον εισβολέα. Για παράδειγμα, μπορεί να λάβει κάποιο e-mail το οποίο φαίνεται πως προέρχεται απο την τράπεζα του και να ζητά να επιβεβαιώσει τον αριθμό του τραπεζικού του λογαριασμού.

γ. Πιο συγκεκριμένα, ένας phisher χρησιμοποιεί προγράμματα spoofing διευθύνσεων emails, τα οποία του επιτρέπουν να εισάγει οποιαδήποτε στοιχεία επιθυμεί στα πεδία «Από» και «Απάντηση σε» των στοιχείων αποστολής ενός ηλεκτρονικού μυνήματος. Παράλληλα, στήνει μία ιστοσελίδα στο Διαδίκτυο που είναι εμφανισιακά πανομοιότυπη με τη σελίδα κάποιας άλλης εταιρείας (απομίμιση αυτής). Καθώς ο χρήστης-θύμα κλικάρει το λίνκ που είναι συννημένο σε ένα email πρεοερχόμενο απο κάποιον ‘’αξιόπιστο’’ προς αυτόν αποστολέα, θα έχει ως αποτέλεσμα να επισκεφθεί τον κατασκευασμένο πλαστό δικτυακό τόπο, όπου θα του ζητηθεί να συμπληρώσει στην ‘’ψεύτικη οθόνη’’ κάποια προσωπικά του στοιχεία όπως το username και το password προκειμένου να εισαχθεί στον λογαριασμό του. Η διαφορά τώρα είναι οτι η ψεύτικη αυτή οθόνη δεν θα εκτελέσει την αναμενόμενη απο τον χρήστη-θύμα λειτουργία πληκτρολογόντας το όνομα χρήστη και τον κωδικό πρόσβασης του πελάτη. Αλλά με αυτόν τον τρόπο αυτό, ο phisher δύναται να κατασκοπεύσει τον χρήστη εκμαιεύοντας όλες τις προσωπικές του πληροφορίες οι οποίες συνήθως χρησιμοποιούνται για την υποκλοπή της ταυτότητας του.

δ. Συνεπώς ένας phisher θα μπορούσε να χρησιμοποιήσει κάποιο site το οποίο φαινομενικά θα μοιάζει με μια δημοφιλή δικτυακή διεύθυνση έτσι ώστε να ξεγελάσει το υποψήφιο του θύμα. Για παράδειγμα η διεύθυνση https://wwwpaypal.com/ (όπου δεν υπάρχει η τελεία μετα τα ‘’www’’) είναι διαφορετική απο την ζητούμενη https://www.paypal.com/. Ομοίως η διεύθυνση https://www.paypal.com/ (όπου η λέξη paypal έχει ως τελευταίο γράμμα ένα

κεφαλαίο “i” αντί ενός μικρού ‘’L”) είναι διαφορετική απο την αυθεντική https://www.paypal.com/.

ε. Τρόποι ηλεκτρονικού ψαρέματος:

(1). Ψάρεμα κωδικών

ΕΙΚΟΝΑ 5. Ψάρεμα κωδικών

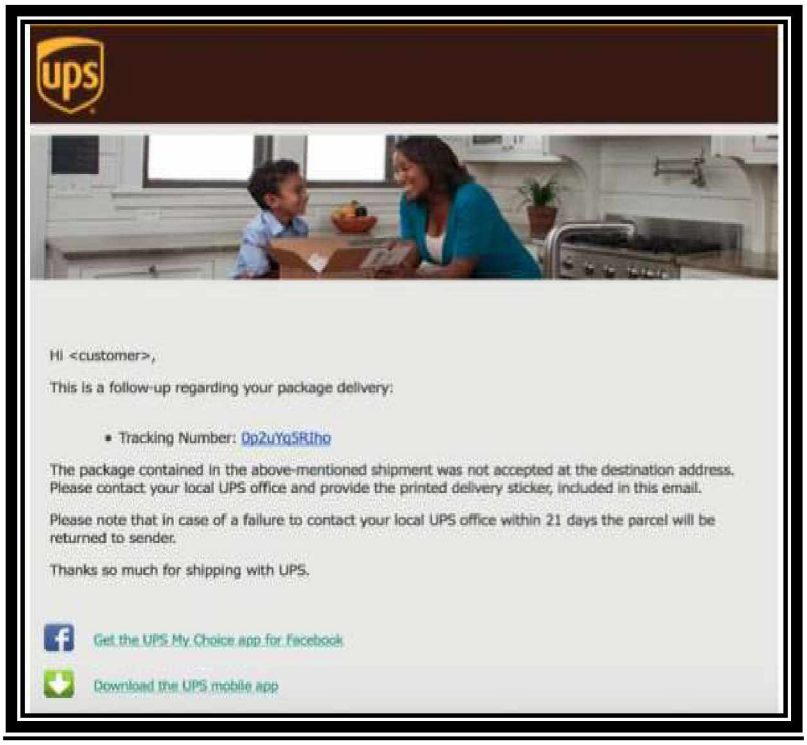
Σε αυτήν την περίπτωση ο phisher στέλνει ένα παραπλανητικό σύνδεσμο που φαινομενικά δείχνει ότι οδηγεί σε μια γνώριμη προς τον παραλήπτη ιστοσελίδα που μπορεί να ανήκει είτε σε χρηματοπιστωτική εταιρεία, είτε σε τράπεζα, είτε σε οποιοδήποτε άλλο οργανισμό, προτρέποντας τον να παραχωρήσει άμεσα τα προσωπικά του στοιχεία έτσι ώστε να μην κλειδωθεί ο λογαριασμός του λόγω πέρατος ημερομηνίας λήξης, είτε οτι χρήζει κάποιας ενημέρωσης, είτε οτι έχει παραβιαστεί απο κάποιον επιτήδειο και πρέπει να επιβεβαιωθεί. Σε όλες αυτές τις περιπτώσεις ο κοινωνικός μηχανικός στηρίζεται και «ποντάρει» στην εγγενή ψυχολογία του θύματος του για την άμεση λύση διαδικασιών, που στην περίπτωση τις αμελήσει, πιθανόν να τον οδηγήσουν σε περαιτέρω εμπλοκές με διαδικασίες και προβλήματα, οπότε τα θύματα λειτουργούν μηχανικά και αυθόρμητα για την αντιμετώπιση αυτών.

Είναι γεγονός οτι σε τέτοιες περιπτώσεις όπου λαμβάνουμε emails από γνώριμους οργανισμούς που μας προτρέπουν για άμεσσες ενέργειες, η προσοχή μας εστιάζεται περισσότερο στην απλή διαδικασία της συμπλήρωσης των αιτούντων στοιχείων, ελαχιστοποιόντας την ανησυχία μας για τυχόν απάτες. Παρακάτω παρατίθενται κάποια παραδείγματα λαμβανομένων emails από γνωστές εταιρείες όπως NETFLIX, UPS και PAYPAL τα οποία είναι ψεύτικα αλλά πλήρως αληθοφανή και προτρέπουν τους υποτιθέμενους πελάτες τους να πατήσουν κάποιο σύνδεσμο για την συμπλήρωση των προσωπικών στοιχείων και κωδικών τους.

(α). "Restart Your Membership"

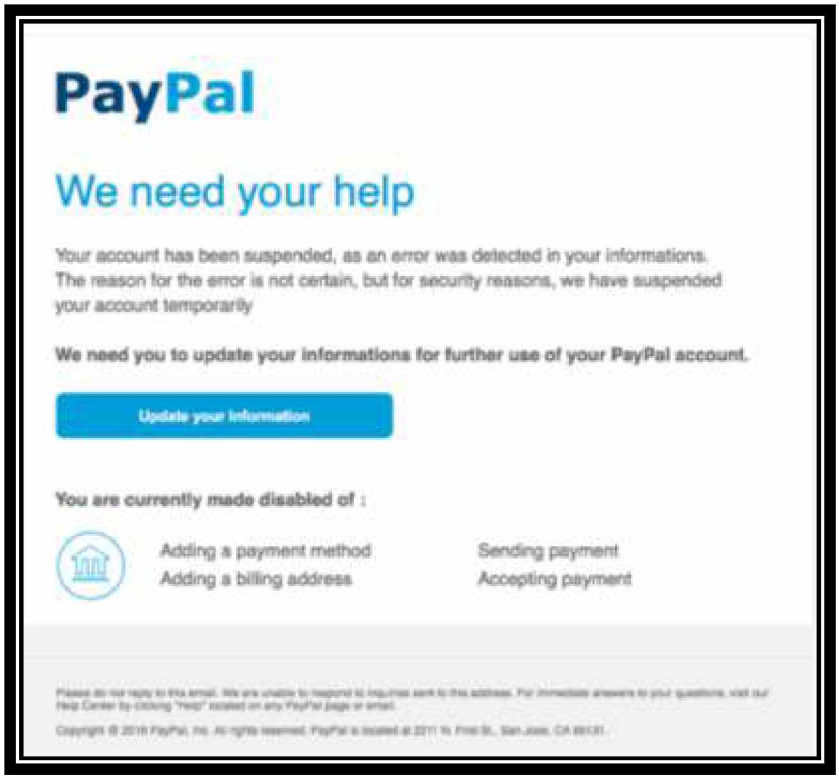
EIKONA 6. NETFLIX

(β). "You Missed a Delivery"



EIKONA 7. UPS

(γ). "Suspended Account"



ΕΙΚΟΝΑ 8. PayPal

(2). Spear Phishing

Ενώ το ηλεκτρονικό ψάρεμα στοχεύει σε ένα ευρύ φάσμα υποψηφίων θυμάτων, το Spear Phishing κατατάσσεται ως ένα υποσύνολο αυτού που στηρίζεται σε μια πιο στοχευμένη και εξειδικευμένη προσσέγγιση. Με τον όρο spear phishing αναφερόμαστε σε μια ηλεκτρονική επίθεση όπου ο στόχος είναι μια συγκεκριμένη ομάδα θυμάτων. Υπάρχει και ένας τύπος του spear phishing, γνωστός ως whaling όπου ο phisher στοχεύει ακόμα πιο πολύ στην λεπτομέρεια και αναζητά προσωποποιημένους στόχους, που κατέχουν καίριες και υψηλές στην ιεραρχεία θέσεις. Στην περίπτωση του Spear Phishing, ο phisher αποστέλλει emails που μοιάζουν αυθεντικά, μαζικά προς όλους τους υπαλλήλους μιας κρατικής υπηρεσίας, οργανισμού ή εταιρείας.

ΕΙΚΟΝΑ 6. Spear Phishing

Τα emails αυτά φαίνεται οτι προέρχονται απο κάποιον συνάδελφο ή απο τον εργοδότη, ο οποίος τα στέλνει προς όλους τους υπόλοιπους συναδέλφους, ζητώντας ονόματα χρηστών ή κωδικούς πρόσβασης με δήθεν σκοπό να αναβαθμίσει ή να ενημερώσει το σύστημα.

Σε μια άλλη περίπτωση ο phisher στέλνει χιλιάδες emails με ποκίλη θεματολογία όπως προσφορές και σημαντικά έγγραφα ή βίντεο σε διάφορες διευθύνσεις "ποντάροντας» οτι κάποιοι απο αυτούς είτε λόγω άγνοιας, είτε λόγω απορίας και περιέργειας, θα τα ανοίξουν και θα δελεασθούν να συνεχίσουν τις περαιτέρω διαδικασίες, γεγονός που ανοίγει την «πόρτα» στον phisher να αποσπάσει σημαντικές προσωπικές πληροφορίες.

Τέλος, υπάρχει και μια άλλη περίπτωση όπου ο phisher στοχοποιεί συγκεκριμένα άτομα απο τα οποία έχει ήδη αποσπάσει προσωπικές τους πληροφορίες (π.χ. φωτογραφίες και ονόματα συγγενικών προσώπων). Για παράδειγμα, φανταστείτε οτι έχετε λάβει ένα email με αποστολέα μια διεύθυνση που παραπέμπει σε όνομα ενός συγγενικού σας προσώπου με συννημένο κάποιο αρχείο με όνομα ''οικογενειακές φωτογραφίες'', λόγω του οτι γνωρίζετε αυτό το πρόσωπο και η διεύθυνση του αποστολέα σας φαίνεται φαινομενικά οικεία, και αφού υπάρχει το ενδεχόμενο να σας έχει στείλει κάποιες φωτογραφίες, δεν θα διστάσετε να το ανοίξετε. Ανοίγοντας όμως, το περιέχομενο του email και «κατεβάζοντας» το συννημένο αρχείο με τις φωτογραφίες, μαζί με το αρχείο αυτό θα κατεβάσετε και ένα κακόβουλο πρόγραμμα το οποίο θα παγιδέψει τον υπολογιστή σας και θα παραδώσει τον έλεγχο του υπολογιστή σας στον phisher, γεγονός που σημαίνει οτι ο phisher θα έχει πρόσβαση σε όλα τα αρχεία και προγράμματα σας.

