ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Σχολή Τεχνολογίας

Τμήμα Ψηφιακών Συστημάτων

Τεχνικές OSINT σε Επιθέσεις Κοινωνικής Μηχανικής: Εκμετάλλευση Πληροφορίας Ανοιχτής Πηγής για Ρήγματα Ασφαλείας και Ανάπτυξη Μέτρων Κυβερνοασφάλειας

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ανδρόνικος Κωνσταντέλος (ΑΜ: 3119169)

Επιβλέπων: ***Ξενάκης Απόστολος , Επίκουρος Καθηγητής***

ΛΑΡΙΣΑ, Ιούνιος 2025

UNIVERSITY OF THESSALY

School of Technology

Digital Systems Department

OSINT Techniques in Social Engineering Attacks: Exploitation of Open Source Intelligence for Security Breaches and Development of Cybersecurity Measures

BACHELOR THESIS

Andronikos Konstantelos (RN: 3119169)

Supervisor: Xenakis Apostolos*, Assistant Professor*

LARISSA, June 2025

Υπεύθυνη Δήλωση περί Ακαδημαϊκής Δεοντολογίας και Πνευματικών Δικαιωμάτων

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα πτυχιακή εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον, και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται 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/Η Δηλών/ούσα

(Υπογραφή)

Ανδρόνικος Κωνσταντέλος

Ημερομηνία: 30/06δ/2025

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων/πουσα	**Ξενάκης Απόστολος** Επίκουρος Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Σάββας Ηλίας** Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Χαϊκάλης Κωνσταντίνος** Αναπληρωτής Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Ημερομηνία έγκρισης: 30-06-2025

Περίληψη

Η παρούσα πτυχιακή εργασία εξετάζει τη σύνδεση ανάμεσα στην **κοινωνική μηχανική (social engineering)** και τις τεχνικές **OSINT (Open Source Intelligence)**, αναδεικνύοντας τον τρόπο με τον οποίο η εκμετάλλευση δημόσια διαθέσιμων πληροφοριών μπορεί να οδηγήσει σε σοβαρά **ρήγματα ασφαλείας** για άτομα και οργανισμούς.

Η κοινωνική μηχανική αποτελεί σύνολο μεθόδων χειραγώγησης που στοχεύουν στην εκμετάλλευση της ανθρώπινης εμπιστοσύνης και αδυναμίας, παρακάμπτοντας τεχνικά μέτρα ασφαλείας. Από την άλλη πλευρά, το OSINT περιλαμβάνει τη συλλογή και ανάλυση πληροφοριών από ανοιχτές πηγές όπως κοινωνικά δίκτυα, μηχανές αναζήτησης, δημόσια αρχεία και data leaks.

Η εργασία αναλύει τους βασικούς τύπους επιθέσεων κοινωνικής μηχανικής — όπως phishing, vishing, smishing, pretexting και tailgating — και εξετάζει πώς το OSINT χρησιμοποιείται στη φάση της αναγνώρισης (reconnaissance) για τη δημιουργία **εξατομικευμένων σεναρίων επίθεσης**. Έμφαση δίνεται στην ψυχολογία του θύματος και στις τεχνικές πειθούς που χρησιμοποιούν οι δράστες.

Παρατίθενται **πραγματικά περιστατικά**, όπως η παραβίαση του Twitter το 2020, για να αναδειχθεί η πρακτική εφαρμογή των τεχνικών αυτών και η αποτελεσματικότητά τους, ακόμα και σε καλά προστατευμένα περιβάλλοντα. Επισημαίνεται ότι ακόμη και επιθέσεις φυσικής πρόσβασης μπορούν να προετοιμαστούν μέσω OSINT, αξιοποιώντας φωτογραφίες, δημόσια έγγραφα ή σχόλια χρηστών.

Η εργασία καταγράφει τις **επιπτώσεις** τέτοιων επιθέσεων — οικονομικές απώλειες, διαρροή δεδομένων, διακοπή λειτουργιών και νομικές κυρώσεις — και καταλήγει σε προτάσεις **αντιμετώπισης**: εκπαίδευση προσωπικού, περιορισμός ψηφιακού αποτυπώματος, τεχνικά μέτρα ασφαλείας και υιοθέτηση κατάλληλων πολιτικών.