1.6 Κακόβουλα Προγράμματα

1. Τα συνήθη κακόβουλα προγράμματα που χρησιμοποιεί ο phisher είναι τα εξής:

α. Σκουλίκι ή Worm

Το worm λειτουργεί με παρόμοιο τρόπο όπως και ένας μεταδοτικός ιός στον ανθρώπινο οργανισμό, αλλά είναι πιο εξελιγμένο όσον αφορά τον τρόπο μετάδοσης του. Το worm αυτοεγκαθίσταται στην μνήμη του υπολογιστή και έχει την δυνατότητα να αυτομεταφέρεται (χωρίς την ανθρώπινη παρέμβαση) σε άλλους υπολογιστές που συνδέονται στο ίδιο δίκτυο με τον μολυσμένο υπολογιστή, γεγονός που το κατατάσσει σέ έναν απο τους πιο επικίνδυνους ιούς. Αυτό που εκμεταλεύεται το worm είναι η αυτόματη αποστολή ή λήψη διαφόρων χαρακτηριτικών (features) τα οποία εγκαθίστανται σε υπολογιστές συνδεδεμένους σε δίκτυα. Ας δούμε πως λειτουργεί το worm:

Έστω κάποιος κάτοχος ηλεκτρονικής διεύθυνσης είναι καχύποπτος όταν πρόκειται να ανοίξει emails απο άγνωστες προς αυτόν διευθύνσεις οπότε το αποφεύγει και φυλάσσεται με αυτόν τον τρόπο απο κάποιο τυχόν κακόβουλο λογισμικό. Επιπλέον αποφεύγει να ανοίγει συννημένα αρχεία απο οποιαδήποτε άλλα εισερχόμενα emails απο τα οποία δεν περίμενε κάποια απάντηση, και επιπρόσθετα ελέγχει εξονυχιστικά μια σελίδα του browser για να βεβαιωθεί οτι περιηγείται σε ένα ασφαλή site, έτσι ώστε να εκτελέσει ασφαλείς και σίγουρες ηλεκτρονικές συναλλλαγές. Και ξαφνικά, μια μέρα λαμβάνει ένα email απο κάποιο οικείο πρόσωπο, το οποίο και φέρει ένα συννημμένο αρχείο. Ο χρήστης είναι σχεδόν βέβαιος οτι δεν πρόκειται για κάτι που φέρει κάποιον ιό ή κάποιο μολυσμένο πρόγραμμα λόγω του οτι το email

αυτό προέρχεται απο γνωστό πρόσωπο, και το πρόσωπο αυτό δεν θα επιθυμούσε να του κάνει κάποια «ζημιά».

Συνεπώς ο χρήστης ανοίγει χωρίς δισταγμό το συνημμένο αρχείο και ξαφνικά, χωρίς να το γνωρίζει "υιοθετεί" στο σύστημα του ένα σκουλίκι (worm. Γιατί όμως κάποιος γνωστός να το κάνει αυτό; Η εξήγηση βρίσκεται στην ανάλυση του τι είναι worm. Το worm είναι ένα μικρό κομμάτι λογισμικού ή αλλιώς ένα πρόγραμμα το οποίο χρησιμοποιεί το διαδίκτυο και τα κενά ασφαλείας των υπολογιστικών συστημάτων έτσι ώστε να αναπαράγει τον εαυτό του και να μολύνει όλους τους άλλους υπολογιστές που είναι συνδεμένοι στο δίκτυο αυτό. Ένα αντίγραφο του worm σκανάρει το διαδίκτυο για να εντοπίσει ένα άλλο μηχάνημα το οποίο έχει ένα συγκεκριμένο κενό ασφαλείας. Επιπρόσθετα, το worm που βρίσκεται σε κάποιου χρήστη τον υπολογιστή μπορεί να σταλεί μέσω email στην οποιαδήποτε διεύθυνση υπάρχει στο address book του χρήστη. Ως αποτέλεσμα, τα άτομα που αναγράφονται στο address book του χρήστη-θύματος θα λάβουν ένα email απο κάποιον τον οποίο γνωρίζουν και εμπιστεύονται, ενώ καθένα απο τα έμπιστα αυτά emails περιέχουν το worm το οποίο και συνεχίζει να ανατροφοδοτείται και να επανακυκλοφορεί προς τις εκάστοτες νέες διευθύνσεις των addresses books των νέων ανυποψίαστων θυμάτων-χρηστών.

β. Δούρειος Ίππος ή Trojan horse.

Το Trojan horse είναι γνωστό ως ο πιο ευρέως διαδεδομένος τύπος ιού στα υπολογιστικά συστήματα (κατα προσέγγιση 70%). Έχει πάρει την ονομασία του απο την ελληνική μυθολογία όπου οι Έλληνες κατασκεύασαν ένα τεράστιο ξύλινο άλογο που το ονόμασαν Δούρειο ίππο και το προσέφεραν ως δώρο στους Τρώες. Οι Τρώες δέχτηκαν με χαρά και ευγνωμοσύνη αυτό το πλούσιο και περίτεχνο δώρο των Ελλήνων και το οθέτηση εντός των τειχών της πόλεως τους. Μέσα στο άλογο αυτό όμως, του οποίου το εσωτερικό ήταν κουφάρι, είχαν κρυφτεί έλληνες στρατιώτες, συνεπώς με το έξυπνο αυτό κόλπο οι Έλληνες κατάφεραν να εξαπατήσουν τους Τρώες και να εισέλθουν μέσα στην Τροία. Με τον ίδιο τρόπο, ο ιός του Trojan horse κρύβεται μέσα σε κάποιο φαινομενικά "αθώο" πρόγραμμα και μόλις εγκατασταθεί στον υπολογιστή του θύματος θα μολύνει κάποια απο τα λειτουργικά αρχεία του συστήματος με αποτέλεσμα την παραχώρηση του ελέγχου του υπολογιστή στον εισβολέα.

Τα υποψήφια θύματα συνήθως παραπλανώνται απο κάποιες ελκυστικές διαφημίσεις που παρουσιάζονται στα κοινωνικά μέσα, όπου όταν ο χρήστης κλικάρει για να τα ανοίξει και να τα παρακολουθήσει, ο browser επανακατευθύνει σε μολυσμένες απο τους εν λόγω ιούς ιστοσελίδες, με συνέπεια την φόρτωση και εκτέλεση των Trojans στο σύστημα του και τελικά την παραχώρηση της πρόσβασης στα αρχεία και δεδομένα του συστήματος στον επιτήδειο.

Η προαναφερόμενη τύπου επίθεση μέσω διαφημίσεων ονομάζεται Clickbait attack και σχεδόν όλοι οι οι χρήστες Η/Υ την έχουν συναντήσει. Δεν είναι λίγες οι φορές που έχουμε παρακολουθήσει διαφημίσεις του τύπου: «Huge snake eats man alive, click to see the video!», ή άλλες με θέματα φυσικών καταστροφών, αυτοκτονιών ή και άλλων τραγωδιών. Όλες αυτές οι διαφημίσεις βασίζονται στην ανθρώπινη περιέργεια με σκοπό να οδηγήσουν τον χρήστη-θύμα να κλικάρει το λίνκ της διαφήμισης προκειμένου να δεί το συννημένο βίντεο και κατα συνέπεια να τον οδηγήσουν σε μολυσμένα websites τα οποία θα μεταδώσουν κάποιον ιό και εν συνεχεία την πρόσβαση στον υπολογιστή του.

Πιο αναλυτικά, ο ιός Trojan horse:

(1) Είναι ένα κακόβουλο πρόγραμμα το οποίο περιέχει επιβλαβή κωδικό και επιτρέπει σε μη εξουσιοδοτημένα άτομα να έχουν πρόσβαση στον μολυσμένο πλέον υπολογιστή του θύματος. Κάποια άλλα Trojans είναι σχεδιασμένα έτσι ώστε να κρύβονται μέσα στο λειτουργικό σύστημα του υπολογιστή και να κατασκοπεύουν οποιαδήποτε πληκτρολόγιση ή άλλη ενέργεια κάνει το θύμα μέσα απο τον υπολογιστή του, χωρίς αυτό να το αντιληφθεί.

ΕΙΚΟΝΑ 7. Trojan Horse-Worm

(2). Όλοι οι χρήστες υπολογιστών που κατέχουν μια ηλεκτρονική διεύθυνση ηλεκτρονικού ταχυδρομίου (email), κατά καιρούς έχουν δεχθεί κάποιο ανεπιθύμητο μύνημα, γνωστό και ως spam, το οποίο περιέχει διαφημιστικά μυνήματα ή κάποια προσφορά για κάποιο δωρεάν προϊόν όπως εκπτωτικά κουπόνια για την αγορά ηλεκτρικών και ηλεκτρονικών συσκευών ή ακόμα δωρεάν παροχές υπηρεσιών υγείας καθώς και δωρεάν αντιϊκά προγράμματα για τον υπολογιστή τους. Και προφανώς, οποιαδήποτε και εαν είναι η προσφορά, το email καθοδηγεί τον χρήστη να ανοίξει το περιεχόμενο ενός αρχείου ή να κλικάρει σε ένα λινκ που εμπεριέχεται σε αυτό με σκοπό την απόκτηση των αγαθών και υπηρεσιών που αυτό σας υπόσχεται. Όμως οι ενέργειες αυτές, που κατα συνέπεια είναι άνοιγμα ενός επισυναπτόμενου αρχείου από καποιον που πραγματικά δεν ξέρει ο χρήστης ποιος είναι, καθώς και άνοιγμα ενός λίνκ που κατευθύνει τον χρήστη σε κάποια σελίδα που ουδέποτε έχει ακούσει ή γνωρίζει για αυτήν, πιθανόν θα οδηγήσουν τον χρήστη σε σοβαρά προβλήματα.

(3). Στην κατηγορία των Trojans viruses ανήκει και ένα πρόγραμμα γνωστό ως RAT (Remote Access Trojan) το οποίο προσφέρει την δυνατότητα στον επιτιθέμενο να αποκτήσει την πλήρη πρόσβαση στον υπολογιστή του χρήστη μέσω της καταγραφής της πληκτρολόγισης, που συχνά αναφέρεται ως “keylogging’’ ή “keyboard capturing’’. Μόλις αυτό το πρόγραμμα εγκατασταθεί στον υπολογιστή, ο επιτιθέμενος έχει την δυνατότητα να λαμβάνει γνώση για την οποιαδήποτε πληκτρολόγιση πραγματοποιεί ο χρήστης-θύμα. Στην ίδια κατηγορία ανήκει και το κατασκοπευτικό λογισμικό (spyware), το

οποίο χρησιμοποιείται για να καταγράφει τις δραστηριότητες του χρήστη, όπως τα πλήκτρα που πληκτρολογούνται, το ηλεκτρονικό ταχυδρομείο, τις σελίδες που έχει επισκεφτεί, καθώς και τι απεικονίζει η οθόνη ανα πάσα στιγμή. Η χρήση των λογισμικών αυτών ξεκίνησε κυρίως για την παρακολούθηση και καταγραφή απο γονείς του τι έβλεπαν τα παιδιά τους στο ιντερνετ, καθώς και απο εργοδότες για να ελέγχουν τους υπαλλήλους τους εάν "χαζεύουν", σερφάροντας στο ίντερνετ. Αργότερα, το λογισμικό αυτό χρησιμοποιήθηκε για την ανίχνευση ενδεχομένων υποκλοπών εμπιστευτικών πληροφοριών και βιομηχανικής κατασκοπείας. Το λογισμικό αυτό έχει το πλεονέκτημα του να μην γίνεται αντιληπτό απο το antivirus γιατί αυτά τα προγράμματα δεν θεωρούνται κακόβουλα παρότι σκοπός τους είναι η παρακολούθηση άλλων χρηστών.

1.7 Τηλεφωνικός διάλογος μεταξύ social engineer και θύματος.

Στην δεύτερη κατηγορία της κοινωνικής μηχανικής που η απάτη επιτελείται βασιζόμενη στις κοινωνικές δεξιότητες του social engineer, ανήκουν οι απάτες με την χρήση τηλεφωνικού διαλόγου μεταξύ social engineer και θύματος.

ΕΙΚΟΝΑ 8. Τηλεφωνικός διάλογος

Ο Άλμπερτ Αινστάιν είχε πει το εξής γνωμικό: "Μόνο δύο πράγματα είναι άπειρα, το σύμπαν και η ανθρώπινη βλακεία, και ως προς το δεύτερο διατηρώ κάποιες αμφιβολίες''. Οι επιθέσεις της κοινωνικής μηχανικής, κατά κόρον επιτυγχάνουν βασιζόμενες πάνω στην μεταφορική ερμηνεία ''ανθρώπινη βλακεία'' η οποία και ερμηνεύεται ως οι ευπάθειες της ανθρώπινης φύσης όπως φόβος, άγνοια, περιέργεια, αφέλεια, απληστία και καλόπιστη εμπιστοσύνη.

Μία τεχνική της κοινωνικής μηχανικής η οποία συνδιάζει τις κοινωνικές δεξιότητες του social engineer και τις ευπάθειες της ανθρώπινης φύσης προκειμένου να χρησιμοποιηθεί για την παραβίαση ενός συστήματος ασφαλείας είναι ο τηλεφωνικός διάλογος με το υποψήφιο θύμα. Με χρήση ενός απλού τηλεφωνήματος ή μιας σειράς τηλεφωνημάτων ο social engineer με δόλιο τρόπο θα εξασφαλίσει τις απαραίτητες εκείνες πληροφορίες που θα του επιτρέψουν την πρόσβαση σε διαφόρων τύπων λογαριασμούς όπως τραπεζικούς ή εταιρικούς.

Στην περίπτωση αυτή, ο επιτήδειος εισβολέας ποντάρει στο στοιχείο του αιφνιδιασμού, καθώς το θύμα απροετοίμαστο για κάτι πονηρό και δόλιο και δείχνοντας καλοπροαίρετη διάθεση, όπως συνήθως κάνουν όλοι οι εργαζόμενοι προκειμένου να εξυπηρετήσουν κάποιον συνάδελφο ή πελάτη τους, πέφτουν στην παγίδα. Ο Kevin Mitnick ανέφερε οτι «...βασική αρχή στην Κοινωνική Μηχανική είναι η δημιουργία ψυχολογικής σύνδεσης με το άλλο άτομο στην άλλη πλευρά της τηλεφωνικής γραμμής με σκοπό την δημιουργία κλίματος εμπιστοσύνης.... κατάσταση την οποία αργότερα θα εκμεταλλευτεί... ».

Αφού πρώτα ο social engineer έχει κάνει την έρευνα του και έχει καταλήξει ποιά εταιρεία ή οργανισμό θα πλήξει, εν συνεχεία ψάχνει και μαθαίνει την τεχνική φρασεολογία και και το δομικό οργανόγραμμα της εταιρείας ή του οργανισμού αντίστοιχα. Επιπλέον, συγκεντρώνει στοιχεία για τα γραφεία απο τα οποία αποτελείται η εταιρεία/ οργανισμός και ποιο το έργο που επιτελεί έκαστο απο αυτά, καθώς και την διαβάθμιση των πληροφοριών που διαχειρίζονται. Όλα αυτά είναι χρήσιμα εργαλεία στα χέρια του εισβολέα έτσι ώστε να κατανοήσει πως «δουλεύει» η εταιρεία και με ποιόν τρόπο θα μπορέσει να δυεισδύσει σε αυτήν.

1.8 Εργαλεία για την επίτευξη των στόχων του social engineer

1. Οι social engineers χρησιμοποιούν διάφορες τακτικές για να αξιοποιήσουν την εξυπηρετικότατα, την εμπιστοσύνη, τη γνώση των εσωτερικών διαδικασιών, την εξουσία, την τεχνολογία καθώς και οποιοσδήποτε συνδυασμό αυτών. Συγκεκριμένα :

α. Εξασφάλιση εμπιστοσύνης. Η ένδειξη και η απόκτηση εμπιστοσύνης μεταξύ των ανθρώπων είναι μέρος της ανθρώπινης φύσης και βασική αρχή του αλτρουϊσμού και της συνεκτικότητας της κοινωνίας. Επιπλέον είναι ζωτικό κομμάτι της συναδελφικότητας και του επαγγελματισμού που επιδεικνύει το προσωπικό μια εταιρείας ή ενός οργανισμού. Προκειμένου ένας social engineer να αποκτήσει τις πληροφορίες που χρειάζεται, πρώτα απ΄όλα πρέπει να κερδίσει την εμπιστοσύνη απο το υποψήφιο θύμα του εκμεταλλευόμενος την ανθρώπινη ανάγκη της ικανοποίησης που νιώθει κάποιος όταν βοηθάει κάποιον έχει ανάγκη την ανάγκη του.

β. Αντίστροφη κοινωνική μηχανική. Ενας social engineer χρησιμοποιεί ως εργαλεία του, το σαμποτάζ, την διαφήμιση και την παροχή βοήθειας με σκοπό την δημιουργία μιας κατάστασης όπου το υποψήφιο θύμα θα χρειαστεί βοήθεια σε κάποια συγκεκριμένη στιγμή και όλως τυχαίως θα εμφανιστεί ο «απο μηχανής θεός – εισβολέας» που θα του προφέρει την χείρα βοηθείας. Αυτός είναι ένας πολύ καλός τρόπος για την ίδρυση της εμπιστοσύνης γιατί ένα άτομο το οποίο παίρνει βοήθεια από τον εισβολέα θα είναι πιο πρόθυμο να του ανταποδώσει αυτήν την καλή πράξη. Για παράδειγμα, αφού ο εισβολέας πρώτα έχει κάνει την έρευνα του για να εντοπίσει το άτομο εκείνο που θα μπορέσει να του παρέξει τις πληροφορίες εκείνες που χρειάζεται ώστε να πετύχει τον δόλιο σκοπό του, προσποιούμενος οτι είναι υπάλληλος του τεχνικού τμήματος της εταιρείας (τμήμα IT) τηλεφωνεί στο υποψήφιο υπάλληλο-θύμα προειδοποιώντας τον ότι υπάρχει πρόβλημα συνδεσιμότητας μεταξύ του υπολογιστή του και του δικτύου της εταιρείας, γεγονός το οποίο δεν αληθεύει. Εν συνεχεία ο εισβολέας θα του κάνει κάποιες ερωτήσεις και θα τον οδηγήσει να κάνει κάποιους τεχνικούς χειριστικούς

ελέγχους στο σύστημα του, και μετά απο κάποιες διασικασίες ελέγχου θα ζητήσει απο τον υπάλληλο να ελέγξει την συνδεσιμότητα του δικτύου, κατάσταση η οποία και προφανώς θα οδηγήσει σε ικανοποιητική λειτουργία της σύνδεσης εφόσον εξ'αρχής δεν υπήρχε πρόβλημα. Έχοντας ο εισβολέας-τεχνικός IT επιλύσει το φαινομενικό πρόβλημα της συνδεσιμότητας, ο υπάλληλος-θύμα αισθάνεται ευγνώμων και υπόχρεος ως προς αυτόν, έτσι δημιουργείται μια σχέση συνεργατικότητας και εμπιστοσύνης μεταξύ των δύο αυτών ατόμων. Η εμπιστοσύνη αυτή γίνεται εργαλείο στα χέρια του εισβολέα για την απόκτηση χρήσιμων πληροφοριών στο εγγύς μέλλον. Έτσι, ο social engineer, κάνοντας χρήση της εδραιωμένης πλέον εμπιστοσύνης θα ζητήσει απο τον υπάλληλο να ανοίξει ένα email το οποίο στάλθηκε απο αυτόν δεδομένου οτι περιέχει κάποιες πληροφορίες χρήσιμες για την ασφάλεια του υπολογιστή του, ενώ αυτό θα περιέχει κάποιο κακόβουλο λογισμικό ή έναν ιό, με τον οποίο ο εισβολέας θα αποκτήσει τον πλήρη έλεγχο του συστήματος αυτού.

γ. Εύκολα προσβάσιμη πληροφορία. Έχοντας οι social engineers ως βασικό εργαλείο τους την τηλεφωνική επικοινωνία, απαιτείται να έχουν πρόσβαση σε τηλεφωνικούς καταλόγους εταιρειών, τραπεζών ή οργανισμών, έτσι ώστε να οργανώσουν το σχέδιο τους και να ¨μεταφιεστούν¨ ως υπάλληλοι της εταιρείας/ τράπεζας/ οργανισμού αντίστοιχα. Οι αριθμοί των τηλεφώνων που χρειάζονται είναι μια εύκολα προσβάσιμη πληροφορία για αυτούς. Για παράδειγμα, σε μια εταιρεία πολλοί αριθμοί του τηλεφωνικού καταλόγου δεν φαίνονται στα μάτια των υπαλλήλων ως ευαίσθητα δεδομένα καθώς τους εκλαμβάνουν σαν εργαλείο για να κάνουν την δουλειά τους και οτι η ανταλλαγή τηλεφώνων, ονομάτων και τοποθεσιών είναι κάτι που βοηθάει και εξυπηρετεί τους συναδέλφους τους για την καλύτερη και εύρυθμη λειτουργία και αποδοτικότητα της εταιρείας. Και πάνω σε αυτήν την αντίληψη έρχεται ο social engineer για να ¨απλώσει¨ τα δίχτυα του. Ένα απλό τηλεφώνημα προς μια εταιρική ρεσεψιονίστ είναι το μόνο που χρειάζεται για να συλλέξει πληροφορίες (όνομα, τηλέφωνο) για κάποιον υπάλληλο που βρίσκεται σε μια συγκεκριμένη θέση ή να αποκτήσει πληροφορίες για ένα θέμα που το χρειάζεται. Τέλος ο social engineer μπορεί να περιηγηθεί στην εταιρική ιστοσελίδα, να συλλέξει πληροφορίες και τηλέφωνα, και μετά κάνοντας χρήση αυτών να συλλέξει τις επιπρόσθετες πληροφορίες που θα του χρειαστούν ώστε να προσεγγίσει τον στόχο του.

δ. Γνώση εσωτερικών διαδικασιών. Ένας social engineer αυξάνει τα ποσοστά επιτυχίας/ εκπλήρωσης του σκοπού του γνωρίζοντας τις διάφορες εσωτερικές λειτουργίες μιας εταιρείας/ τράπεζας/ οργανισμού. Προκειμένου ο social engineer να ¨μεταμφιεστεί¨ ως συνάδελφος του υποψήφιου θύματος του και να γίνει πειστικός ώστε να τον ξεγελάσει, απαιτείται να γνωρίζει την κατάλληλη χρήση ορολογίας της εταιρείας/ τράπεζας/ οργανισμού καθώς και την ¨αργκό¨ που χρησιμοποείται απο τους υπαλλήλους για τις διάφορες διαδικασίες.

Για παράδειγμα, γνωρίζοντας την διαδικασία που ακολουθεί ένα γραφείο υποστήριξης για την αναγνώριση της ταυτότητας ενός υπαλλήλου, ο social engineer θα συλλέξει πρώτα όλα εκείνα τα στοιχεία που γνωρίζει οτι θα του ζητηθούν για την επιβεβαίωση της ταυτότητας του υποτιθέμενου υπαλλήλου και έτσι ανταποκρίνοντας στις ερωτήσεις αντίστοιχα θα αυξήσει την πειστικότητα της κλήσης ώστε να πετύχει τον σκοπό του.