Συμπερασματικά, ο συνδυασμός OSINT και κοινωνικής μηχανικής δημιουργεί ένα **πολυδιάστατο και εξελισσόμενο κίνδυνο**, ο οποίος μπορεί να αντιμετωπιστεί μόνο μέσω διαρκούς ενημέρωσης, προληπτικής δράσης και ενίσχυσης της κυβερνοασφάλειας σε οργανωτικό και ατομικό επίπεδο.

Abstract

This thesis investigates the intersection between **social engineering** and **Open Source Intelligence (OSINT)** techniques, highlighting how the exploitation of publicly available information can lead to severe **security breaches** for individuals and organizations.

Social engineering refers to a set of manipulation techniques targeting human behavior, bypassing technical security mechanisms by exploiting trust, urgency, and psychological weaknesses. OSINT, on the other hand, involves the collection and analysis of legally accessible data from open sources such as social networks, search engines, public records, and leaked databases.

The study outlines the main types of social engineering attacks — including phishing, vishing, smishing, pretexting, and tailgating — and examines how OSINT is used in the **reconnaissance phase** to craft **highly personalized and convincing attack scenarios**. Special attention is paid to victim psychology and influence principles employed by attackers.

Real-world incidents, such as the **2020 Twitter breach**, are analyzed to demonstrate the practical application and high effectiveness of these combined methods, even against well-secured environments. The thesis also explores how OSINT can be used to facilitate **physical intrusions**, leveraging images, public documents, or user reviews.

It further assesses the **impacts** of such attacks — including financial losses, data leakage, operational disruption, and legal penalties — and proposes **mitigation measures** such as employee awareness training, digital footprint minimization, technical safeguards (e.g., MFA), and organizational security policies.

In conclusion, the combination of OSINT and social engineering forms a **multifaceted and evolving threat**, which can only be effectively countered through continuous education, proactive measures, and the reinforcement of cybersecurity both at the individual and institutional level.

Περιεχόμενα

1 Εισαγωγή

Η ραγδαία ψηφιοποίηση της κοινωνίας έχει αυξήσει δραματικά τον όγκο πληροφοριών που διατίθενται δημοσίως στο διαδίκτυο. Αυτή η πληθώρα πληροφοριών ανοικτής πηγής (OSINT)

από προφίλ κοινωνικών δικτύων έως δημόσια έγγραφα, διευκολύνει τις επιθέσεις κοινωνικής μηχανικής, καθώς παρέχει στους επιτιθέμενους τα μέσα να μελετήσουν πιθανά θύματα και να εξαπατήσουν πιο πειστικά. Η κοινωνική μηχανική αναφέρεται σε ένα σύνολο τεχνικών εξαπάτησης και ψυχολογικής χειραγώγησης που στοχεύουν την ανθρώπινη συμπεριφορά, συνιστώντας βασικό παράγοντα παραβίασης ασφαλείας, καθώς αξιοποιούν εγγενείς αδυναμίες της ανθρώπινης κρίσης (Nonum et al., 2025). Σε αντίθεση με καθαρά τεχνικές κυβερνοεπιθέσεις,

η κοινωνική μηχανική εκμεταλλεύεται τον «ανθρώπινο παράγοντα», συχνά θεωρούμενο ως ο ασθενέστερος κρίκος στην ασφάλεια συστημάτων. Σύμφωνα με πρόσφατες μελέτες, το 82% των παραβιάσεων ασφάλειας περιλαμβάνει κάποιο ανθρώπινο σφάλμα ή κοινωνική επίθεση όπως το ηλεκτρονικό ψάρεμα (phishing) ή η εξαπάτηση μέσω τηλεφώνου (vishing) επιβεβαιώνοντας ότι το κοινωνικό engineering αποτελεί πρωταρχικό μέσο παραβίασης (Bonnie, 2024, *The Human Factor 2025: Vol. 1 Social Engineering | ProofPoint US*, 2025).