ε. Επιρροή. Η επιρροή ή αλλιώς η άσκηση εξουσίας πάνω σε κάποιον ή η χρήση χειριστικής συμπεριφοράς, είναι ένα απο τα σημαντικότερα όπλα και εργαλεία του social engineer που του επιτρέπει να προκαλέσει τον φόβο και την αναγκαστική συμπεριφορά στο υποψήφιο θύμα του. Για να το πετύχει αυτό "μεταμφιέζεται" σε μια δεσποτική φιγούρα, όπως αυτή του μάνατζερ είτε του προϊσταμένου ενός τμήματος, ή κάποιου άλλου υψηλόβαθμου συναδέλφου που χρειάζεται άμεσα πληροφορίες. Καθόσον έχει συγκεντρώσει και επεξεργαστεί πληροφορίες για τους υπευθύνους, ο social engineer μπορεί να παρουσιαστεί στον υποψήφιο στόχο του με τέτοιον δυναμικό τρόπο και αέρα υπεροχής, ο οποίος θα υποδηλώνει οτι δεν δέχεται το "οχι" ή το "δεν μπορώ" ως απάντηση στις απαιτήσεις του, έτσι ώστε να συλλέξει τις πληροφορίες που χρειάζεται για να εκπληρώσει τον σκοπό του. Εφόσον ο υποψήφιος στόχος πέσει στην παγίδα και αποκαλύψει εκείνες τις ευαίσθητες πληροφορίες που του ζητήθηκαν, τότε η εμπιστοσύνη μεταξύ του social engineer και του υπαλλήλου-θύματος γεφυρώνεται, εννοώντας πως μελλοντικά ο πρώτος μπορεί να χρησιμοποιήσει την ίδια μέθοδο κατά του ίδιο ατόμου και να ζητήσει επιπλέον πληροφορίες.

στ. Τεχνολογία. Ο social engineer χρησιμοποιώντας τις τεχνολογικές του γνώσεις σε συνδυασμό με τις κοινωνικές του δεξιότητες αυξάνει τα ποσοστά επιτυχίας σε μια επικείμενη επίθεση. Εφαρμόζοντας τις τεχνικές της κοινωνικής μηχανικής, ο social engineer δύναται να συλλέξει πληροφορίες για την αρχιτεκτονική υπολογιστών μιας εταιρείας, δηλαδή τι λογισμικό φέρουν τα υπολογιστικά συστήματα, τους κανόνες ασφαλείας όπως antiviruses, firewalls και proxy servers, έτσι ώστε να εξαπολύσει έναν ιό που θα μπορούσε να ρίξει κάτω ένα ολόκληρο δίκτυο.

1.9 Vishing

1. Το Vishing[6] είναι ένας όρος που χρησιμοποιείται στην πληροφορική για να περιγράψει την διαδικασία κατα την οποία ένας επιτήδειος εισβολέας διαπράτει ηλεκτρονικό ψάρεμα σε συνδιασμό με την τηλεφωνική κλήση - φωνή (voice + phishing = vishing). Η διαδικασία του vishing με χρήση VOIP μέσα απο αυτοματοποιημένη κλήση πραγματοποιείται σε τέσσερα (4) στάδια:

α. Κλήση των υποψηφίων θυμάτων. Ενας «war dialer», δηλαδή ένα πρόγραμμα το οποίο μπορεί να αναγνωρίσει τους τηλεφωνικούς αριθμούς εκείνους που συνδέονται με modems και τα καταχωρεί σε μια βάση δεδομένων, χρησιμοποιείται σε ένα αυτοματοποιημένο σύστημα για να γίνει κλήση σε μια λίστα τηλεφωνικών αριθμών, οι οποίοι έχουν κλαπεί απο κάποιο οικονομικό ή μη οργανισμό.

[6] https://www.rsa.com/content/dam/en/white-paper/phishing-vishing-smishing.pdf

ΦΩΤΟΓΡΑΦΙΑ 9. Vishing

β. Ηχογραφημένο Δόλωμα. Εφόσον κάποιος απο τους καλώντες απαντήσει, ένα αυτοματοποιημένο ηχογραφημένο μύνημα ειδοποιεί το υποψήφιο θύμα οτι κάποια ύποπτη ενέργεια πραγματοποιήθηκε στον τραπεζικό του λογαριασμό. Το μύνημα προτρέπει το θύμα να καλέσει άμεσα την 24ωρη εξυπηρέτηση της τράπεζας, παρέχοντας του έναν επετιδευμένα λάθος αριθμό που αντιστοιχεί στον αριθμό του visher.

γ. Συλλογή Πληροφοριών. Όταν το υποψήφιο θύμα καλέσει τον υποδυκνειόμενο απο το σύστημα αριθμό, αυτοματοποιημένες οδηγίες του ζητούν να εισάγει στο πληκτρολόγιο της συσκευής του την ημερομηνία γεννήσεως του, το ΑΦΜ, την ημερομηνία λήξεως της κάρτας, τον αριθμό της κάρτας και τέλος το CVV.

δ. Εκτέλεση Απάτης. Εχοντας όλες αυτές τις πληροφορίες στην διάθεση του, ο visher δύναται να διαπράξει απάτη με την χρήση των στοιχείων της κάρτας του θύματος.

2. Αναλυτικά, κατά την διαδικασία του vishing, ο εισβολέας (ή αλλιώς visher) εκμεταλλεύεται την άγνοια του θύματος σχετικά με μεθόδους ‘’caller ID spoofing’’ με χρήση αυτοματοποιημένων τηλεφωνικών κέντρων και την εμπιστοσύνη του προς τις ενσύρματες υπηρεσίες τηλεφωνίας, οι οποίες παραδοσιακά στην άλλη άκρη της γραμμής καταλήγουν σε μια υπαρκτή τοποθεσία ‘’γνωστή’’ στην τηλεφωνική εταιρεία στην οποία το θύμα είναι συνδρομητής αφού αντιστοιχεί σε κάποιον λογαριασμό, και η οποία μπορεί να είναι μια γνωστή και επώνυμη εταιρεία, μια τράπεζα ή οποισδήποτε άλλος οργανισμός, αξιόπιστος προς το θύμα. Το θύμα συνεπώς, εύκολα και χωρίς προβληματισμό θα πεισθεί για την αξιοπιστία του καλούντος αριθμού αφού μπορεί να τον διασταυρώσει με την υπάρχουσα τοποθεσία του μέσω ενός τηλεφωνικού καταλόγου, μέσω ίντερνετ ή μέσω ενός άλλου επίσημου εγγράφου.

3. Το υποψήφιο θύμα λαμβάνει μία τηλεφωνική κλήση είτε στο σταθερό είτε στο κινητό του τηλέφωνο. Απαντώντας στην κλήση αυτή, λαμβάνει ένα ηχογραφημένο μύνημα προερχόμενο απο υπολογιστή το οποίο προσομοιάζει την ανθρώπινη φωνή, γνωστό ως “speech synthesis”

ενημερώνοντας το θύμα ότι ύποπτες δραστηριότητες λαμβάνουν χώρα στον λογαριασμό της πιστωτικής του κάρτας, είτε στον λογαριασμό του δανείου, είτε και σε οποιοδήποτε άλλη χρηματοληπτική υπηρεσία εμπλέκεται με το όνομα του. Εν συνεχεία, το θύμα συμβουλεύεται να καλέσει έναν συγκεκριμένο τηλεφωνικό αριθμό και να παρέξει κάποιες προσωπικές πληροφορίες έτσι ώστε να επιβεβαιώσει την γνησιότητα της ταυτότητας του και να επιβεβαιώσει οτι ο ίδιος δεν ενεπλάκει σε οποιαδήποτε κίνηση του λογαριασμού του. Με τις σύγχρονες τηλεφωνικές υπηρεσίες VOIP (Voice Over Internet Protocol) ή αλλιώς ‘’τηλεφωνία μέσω διαδικτύου’’, ο αριθμός αυτός μέσω μιας διαδικασίας η οποία ονομάζεται caller ID spoofing μπορεί να φαίνεται οτι αντιστοιχεί σε μια νόμιμη-αυθεντική πηγή, όπως π.χ μία τράπεζα ή ένα κυβερνητικό οργανισμό, όμως το θύμα θα καλέσει τον αριθμό τηλεφώνου του εισβολέα. Απο εκεί και πέρα ο social engineer θα εκμαιεύσει απο το θύμα όλες εκείνες τις πληροφορίες με τις οποίες θα πραγματοποήσει τον παράνομο σκοπό του.

1.10 Κοινωνική Μηχανική και Μέσα Κοινωνικής Δικτύωσης

1. Δεδομένου οτι στην σημερινή εποχή τα μέσα κοινωνικής δικτύωσης βρίσκονται σε πολύ υψηλή δημοτικότητα και καθορίζουν πλέον τις κοινωνικές και επαγγελματικές σχέσεις των ανθρώπων, πολλοί χρήστες δημοσιεύουν τις ενέργειες τους, τις συνήθειες τους και εν γένει τον τρόπο ζωής τους. Έτσι υπερεκθέτουν τα προσωπικά τους στοιχεία προς κοινή και κατά τρόπο μη ελεγχόμενη αξιοποίηση τους, γνωστός όρος στα αγγλικά ως ‘’oversharing’’. Συλλέγοντας όλες αυτές τις πληροφορίες που είναι διαθέσιμες απλόχερα μέσα απο τις πλατφόρμες κοινωνικής δικτύωσης, ένας social engineer δύναται να δημιουργήσει ένα προφίλ του χρήστη-θύματος και να αναπτύξει τρόπους και μεθόδους με τους οποίους θα μπορέσει να προσεγγίσει το θύμα του, και κερδίζοντας την εμπιστοσύνη του, να του υποκλέψει ευαίσθητα προσωπικά δεδομένα. Συγκεκριμένα, ένας υποψήφιος εισβολέας θα μπορούσε μέσω του facebook, του my space του twitter και του instagram να συγεντρώσει στοιχεία της ταυτότητας του υποψήφιου θύματος, όπως όνομα και επίθετο, ηλικία, τόπο διαμονής, την διεύθυνση του ηλεκτρονικού ταχυδρομίου, καθώς και τις συνήθειες του.

ΦΩΤΟΓΡΑΦΙΑ 10. Μέσα κοινωνικής Δικτύωσης

2. Επιπλέον ο εισβολέας θα συγκεντρώσει πληροφορίες για το τι μας αρέσει και τι όχι στο χρήστη, ακόμα μπορεί να μάθει για μέρη και τοποθεσίες που έχει επισκεφτεί, την δουλειά του καθώς και τις προηγουμενες εργασίες του. Επιπλέον ο εισβολέας μπορεί να συλλέξει πληροφορίες για τις σχέσεις του, προσωπικές και φιλικές, καθώς και πληροφορίες για τους συγγενείς και τους συναδέλφους του. Τέλος ο social engineer θα ενημερωθεί για τα hobbies και τις προτιμήσεις του θύματος ως προς τις τάσεις της μόδας και τον αθλητισμό, καθώς και για τα πολιτικά και θρησκευτικά του πιστεύω.

3. Μια άλλη πλατφόρμα κοινωνικής δικτύωσης με αυξανόμενο ρυθμό χρήσης είναι το LinkedIn, το οποίο είναι ένα δίκτυο αποκλειστικά σχεδιασμένο για επαγγελματίες. Σε αυτήν την πλατφόρμα πολλοί χρήστες δημοσιεύουν ολόκληρο το βιογραφικό τους και το "μοιράζονται" πολλές φορές και με ανθρώπους τους οποίους δεν γνωρίζουν.

4. Έχοντας όλες αυτές τις πληροφορίες στην διάθεση του προς εκμετάλλευση, ο εισβολέας μπορεί να προσωποποιήσει την επίθεση του μέσω κοινωνικής μηχανικής και των spam ηλεκτρονικών μυνημάτων. Έτσι, τα malware-laced emails δεν θα φαίνονται επικίνδυνα λόγω του θα προέρχονται απο κάποιο φιλικό πρόσωπο ή συνεργάτη του θύματος ή θα αναφέρονται σε μέρη και τοποθεσίες τα οποία είναι οικεία σε αυτόν. Επιπρόσθετα, ο εισβολέας υποκλέπτοντας κάποιο password ή username κάποιου λογαριασμού κάνοντας χρήση της τεχνικής ''spear phishing'' και έχοντας στην κατοχή του την διεύθυνση του ηλεκτρονικού ταχυδρομίου του χρήστη-θύματος, ο εισβολέας δύναται να δοκιμάσει τα υποκλεμένα ήδη password και user name σε τραπεζικούς λογαριασμούς του χρήστη, γνωρίζοντας οτι πολλοί χρήστες υπολογιστών που έχουν ανοίξει πολλούς ηλεκτρονικούς λογαριασμούς, συνήθως χρησιμοποιούν τα ίδιους κωδικούς προς χάρην ευκολίας και ταχύτητας. Ακόμα, ο εισβολέας χρησιμοποιόντας τις πληροφορίες που αναλύσαμε παραπάνω μπορεί να "μαντέψει" κάποιον κωδικό ή να απαντήσει σε ερωτήσεις ασφαλείας κάποιων sites (π.χ όνομα σκύλου, μάρκα αυτοκινήτου, πατρόνυμο μητέρας κτλπ).

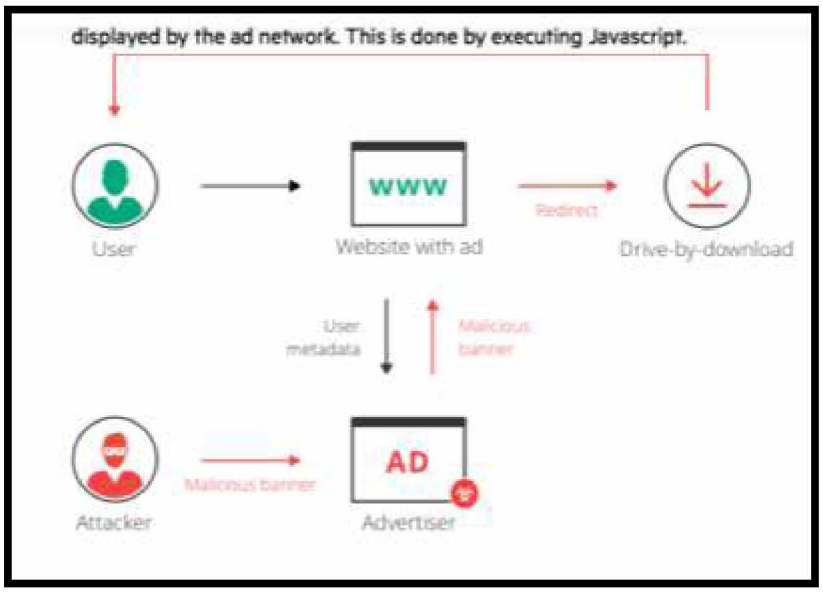
1.11 Malvertising

Ένας άλλος τρόπος που χρησιμοποιεί ο social engineer για να εκτοξεύσει τις επιθέσεις του στους διαδικτυακούς χρήστες είναι το "malvertising". Σε αυτήν την περίπτωση, ο επιτιθέμενος εκμεταλλεύεται την περιπλοκότητα του διαδικτυακού διαφημιστικού μηχανισμού, ο οποίος περιλαμβάνει την ιστοσελίδα του εκδότη, τον μηχανισμό προβολής διαφημίσεων και τον μηχανισμό ανακατέθυνσης των διαφημίσεων μεταξύ servers διαφημιστών, πελατών και εκδότη, με συνέπεια να τροποποεί την κατεύθυνση της διαφήμισης αφότου πρώτα την έχει υποβάλλει στο διαφημιστικό δίκτυο ή να τοποθετεί επιβλαβή κώδικα σε σημεία που είναι αρκετά δύσκολο να εντοπιστούν.

Οι επιτιθέμενοι ανεβάζουν αυτούς τους μολυσμένους κώδικες σε ιστοσελίδες που προωθούν διαφημίσεις στο διαδίκτυο, πληρώνοντας τους παρόχους για τις διαφημίσεις αυτές σαν να είναι αληθινοί πελάτες που προωθούν τα εμπορεύματα τους. Έτσι για παράδειγμα κάποιος μπορεί να επισκεφθεί έναν ιστότοπο μιας γνωστής και αξιόπιστης εφημερίδας και να εμφανιστεί μια διαφήμιση ως «banner ad» η οποία και θα του κινήσει το

ενδιαφέρον και χωρίς δισταγμό θα κλικάρει για να την δεί, ενώ σε άλλη περίπτωση θα την παρέκαμπτε λόγω της χρήσης των firewalls. Κατ'επέκταση, κλικάροντας πάνω στην διαφήμιση, ο επισκέπτης κατευθύνει ή ανακατευθύνει τον browser του σε κάποιο ιστότοπο που φαίνεται αληθινός αλλά είναι αντίγραφο του πραγματικού και περιέχει κακόβουλο ή κατασκοπευτικό κώδικα.

Το πλεονέκτημα της επίθεσης αυτής είναι οτι ο επιτιθέμενος μπορεί να μεταδώσει το κακόβουλο κώδικα σε ορισμένη - συγκεκριμένη χρονική περίοδο και σε χρήστες με συγκεκριμένα χαρακτηριστικά και μετά να τον αποσύρει, γεγονός που του επιτρέπει να μην είναι ανιχνεύσιμος μετά το χτύπημα του. Αυτός ο τρόπος επίθεσης έχει επιτρέψει στους κοινωνικούς μηχανικούς να στοχοποιήσουν επισκέπτες επώνυμων και αξιόπιστων ιστοσελίδων, όπως για παράδειγμα The New York Times Online, The London Stock Exchange και Spotify, οι οποίες και είχαν εκτεθεί στο malvertising.



ΦΩΤΟΓΡΑΦΙΑ 11. Malvertising

Η μια προσσέγγιση είναι μέσω μιας διαφημιστικής εικόνας - λεζάντας, όπου ο χρήστης κλικάρει πάνω σε αυτήν ώστε να επισκεφθεί στον ιστότοπο της διαφήμισης, δηλαδή να παρακολουθήσει ολόκληρη την διαφήμιση, οπότε και ο ιστότοπος αυτός περιέχει κάποιον επιβλαβή κώδικα ή τον ανακατευθύνει σε κάποιο άλλο μολυσμένο site.

Πολλές φορές όμως μια κακούβουλη διαφήμιση μπορεί να έχει την μορφή ενός Flash προγράμματος. Το πρόγραμμα αυτό έχει την ιδιότητα να τρέχει τον επιβλαβή κώδικα στου χρήστη τον browser αυτόματα χωρίς την παρέμβαση του χρήστη (δεν απαιτείται κλικάρισμα πάνω στην διαφήμιση). Το Flash πρόγραμμα έχει ενσωματωμένη μια λειτουργία με την οποία ο επιτιθέμενος μπορεί να καθορίσει την ημερομηνία και χρόνο προσβολής απο το κακόβουλο λογισμικό στον υπολογιστή του θύματος. Αυτό γίνεται για να καθυστερήσει η επίθεση εως ότου το διαφημιστικό δίκτυο εξετάσει και εγκρίνει την διαφήμιση.

Κεφάλαιο 2
Αντιμετώπιση Κοινωνικής Μηχανικής

ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΚΑΤΑ ΤΗΣ ΚΟΙΝΩΝΙΚΗΣ ΜΗΧΑΝΙΚΗΣ – ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

ΕΙΚΟΝΑ 12. Τρόποι Αντιμετώπισης Κοινωνικής Μηχανικής

2.1 Εισαγωγή

1. Η κοινωνική μηχανική αποτελεί πλέον έναν απο τους μεγαλύτερους κινδύνους όσον αφορά την ασφάλεια πληροφοριών. Στην σύγχρονη εποχή, τα επεισόδια της κοινωνικής μηχανικής αυξάνονται συνεχώς με γεωμετρική πρόοδο καθόσον όλο και νέοι και πιο εξελιγμένοι τρόποι ανακαλύπτονται προσπαθώντας να ξεγελάσουν και να παγιδεύσουν τους ανυποψίαστους χρήστες, με σκοπό να τους αποσπάσουν εκείνες τις πληροφορίες οι οποίες θα χρησιμοποιηθούν κατάλληλα απο τους social engineers για να επιτύχουν την απάτη τους. Συνεπώς, και η ασφάλεια ενάντια στην κοινωνική μηχανική πρέπει να εξελίσσεται συνεχώς έτσι ώστε να περιορίσει όσο το δυνατόν περισσότερο τα επεισόδια επιθέσεων. Σε αυτό το κεφάλαιο θα αναλυθούν οι τρόποι προστασίας και οι διάφορες πολιτικές και διαδικασίες που πρέπει να ακολουθούνται από τους υπαλλήλους μιας εταιρείας/ οργανισμού /τράπεζας για να απομειώσουν τον κίνδυνο της δημιουργίας απάτης μέσω των τεχνικών της κοινωνικής μηχανικής.

2.2 Ανθρώπινος Παράγοντας

1. Καθόσον οι τεχνικές της κοινωνικής μηχανικής βασίζονται στις ευπάθειες της ανθρώπινης φύσης, ο ανθρώπινος παράγοντας είναι εκείνος που θα παίξει τον σημαντικότερο ρόλο στην προστασία και τον έλεγχο τη πληροφορίας. Η προστασία μιας εταιρείας/ οργανισμού/ τράπεζας από τους κινδύνους που η κοινωνική μηχανική επιφυλάσσει, ξεκινά από την επιμόρφωση του προσωπικού σχετικά με την πραγματική αξία τη πληροφορίας, την ενημέρωσή του για τις τεχνικές παραπλάνησης που μπορεί να χρησιμοποιηθούν και την ταυτόχρονη εκπαίδευσή του σε μεθόδους προστασίας για διαφύλαξη του απορρήτου των πληροφοριών. Για παράδειγμα, θα ήταν πιο εύκολο για κάποιον υπάλληλο που δεν γνωρίζει την αξία της πληροφορίας να δώσει σε κάποιον συνάδελφο του, τον κωδικό (password) του υπολογιστή του, απο το να έδινε το κλειδί ενός χρηματοκιβωτίου σε κάποιον μηχανικό ασφαλείας

για τυχόν επισκευή της κλειδαριάς, ενώ στην προκειμένη περίπτωση το χρηματοκιβώτιο μπορεί να περιέχει ένα χρηματικό ποσό του οποίου η αξία είναι αμελητέα σε σύγκριση με την αξία της πληροφορίας.

ΕΙΚΟΝΑ 13. Ανθρώπινος Παράγοντας

2. Η θέσπιση πολιτικών χρήσης και αυθεντικότητας καθώς και η εκπαίδευση και ενημέρωση των εργαζομένων για τους κινδύνους που απορρέουν απο απάτες κοινωνικής μηχανικής είναι το πρώτο και σημαντικότερο βήμα για την προστασία μιας επιχείρησης/ οργανισμού/ εταιρείας. Συνήθως, τα άτομα που γίνονται θύματα μιας απάτης απο κάποιον που προσποιείται τον διευθυντή ή τον τεχνικό συμβουλο (IT) της εταιρείας στην οποία εργάζονται, είναι εκείνα τα οποία δεν έχουν ακούσει ποτέ και τίποτα για παρόμοιες απάτες. Ο εκπαιδευμένος και ενημερωμένος χρήστης είναι, κατα ένα μεγάλο ποσοστό, και προστατευμένος. Η ενημέρωση για την ασφάλεια και η συνειδητοποίηση των κινδύνων απο την χρήση υπολογιστικών συστημάτων και διαδικτύου πρέπει να είναι βασικό κομμάτι της εκπαίδευσης και επιμόρφωσης του κάθε χρήστη, και για να είναι αποτελεσματική πρέπει να είναι συνεχής και σύγχρονη με τα νέα δεδομένα. Εφίσταται η επαγρύπνιση προσωπικού σχετικά με θέματα ασφαλείας. Για παράδειγμα, όποτε ζητούνται μέσω τηλεφωνικής κλήσης στοιχεία όπως εσωτερικοί τηλεφωνικοί αριθμοί ή προσωπικά στοιχεία υπαλλήλων, το προσωπικό πρέπει πρώτα να ζητάει τα στοιχεία του καλούντος και μετά απο διασταύρωση για την αυθεντικότητα του προσώπου αυτού απο τα αρχεία της εταιρείας, τον καλεί πίσω.