Η σύζευξη των OSINT τεχνικών με τις επιθέσεις κοινωνικής μηχανικής δημιουργεί ένα ιδιαίτερα επικίνδυνο σενάριο. Οι κακόβουλοι φορείς μπορούν να συλλέξουν από ανοιχτές πηγές πλήθος δεδομένων για ένα υποψήφιο θύμα ή οργανισμό – ονόματα και θέσεις προσωπικού, στοιχεία επικοινωνίας, παρουσίες στα μέσα κοινωνικής δικτύωσης, ακόμα και τεχνικές πληροφορίες για συστήματα – και να χρησιμοποιήσουν αυτές τις πληροφορίες για να σχεδιάσουν στοχευμένες εξαπατήσεις. Με αυτόν τον τρόπο, *οι επιθέσεις κοινωνικής μηχανικής γίνονται πιο πειστικές και αποτελεσματικές*, καθώς φαίνεται να προέρχονται από αξιόπιστες πηγές ή να σχετίζονται στενά με το προφίλ του εκάστοτε στόχου. Για παράδειγμα, μια επίθεση phishing που εξατομικεύεται με το όνομα, τη θέση εργασίας και τα ενδιαφέροντα του θύματος έχει σημαντικά αυξημένες πιθανότητες επιτυχίας. Επίσης η

ενσωμάτωση γενετικών μοντέλων τεχνητής νοημοσύνης (GenAI) έχει ενισχύσει περαιτέρω την αποτελεσματικότητα των επιθέσεων κοινωνικής μηχανικής, επιτρέποντας την αυτοματοποιημένη παραγωγή προσωποποιημένων phishing μηνυμάτων (Schmitt & Flechais, 2024; Yu et al., 2024).

2 Κοινωνική Μηχανική: Θεωρία και Τύποι Επιθέσεων

Μεταξύ τίτλων κεφαλαίου και πρώτης υποενότητας, καλό είναι να υπάρχει κάποιο εισαγωγικό κείμενο 2-3 σειρών (που συνήθως προλογίζει όσα ακολουθούν).

2.1 Ορισμός και Χαρακτηριστικά

Η κοινωνική μηχανική (social engineering) περιγράφεται ως η τέχνη της χειραγώγησης ανθρώπων ώστε να αποκαλύψουν εμπιστευτικές πληροφορίες ή να εκτελέσουν ενέργειες που αντιβαίνουν στο συμφέρον τους ή την πολιτική ασφαλείας ενός οργανισμού. Σε αντίθεση με τις τεχνικές επιθέσεις, οι οποίες στοχεύουν ευπάθειες λογισμικού ή δικτύων, οι επιθέσεις κοινωνικής μηχανικής εκμεταλλεύονται ψυχολογικές αδυναμίες, όπως η εμπιστοσύνη, ο φόβος, η απληστία ή η επιθυμία για βοήθεια. Κεντρικό στοιχείο αυτών των επιθέσεων είναι η παραπλάνηση, οι επιτιθέμενοι παρουσιάζονται πειστικά ως κάποιο αξιόπιστο πρόσωπο ή φορέας όπως συνεργάτης, τεχνική υποστήριξη, διευθυντικό στέλεχος με σκοπό να πείσουν το θύμα να αποκαλύψει πληροφορίες ή να παρακάμψει διαδικασίες ασφαλείας.

Βασικό χαρακτηριστικό της κοινωνικής μηχανικής είναι ότι αξιοποιεί τη φυσική τάση των ανθρώπων να δείχνουν εμπιστοσύνη και να βοηθούν. Πολλές επιθέσεις στηρίζονται στην πρόκληση ενός αισθήματος κατεπείγοντος ή αυθεντίας για παράδειγμα, ένας επιτιθέμενος μπορεί να προσποιηθεί τον προϊστάμενο που απαιτεί άμεσα πρόσβαση σε κάποιο σύστημα. Άλλες τεχνικές χειραγώγησης περιλαμβάνουν την επίκληση στην *περιέργεια* ή στον *φόβο*. Η επιτυχία τέτοιων τεχνικών εδράζεται στην ψυχολογία: μελετες δείχνουν ότι οι επιθέσεις κοινωνικής μηχανικής βασίζονται στην εμπιστοσύνη και ευπιστία των θυμάτων για να επιτύχουν. Με απλά λόγια, οι άνθρωποι είναι πιο πιθανό να κάνουν λάθη ασφαλείας όταν πειστούν ότι μια απατηλή αίτηση είναι νόμιμη και ακίνδυνη.