3. Η εκπαίδευση του προσωπικού μιας εταιρείας/ τράπεζας/ οργανισμού θα μπορούσε να επικεντρωθεί σε τέσσερις βασικούς κανόνες:

α. Κανόνας 1. Αποφυγή απόκρισης σε αυτόκλητα/ αυθαίρετα emails ή τηλεφωνικές κλήσεις χωρίς πρώτα να ταυτοποήσουμε το άτομα στην άλλη πλευρά της γραμμής (π.χ. καλώντας τον τηλεφωνικώς πρώτα).

β. Κανόνας 2. Αποφυγή ανοίγματος ενός συννημένου αρχείου απο μη αξιόπιστες πηγές. Χρήση μη εταιρικού/ υπηρεσιακού Η/Υ για πρόσβαση και σερφάρισμα σε οποιοδήποτε site ή έγγραφο, ο οποίος υπολογιστής δεν θα περιέχει ευαίσθητες πληροφορίες.

γ. Κανόνας 3. Αλλαγή κωδικού τακτικά (κάθε δύο (2) μήνες) και σποραδικά (χωρίς συγκεκριμένο πλάνο και προβλεψιμότητα), έτσι ώστε ένας επιτήδειος social engineer να μήν μπορεί να δημιουργήσει εύκολα σχέδιο επίθεσης.

δ. Κανόνας 4. Επιμόρφωση προσωπικού περί συνεπειών από την άγνοια των απειλών κοινωνικής μηχανικής, αναλύοντας πραγματικές καταστάσεις και παραδείγματα μέσω εργασιακής εμπειρίας (lessons learned).

2.3 Άμυνα σε επιθέσεις κοινωνικής μηχανικής

1. Μια καλή άμυνα ενάντια σε μια επίθεση κοινωνικής μηχανικής θα πρέπει να περιλαμβάνει:

α. Πολιτικές κωδικών πρόσβασης και πρότυπα. Για μια εταιρεία/ οργανισμό/ τράπεζα μια δομημένη πολιτική κωδικών πρόσβασης, που θα εξασφάλιζε την αποτροπή μιας επίθεσης κοινωνικής μηχανικής θα πρέπει να περιλαμβάνει πληροφορίες σχετικές με:

(1). Την απόκρυψη των κωδικών πρόσβασης του εκάστοτε χρήστη από τους συναδέλφους τους.

(2). Την μη χρησιμοποίηση των defaults απο το σύστημα κωδικών πρόσβασης.

(3). Τον καθορισμό μεθόδων για την εμπιστευτική παράδοση των κωδικών προς τους χρήστες (προσωπική απόδειξη παραλαβής).

(4). Την περιοδική αλλαγή του κωδικού πρόσβασης (π.χ ανα δύο (2) μήνες).

(5). Την ύπαρξη χρονικής περίοδου λήξεως των κωδικών πρόσβασης.

(6). Το Κλείδωμα του λογαριασμού μετά από τρεις (3) αποτυχημένες προσπάθειες εισόδου (login).

(7). Την δημιουργία ισχυρών κωδικών με χρήση αλγορίθμου και ταυτόχρονη χρήση αλφαριθμητικών και αριθμών.

(8). Την αποφυγή καταχώρησης κωδικών εντός αρχείων σε υπολογιστές που συνδέονται στο διαδίκτυο.

(9). Την αποφυγή χρήσης των ίδιων κωδικών σε διαφορετικά προγράμματα και λογαριασμούς έτσι ώστε ένας επιτιθέμενος να δυσκολευτεί περισσότερο να υποκλέψει τους κωδικούς.

(10). Την αποφυγή καταγραφής κωδικών σε post-it και επικόληση τους δίπλα στην οθόνη ή στο πληκτρολόγιο για εύκολη πρόσβαση (κάτι που πολλές φορές συνηθίζεται απο τους υπαλλήλους).

ΕΙΚΟΝΑ 14. Άμυνα σε επιθέσεις κοινωνικής μηχανικής

β. Δοκιμές διείσδυσης (Penetration tests). Οι οργανισμοί/ τράπεζες/ εταιρείες θα πρέπει τακτικά να εκτελούν δυεισδυτικές αξιολογήσεις, τα γνωστά penetration tests, είτε απο εσωτερικούς είτε απο εξωτερικούς παράγοντες με την χρήση κατάλληλων εργαλείων και τεχνικών ethical hacking για να δοκιμάσουν την ασφάλεια ενός δικτύου και του υπολογιστικού συστήματος. Αυτές οι δοκιμές πρέπει να περιέχουν τεχνικές κοινωνικής μηχανικής όπως χρήση spam emails και κακόβουλων λογισμικών για την παροχή μιας ακριβής αξιολόγησης. Επιπρόσθετα, τα tests αυτά είναι απαραίτητο να εκτελούνται κατ' ελάχιστον μια φορά τον χρόνο και να προσαρμόζονται στην συχνότητα τους αναλόγως του μεγέθους και του ιστορικό του οργανισμού/ εταιρείας/ τράπεζας.

γ. Ταξινόμιση δεδομένων. Επειδή οι social engineers στηρίζουν τις τεχνικές τους πάνω στην εκμαίευση πληροφοριών/ στοιχείων απο τους υπάλληλους της εταιρείας/ οργανισμού/ τράπεζας την οποία θέλουν να παγιδεύσουν για να πετύχουν τον σκοπό τους, κρίνεται απαραίτητη η ύπαρξη ενός μοντέλου ταξινόμησης δεδομένων όπου οι εργαζόμενοι θα βλέπουν και θα τηρούν. Κάθε είδος ταξινόμησης θα πρέπει να έχει διαφορετικά επίπεδα ευαισθησίας ως προς την ιεραρχία/ δομή της εταιρείας/ τράπεζας/ οργανισμού. Η ταξινόμιση δεδομένων προστατεύει τροποτινά την πληροφορία απο τους υπαλλήλους οι οποίοι δεν απαιτείται να την γνωρίζουν, προκειμένου να επιτελέσουν την εργασία τους. Επιπρόσθετα, εξασφαλίζεται η ακεραιότητα των δεδομένων ανάλογα την ταξινόμηση τους, καθώς και θα πρέπει να υπάρχει ένας υπεύθυνος για την ενημέρωση των αρχείων αναλόγως της ταξινόμισης. Τα αρχεία αυτά ταξινομούνται στις κάτωθι διαβαθμίσεις:

(1). Απόρρητα: Ιδιαίτερα ευαίσθητα έγγραφα εσωτερικής χρήσης. Η άκρως απόρρητη πληροφορία θα πρέπει να προστατεύεται πίσω από κάποιο τοίχος προστασίας (firewall) όπου μόνο συγκεκριμένα άτομα ειδικής διαβάθμισης/ θέσης (πχ Διευθυντής) θα έχουν πρόσβαση στους διακομηστές (hosts) όπου περιέχουν τα ανωτέρω δεδομένα και πληροφορίες

(2). Εμπιστευτικά: Έγγραφα τα οποία εάν κοινοποιηθούν έστω και εντός της επιχείρησης θα μπορούσαν να βλάψουν σημαντικά της διάφορες ενέργειες που βρίσκονται σε εξέλιξη.

(3). Έγγραφα για εσωτερική χρήση: Πληροφορίες που δεν έχουν εγκριθεί για την γενική κυκλοφορία τους εκτός της εταιρείας/ οργανισμού/ τράπεζας.

(4). Δημόσια έγγραφα: Πληροφορίες δημόσιου τομέα, τα οποία δύναται να κοινοποιούνται και στο site της εταιρείας/ οργανισμού/ τράπεζας.

δ. Αποδεκτή χρήση πολιτικής. Μια αποδέκτη χρήση πολιτικής περιλαμβάνει τα κάτωθι:

(1). Διάθεση συστημάτων πληροφοριών και δικτύου μόνο σε εξουσιοδοτημένο προσωπικό.

(2). Απαγόρευση παροχής ή χρήσης κωδικών απο μη εξουσιοδοτημένο προσωπικό.

(3). Απαγόρευση κοινοποίησης πληροφοριών διαβάθμισης εμπιστευτικών και άνω σε τρίτους.

(4). Απαγόρευση χρήσης εταιρικών λογαριασμών ηλεκτρονικού ταχυδρομίου για προσωπικούς λόγους.

(5). Απαγόρευση κατάχρησης της εταιρικής σύνδεσης στο διαδίκτυο για προσωπικούς λόγους.

(6). Απαγόρευση εγκατάστασης ή και χρήσης μη εξουσιοδοτημένων ή παράνομων λογισμικών.

(7). Αυστηρές ρήτρες για την αποφυγή χρήσης του εταιρικού διαδικτύου για παράβαση νομοθετικών ή συνταγματικών διατάξεων.

ε. Διαδικασία τερματισμού. Μια αποτελεσματική διαδικασία τερματισμού κρίνεται αναγκαία για την αποτροπή των υπαλλήλων, που έχουν απολυθεί από την εταιρεία να κάνουν χρήση της πρόσβασης που είχαν σε διαβαθμισμένες πληροφορίες και να προκαλέσουν κάποια βλάβη. Συνεπώς, κάθε φορά που ένας υπάλληλος σταματήσει να εργάζεται λόγω απόλυσης του, μια άμεση διαδικασία τερματισμού πρόσβασης πρέπει να λαμβάνει χώρα περιλαμβάνοντας την αφαίρεση της πρόσβασης στο εταιρικό δίκτυο, καθώς και της πρόσβασης στις εταιρικές εφαρμογές. Είναι σημαντικό, η διαδικασία του τερματισμού να ξεκινάει απο την στιγμή της ανακοίνωσης της απόλυσης του εργαζομένου και να τελειώνει προ της απομάκρυνσης του απο την εταιρεία. Επιπρόσθετα, όταν ένας υπάλληλος παίρνει μια μακράς διαρκείας άδεια, όπως για παράδειγμα σπουδαστική ή άδεια ανατροφής τέκνου θα πρέπει να υπάρχει μια διαδικασία προσωρινού τερματισμού.

2.4 Αντιμετώπιση επεισοδίου κοινωνικής μηχανικής

Στην περίπτωση που μια επίθεση λαμβάνει χώρα ή έλαβε χώρα απαιτείται άμεσα περιορισμός της επίθεσης και συλλογή όσο το δυνατόν περισσότερων και σαφέστερων πληροφοριών σχετικά αυτήν. Μια επίθεση μικρής έκτασης και σημαντικότητας ίσως να είναι η έναρξη ή η προετοιμασία για

μια επακόλουθη σειρά επιθέσεων. Η τακτική των social engineers, ούτως ή άλλος είναι η κλιμάκωση των επιθέσεων μέχρι να φτάσουν στον επιθυμητό τους στόχο. Η αναγνώριση και αντιμετώπιση μιας επίθεσης είναι ένας αποτελεσματικός τρόπος για την αποτροπή μελλοντικών επιθέσεων και αναχαίτησης της εφαρμογής σχεδίου του επιτιθέμενου. Συνεπώς για να αντιμετωπιστούν αυτές οι επιθέσεις, πρωτού συμβούν, απαιτείται ένα προσχέδιο προσαρμοσμένο στις ιδιαιτερότητες του κάθε συστήματος, το οποίο θα περιλαμβάνει τις άμεσες αντιδράσεις του προσωπικού στην περίπωση αντίληψης αυτού. Η γνώση για αρχικές αντιδράσεις και γνώση για το ποιόν θα ενημερώσουν και πότε, παίζει σημαντικό ρόλο στην αντιμετώπιση των επιθέσεων. Μια βάση δεδομένων με καταγραφές απο προηγούμενες επιθέσεις είναι απαραίτητη για την ενημέρωση και επαγρύπνιση του προσωπικού.

2.5 Τρόποι αντιμετώπισης Ηλεκτρονικού Ψαρέματος (phishing):

1. Μια επίθεση ηλεκτρονικού ψαρέματος συνήθως πραγματοποιείται μέσω ενός μυνήματος ηλεκτρονικού ταχυδρομείου με το οποίο ο επιτιθέμενος προσπαθεί να πείσει το υποψήφιο του θύμα να[7]:

   α. Να κλικάρει ένα link

   β. Να ανοίξει ένα αρχείο

   γ. Να εγκαταστήσει ένα λογισμικό

   δ. Να εισάγει το username και το password σε μια σελίδα η οποία φαίνεται νόμιμη.

2. Μέτρα προστασίας[8]:

   α. Ενημέρωση του λογισμικού. Οι phishers οι οποίοι χρησιμοποιούν κακόβουλα λογισμικά (malwares) συνήθως στηρίζονται σε software bugs (Software bug είναι ένα λάθος, σφάλμα, αποτυχία, ή ελάττωμα σε ένα πρόγραμμα λογισμικού που το οδηγεί σε ανεπιθύμητη συμπεριφορά) έτσι ώστε να εισαγάγουν το malware στο υπολογιστικό σύστημα το οποίο στοχεύουν να παγιδεύσουν. Όταν το bug αυτό γίνει ευρέως γνωστό, οι κατασκευαστές λογισμικών θα απελευθερώσουν μια ενημέρωση (update) προκειμένου να το διορθώσουν το οποίο σημαίνει οτι παλιότερα μη ενημερωμένα λογισμικά θα έχουν πολύ περισσότερα bugs τα οποία θα έχουν μεγαλύτερη τρωτότητα όσον αφορά την εγκατάσταση απο επιτήδειους malwares. Συνεπώς τηρώντας ενημερωμένο κάποιος χρήστης το λογισμικό του αμβλύνει τις πιθανότητες μιας προσβολής απο κακόβουλο λογισμικό.

   β. Χρήση διαχειριστή κωδικού με εγκατεστημένο πρόγραμμα αυτόματης συμπλήρωσης σε βάση δεδομένων (auto-fill). Ο Διαχειριστής κωδικού είναι ένα εργαλείο το οποίο χρησιμοποιείται για την δημιουργία και αποθήκευση κωδικών έτσι ώστε ο χρήστης να δύναται να χρησιμοποιήσει

[7] https://ssd.eff.org/en/module/how-avoid-phishing-attacks
[8] https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

πολλούς διαφορετικούς κωδικούς σε διαφορετικά sites και υπηρεσίες χωρίς να χρειάζεται να τα μνημονεύει κάθε φορά. Το μόνο πράγμα που χρειάζεται ο χρήστης είναι να θυμάται μόνο το κεντρικό κωδικό (master password) με τον οποίο θα μπορεί να έχει πρόσβαση στην κρυπτοκαλυμένη βάση δεδομένων του συνόλου των κωδικών. Συνεπώς, ο διαχειριστής κωδικού συπληρώνει αυτόματα την βάση δεδομένων του με κωδικούς που χρησιμοποιήθηκαν ενώ παράλληλα απομνημονεύει την αντιστοιχία σελίδων και κωδικών που αντιστοιχούν σε αυτές. Έτσι ενώ θα ήταν εύκολο για κάποιον χρήστη να παγιδευτεί απο μια πλαστή σελίδα εισαγωγής (login page), ο διαχειριστής κωδικού θα τον προστατεύσει απο αυτήν λόγω του οτι στην βάση δεδομένων του δεν θα περιέχει την πλαστή αυτή σελίδα και κατα συνέπεια είναι αδύνατο να πραγματοποήσει την αντιστοιχία με κάποιον απο τους καταχωρημένους κωδικούς. Τέλος, ο διαχειριστής κωδικού μπορεί να λειτουργήσει και ως ανιχνευτής πλαστών σελίδων γιαί εαν αυτός αρνηθεί να κάνει auto-fill έναν κωδικό, αυτόματα σημαίνει οτι η σελίδα αυτή πληρεί συνθήκες αμφισβίτησης γνησιότητας.

γ. Επιβεβαίωση των emails μέσω επικοινωνίας με τον αποστολέα τους. Ενας τρόπος για να ανιχνεύσει ένας χρήστης εάν το email που έλαβε προέρχεται απο μια επίθεση ηλεκτρονικού ψαρέματος ή μη, είναι να το ελέγξει με την χρήση ενός διαφορετικού διαύλου επικοινωνίας με τον υποτιθέμενο αποστολέα. Για παράδειγμα, εάν ένα εισερχόμενο email υποτίθεται οτι έχει σταλεί απο μια τράπεζα, τότε είναι συνετό να μην κλικάρει ο χρήστης τον σύνδεσμο (link) ο οποίος περιέχεται συννημένος, αλλά αντιθέτως να καλέσει πρώτα τηλεφωνικά την τράπεζα ή να ανοίξει τον φυλλομετρητή του υπολογιστή του (γνωστό και ως browser) και να πληκτρολογήσει το URL του τραπεζικού ιστοτόπου για να ελέγξει την γνησιότητα του. Ομοίως, εάν κάποιος γνωστός αποστείλει ένα email με συννημμένες φωτογραφίες η κάποιο άλλο αρχείο, τότε προτείνεται ο χρήστης να επικοινωνήσει πρώτα τηλεφωνικά με τον αποστολέα για να επιβεβαιώσει την αποστολή αυτού του email πρωτού προβεί στο άνοιγμα των συννημμένων του.

δ. Άνοιγμα υπόπτων αρχείων με το Google Drive. Κάποια άτομα, λόγω της επαγγελματικής τους δραστηριότητας υπάρχει περίπτωση να περιμένουν να παραλάβουν emails μετα συννημένων αρχείων απο άγνωστους προς αυτούς αποστολείς. Για παράδειγμα, ένας οικονομικός αξιωματικός που έχει αναρτήσει στο διαδίκτυο μια προκύρυξη για την ανάθεση μιας εργασίας, κάτι που είναι πολύ συχνό και σύνηθες, θα αναμένει να λάβει κάποιες προσφορές ή κάποια έγγραφα γενικότερα απο διάφορες ενδιαφερόμενες ως προς τον διαγωνισμό, πηγές. Αλλά, είναι δύσκολο να πιστοποιήσεις ότι ένα έγγραφο Word, κάποια φύλλα Excel ή ένα Pdf αρχείο δεν περιέχουν ένα κακόβουλο λογισμικό. Σε αυτές τις περιπτώσεις, ως λύση ενδύκνειται ο χρήστης να μην διπλοκλικάρει το ‘’κατεβασμένο’’ αρχείο, αλλά να το ‘’ανεβάσει’’ πρώτα στο Google Drive ή σε κάποιο άλλο διαδικτυακό document reader. Αυτό με την σειρά του θα μετατρέψει το αρχείο σε ένα image ή σε ένα HTML αρχείο, το οποίο και θα αποτρέψει την εγκατάσταση ενός κακόβουλου λογισμικού στον υπολογιστή του.

Επιπρόσθετα, στην αγορά κυκλοφορούν πολλά λειτουργικά συστήματα-λογισμικά σχεδιασμένα για να παρέχουν προστασία απο κακόβουλα λογισμικά. Για παράδειγμα υπάρχουν τα TAILS και Qubes τα οποία βασίζονται σε λειτουργικό σύστημα Linux. Το TAILS είναι σχεδιασμένο έτσι ώστε να ‘’μπουτάρεται’’ (booted) και να τρέχει (run) ολοκληρωτικά μόνο μέσα απο έναν

εξωτερικό δίσκο, ένα USB stick, ή μια κάρτα SD. Αυτός ο σχεδιασμός δίνει την δυνατότητα στον χρήστη να εξασφαλίζει οτι κανένα ίχνος των ενεργειών που εκτελεί, εγγράφονται στον σκληρό δίσκο του υπολογιστή του, γεγονός που επιβεβαιώνει ότι κανένα κακόβουλο λογισμικό το οποίο τρέχει στο λειτουργικό σύστημα του υπολογιστή, δεν θα εμπλακεί με αυτό του TAILS. Το Qubes αντίστοιχα, είναι ένα πρόγραμμα το οποίο ξεχωρίζει τις εφαρμογές έτσι ώστε να μην υπάρχει αλληλεπίδραση μεταξύ τους, γεγονός που περιορίζει την αποτελεσματικότητα και την δυναμική ενός κακόβουλου λογισμικού. Τέλος μια online υπηρεσία ονόματι Virus Total, παρέχει την δυνατότητα στον χρήστη να υποβάλλει τα ύποπτα/ αναξιόπιστα links και αρχεία σε αυτό, και αυτο έχοντας έναν μηχανισμό με διάφορες antivirus λειτουργίες να φιλτράει και να ελέγξει τα παραπάνω αρχεία και links και να αναφέρει τα αποτελέσματα βαθμού αξιοπιστίας στον χρήστη.

ε. Προσοχή στις οδηγίες που αναγράφονται στα emails. Κάποια emails ηλεκτρονικού ψαρέματος εμφανίζονται έχοντας ως αποστολέα το τεχνικό τμήμα υποστήριξης (IT) και ζητάει απο τον χρήστη να αποστείλει τους κωδικούς χρήσης του υπολογιστή του ή να επιτρέψει σε έναν τεχνικό του τμήματος την remote πρόσβαση στο σύστημα ή να καταστήσει ανενεργά κάποιες απο τις λειτουργίες ασφαλείας του συστήματος του έτσι ώστε το τεχνικό τμήμα να μπορεί να επισκευάσει κάποιες ανωμαλίες και δυσλειτουργίες του συστήματος. Συνεπώς κάποιος πρέπει να είναι πολύ προσεκτικός πρωτού δώσει έτσι απροκάλυπτα οποιοδήποτε τεχνικό δεδομένο ή πληροφορία, ή ακόμα να ακολουθήσει κάποιες κατευθυνόμενες τεχνικές οδηγίες εκτός εάν είναι απολύτως σίγουρος οτι ο αποστολέας του email ή αυτός που ζήτησε εν γένει τις πληροφορίες ανήκει όντως στο τεχνικό τμήμα και δεν είναι κάποιος επιτήδειος.

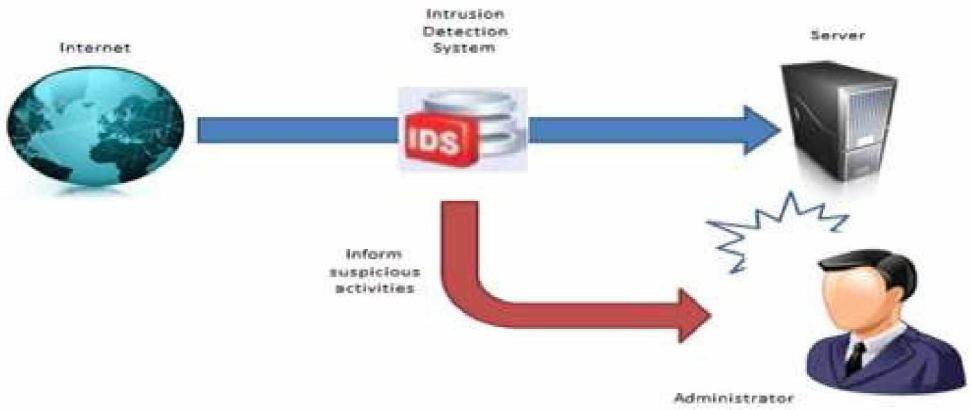
στ. Χρήση λογισμικού προστασίας ενάντια σε προγράμματα κατασκοπείας (Anti-spyware). Οι χρήστες υπολογιστικών συστημάτων προκειμένου να προστατεύσουν την ιδιωτικότητα τους και να το απόρρητο των πληροφοριών του υπολογιστή τους απο ποικίλα κατασκοπευτικά προγράμματα απαιτείται να αναπτύξουν δύο (2) επίπεδα προστασίας και ασφάλειας. Για παράδειγμα, οι υπεύθυνοι του τεχνικού τμήματος υπολογιστών ενός οργανισμού πρέπει πρωταρχικά να εγκαταστήσουν ένα spyware-detection λογισμικό, όπως αυτό της εταιρείας SpyCop (www.spycop.com) σε όλους τους διαθέσιμους σταθμούς εργασίας και να απαιτήσουν απο τους εργαζόμενους να εκτελούν περιοδικά σκαναρίσματα.

ζ. Προστασία από Ηλεκτρονικό Ψάρεμα και Κακόβουλο Λογισμικό στο Firefox. Όπως αναφέρεται στο site της Mozilla, το Firefox ενσωματώνει Προστασία από Ηλεκτρονικό Ψάρεμα (Phishing) και Κακόβουλο Λογισμικό (Malware) για να βοηθήσει τον χρήστη να παραμείνει ασφαλής στο διαδίκτυο. Αυτές οι λειτουργίες προειδοποιούν τον χρήστη όταν μια ιστοσελίδα που επισκέπτεται έχει αναφερθεί ως πλαστό αντίγραφο (γνωστή και ως σελίδα “ηλεκτρονικού ψαρέματος”) μιας νόμιμης ιστοσελίδας, ως πηγή Ανεπιθύμητου Λογισμικού ή ως Ιστοσελίδα Επιθέσεων, σχεδιασμένη να βλάψει τον υπολογιστή του (γνωστή και ως κακόβουλο λογισμικό). Αυτή η λειτουργία προειδοποιεί τον χρήστη και για τα αρχεία που κατεβάζει και ανιχνεύονται ως κακόβουλο λογισμικό. ‘’Η Προστασία αυτή λειτουργεί ελέγχοντας αν οι ιστοσελίδες που επισκέπτεστε ανήκουν σε κάποια λίστα αναφοράς για ηλεκτρονικό ψάρεμα, ανεπιθύμητο λογισμικό και κακόβουλο λογισμικό. Αυτές οι λίστες λαμβάνονται και ενημερώνονται αυτόματα κάθε περίπου 30 λεπτά, όταν

οι λειτουργίες Προστασίας από Ηλεκτρονικό Ψάρεμα και Κακόβουλο Λογισμικό είναι ενεργές. Όταν ο χρήστης κατεβάζει το αρχείο μια εφαρμογής, το Firefox ελέγχει αν η ιστοσελίδα που το φιλοξενεί ανήκει σε μια λίστα από ιστοσελίδες γνωστές για τη φιλοξενία "κακόβουλου λογισμικού". Αν η ιστοσελίδα βρεθεί στη λίστα αυτή, το Firefox αποκλείει αμέσως το αρχείο, διαφορετικά ρωτά την υπηρεσία Ασφαλούς Περιήγησης της Google αν το λογισμικό είναι ασφαλές, αποστέλλοντας σε αυτή μερικά από τα μεταδεδομένα της λήψης. Αυτές οι λειτουργίες είναι ενεργοποιημένες από προεπιλογή, οπότε, αν δεν αλλάξουν οι ρυθμίσεις ασφαλείας, είναι σχεδόν σίγουρο ότι ο χρήστης χρησιμοποιεί ήδη."[9]

η. Χρήση προγραμμάτων antispam – antimalware. Το Antispam είναι ένα λογισμικό το οποίο χρησιμοποιείται για να αποτρέψει ή να μπλοκάρει αυτόκλητα ή αυθαίρετα emails (γνωστά και ως spam) απο τα να ανοιχθούν ή να παραληφθούν. Τα προγράμματα αυτά χρησιμοποιούν ποικίλους τρόπους ώστε να ανιχνεύσουν τα spams, αυτοί μπορεί να είναι whitelists, blacklists, adresslists, καθώς και keyword matching. Η εγκατάσταση ενός αποτελεσματικού anti-malware λογισμικού θα προσέφερε προστασία ενάντια σε Trojan Horses, όπως το Kaspersky Anti-Virus το οποίο θα ανιχνεύσει και θα αποτρέψει την επίθεση.

2.6 Χρήση Intrution Detected Systems (IDS)



ΕΙΚΟΝΑ 15. IDS

1. Τα IDS πρέπει να χρησιμοποιούνται με τέτοιον τρόπο ώστε να[10]:

α. Εντοπίζουν προσπάθειες αποστολής μεγάλου όγκου εξερχόμενων πληροφοριών από του δικτυακού υπολογιστές σε εξωτερικούς. Χρήση Web Tap, το οποίο ανιχνεύσει προσπάθειες αποστολής σημαντικού όγκου εξερχομένων πληροφοριών δια μέσου HTTP καναλιών (tunnels) ξεγελώντας τους web servers' του δικτύου το οποίο προστατεύεται απο firewall.

β. Βοηθούν στην ανίχνευση προγραμμάτων κατασκοπευτικού λογισμικού (spyware programs).

[9] https://support.mozilla.org/en-US/
[10]http://ir.lib.uth.gr/bitstream/handle/11615/13579/P0013579.pdf?sequence=1&isAllowed=y

γ. Ανιχνεύουν προγράμματα backdoor. Όταν ένα κακόβουλο πρόγραμμα εγκατασταθεί σε ένα Η/Υ, όπως για παράδειγμα ένα δούρειος ίππος, το επόμενο βήμα είναι να δημιουργηθεί ένας τρόπο επικοινωνίας μεταξύ επιτιθέμενου και συστήματος, το οποίο και επιτυγχάνεται με την εγκατάσταση ενός backdoor προγράμματος.

δ. Εξετάζουν τα εξερχόμενα πακέτα που αποστέλλονται από του δικτυακούς Η/Υ σε εξωτερικούς servers' και να ελέγχουν αν σε αυτά περιέχονται κωδικοί χρηστών. Στην περίπτωση μεταφοράς μη κρυπτογραφημένων κωδικών χρηστών θα πρέπει να διακόπτεται η μετάδοση των πακέτων αυτών για λόγους προστασίας από κακόβουλους χρήστες.

ε. Εντοπίζουν κακόβουλο λογισμικό, ήτοι Δούρειο Ίππο προτού εγκατασταθεί στο σύστημα και εκτελέσει τη λειτουργία που του έχει προγραμματίσει ο επιτιθέμενος.

2.7 Μια άλλη χρήση των μεθόδων Κοινωνικής Μηχανικής

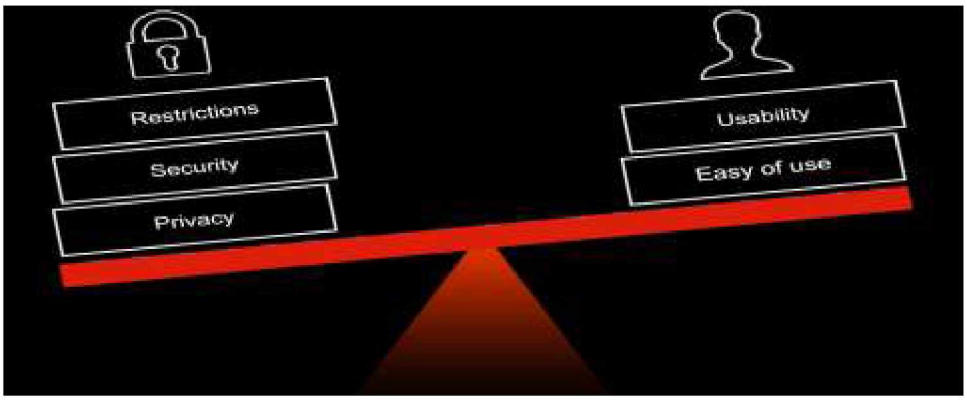
1. Πρόσφατα γνωστοποιήθηκε οτι η Turk Telekom ένας απο τους κορυφαίους παρόχους υπηρεσιών διαδικτύου της Τουρκίας, χρησιμοποίησε τεχνολογία φιλτραρίσματος ιστού για την εγκατάσταση λογισμικού υποκλοπής spyware στους υπολογιστές των πελατών της. Το Citizen Lab (παρατηρητήριο ψηφιακής ελευθερίας) ανακοίνωσε ότι Τούρκοι χρήστες που επιδίωξαν να κατεβάσουν δημοφιλή προγράμματα όπως το Skype και Avast Antivirus, κατευθύνθηκαν εν αγνοία τους σε πλαστές ιστοσελίδες οι οποίες περιείχαν λογισμικό spyware. Για να επιτευχθεί αυτό, η Turk Telekom χρησιμοποίησε διάφορους τύπους λογισμικών απο Βρετανία, Καναδά, Γερμανία και Αμερική, που επί του παρόντος δεν υπόκεινται σε νόμους ελέγχου των εξαγωγών.

2. ''Σύμφωνα με το Citizen Lab, οι φορείς εκμετάλλευσης των κατασκοπευτικών εφαρμογών (spyware) στοχεύουν διευθύνσεις IP σε πέντε πόλεις, μεταξύ των οποίων την Άγκυρα και τα Άδανα, που φιλοξενούν την αεροπορική βάση Incirlic. Στην υπόθεση αυτή, το λογισμικό χρησιμοποιήθηκε για τη παρακολούθηση αντιφρονούντων, τη στιγμή που είναι γνωστό πως τουλάχιστον 600 άτομα συνελήφθησαν πρόσφατα επειδή δημοσίευσαν αρνητικά σχόλια στα κοινωνικά δίκτυα. Σύμφωνα με νεότερες αναφορές από την ίδια πηγή, γερμανικό λογισμικό της εταιρίας FinFisher, χρησιμοποιήθηκε το τελευταίο διάστημα για τη παρακολούθηση των Κούρδων στη βόρεια Συρία. Η τελευταία προσπάθεια της τουρκικής κυβέρνησης για την τοποθέτηση spyware ευρείας κλίμακας καταδεικνύει την έλλειψη ελέγχου των εξαγωγών λογισμικού υψηλής τεχνολογίας spyware, που επιτρέπει σε αυταρχικά καθεστώτα όπως η Τουρκία να συνεχίζουν τη κατάχρηση της δυτικής τεχνολογίας για τη μαζική λογοκρισία και την ευρεία παρακολούθηση.''[11]

[11] https://citizenlab.ca/?s=turk+telekom

ΕΠΙΛΟΓΟΣ

Όπως έχει αναφέρει ο Mitnick στο βιβλίο του “Η τέχνη της απάτης”, η ασφάλεια των συστημάτων είναι υπόθεση ισορροπιών.



ΕΙΚΟΝΑ 16. Η ασφάλεια είναι υπόθεση ισορροπιών.

Η ελάχιστη ασφάλεια κάνει το σύστημα ευάλωτο ενώ η υπερβολική ασφάλεια εμποδίζει την ομαλή ροή των εργασιών και σε τελευταία ανάλυση των λειτουργιών τι οποίες είναι σχεδιασμένο το σύστημα να εκτελεί. Η πρόκληση για έναν μηχανικό ασφαλείας δικτύων είναι η επίτευξη της σωστής ισορροπίας μεταξύ ασφάλειας και παραγωγικότητας. Και δεν θα πρέπει να ξεχνάμε ότι πίσω απο τις υπολογιστικές μηχανές βρίσκεται ο άνθρωπος, συνεπώς η σημαντικότερη από όλες τι απειλές είναι η ανθρώπινη φύση που αποτελεί τον πιο αδύναμο κρίκο στην αλυσίδα της ασφάλειας των υπολογιστικών συστημάτων.[12]

[12] σελ 46, The art of Human hacking, christofer Hanargy, John Wiley & Sons, 29 Νοε 2010.

Βιβλιογραφία:

1. Φάκελος Σνόουντεν, 2014, Εκδόσεις Καστανιώτη.

2. Άρθρα απο **το site https://privacy.ellak.gr**

3. The art of Human hacking, christofer Hanargy, John Wiley & Sons, 29 Νοε 2010.

4. Ασφάλεια της πληροφορίας, Ανδρέας Σουρής, Δημήτρη Πατσός, Νίκος Γρηγοριάδης, έκδοση 1η, 2004, Εκδόσεις Νέων Τεχνολογιών.

5. Computer Security, William Stallings, Lawrie Brown, 2008, Pearson Education. Inc.

6. https://ssd.eff.org/en/module/how-avoid-phishing-attacks

7.https://support.mozilla.org/el/kb/enswmatwmenh-prostasia-apo-phishing-malware#w_asa-iaiciklalis-eia-kiieleahgia-aalcegcgga-gau-ukijealliju-eeaikg-jgi-ogjuhlekl-ulhickiju

8.http://docplayer.gr/8367828-Koinoniki-mihaniki-kai-asfaleia-ilektronikon-ypologiston-i-ptyhiaki-ergasia-2-o-1-mpletsas-ioannis-a-m-2004036-etiivlepon-kathigitis.html

9.http://ir.lib.uth.gr/bitstream/handle/11615/13579/P0013579.pdf?sequence=1&isAllowed=y

10.http://nefeli.lib.teicrete.gr/browse/sdo/acfi/2015/FazosGeorgios,FtoulisDimitrios/attached-document-1434447117-355038-13169/FazosGeorgios_FtoulisDimitrios2015.pdf

11.http://digilib.teiemt.gr/jspui/bitstream/123456789/1430/1/012010274.pdf

12. https://ssd.eff.org/en/module/how-avoid-phishing-attacks

13. https://computer.howstuffworks.com/what-is-spear-phishing.htm