2.2 Κατηγορίες Επιθέσεων Κοινωνικής Μηχανικής

Οι επιθέσεις κοινωνικής μηχανικής παίρνουν πολλές μορφές, από σχετικά απλές έως εξαιρετικά στοχευμένες και περίπλοκες. Ορισμένες από τις κυριότερες κατηγορίες περιλαμβάνουν:

- **Phishing (Ηλεκτρονικό Ψάρεμα):** Η πιο διαδεδομένη μορφή, όπου ο επιτιθέμενος στέλνει παραπλανητικά email ή μηνύματα παρουσιάζοντας μια ψεύτικη ιστορία (π.χ. ειδοποίηση τράπεζας, προσφορά) ώστε να παρασύρει το θύμα να αποκαλύψει κωδικούς πρόσβασης, αριθμούς καρτών ή να πατήσει σε κακόβουλους συνδέσμους. Το phishing συνιστά την αιχμή του δόρατος για πολλές παραβιάσεις – εκτιμάται ότι η πλειονότητα των κυβερνοεπιθέσεων ξεκινά με ένα email phishing προς κάποιον ανυποψίαστο χρήστη

  (Salahdine & Kaabouch, 2019).

- **Spear Phishing (Στοχευμένο Phishing):** Μια εξελιγμένη παραλλαγή του phishing, όπου τα μηνύματα είναι ειδικά προσαρμοσμένα στο συγκεκριμένο θύμα ή οργανισμό. Ο δράστης πρώτα **συλλέγει πληροφορίες** για το θύμα (συχνά μέσω OSINT) – όπως όνομα, θέση, συνεργάτες, πρόσφατες δραστηριότητες – και εν συνεχεία στέλνει ένα πειστικό μήνυμα που φαίνεται να έχει νόημα στο πλαίσιο του θύματος. Για παράδειγμα, ένα spear-phishing email μπορεί να προσποιείται ότι προέρχεται από τον διευθύνοντα σύμβουλο της εταιρείας του θύματος, αναφερόμενο σε ένα πραγματικό εσωτερικό έργο, κάνοντας έτσι την απάτη πολύ πιο αληθοφανή (Salahdine & Kaabouch, 2019).

  Vishing (Voice Phishing): Η κοινωνική μηχανική μέσω τηλεφωνικών κλήσεων. Ο επιτιθέμενος χρησιμοποιεί τη φωνητική επικοινωνία – συνήθως προσποιούμενος έναν αξιωματούχο ή τεχνικό – για να πείσει το θύμα να αποκαλύψει ευαίσθητα στοιχεία ή να εκτελέσει κάποια ενέργεια. Για παράδειγμα, δράστες μπορεί να τηλεφωνούν σε υπαλλήλους εταιρείας υποδυόμενοι την τεχνική υποστήριξη και να τους ζητούν κωδικούς ή έγκριση διότι «υπάρχει πρόβλημα στο σύστημα». Η μέθοδος αυτή χρησιμοποιήθηκε και στο περίφημο περιστατικό παραβίασης του

Twitter (2020), όπως θα δούμε αναλυτικά στο Κεφάλαιο 7, όπου οι δράστες κάλεσαν υπαλλήλους προσποιούμενοι το τμήμα IT (Salahdine & Kaabouch, 2019).

- **Smishing:** Παρόμοιο με το phishing, αλλά μέσω SMS ή εφαρμογών μηνυμάτων. Το θύμα λαμβάνει ένα απατηλό μήνυμα κειμένου (π.χ. υποτιθέμενη ειδοποίηση από τράπεζα ή courier) που περιέχει κάποιο ύποπτο σύνδεσμο ή οδηγία να καλέσει σε έναν αριθμό. Ενώ πιο σύντομα σε περιεχόμενο, τα SMS μπορούν να φανούν πειστικά, ιδίως όταν εκμεταλλεύονται υπηρεσίες που χρησιμοποιεί το θύμα (Mehta et al., 2021).
- **Pretexting:** Σε αυτήν την περίπτωση, ο επιτιθέμενος κατασκευάζει ένα ολόκληρο *σενάριο* (pretext) για να αλληλεπιδράσει με το θύμα και να αποσπάσει πληροφορίες. Για παράδειγμα, μπορεί να παρουσιαστεί ως ερευνητής ή νέος πελάτης και να εμπλέξει το θύμα σε μια σειρά συνομιλιών, αποκτώντας σιγά-σιγά εμπιστοσύνη και ευαίσθητες λεπτομέρειες. Το pretexting συχνά προϋποθέτει εκτενή έρευνα στο θύμα εκ των προτέρων, ώστε το σενάριο να είναι πειστικό (Chetioui et al., 2022).
- **Baiting και Quid Pro Quo:** Στις επιθέσεις δόλωμα (baiting), ο δράστης δελεάζει το θύμα με μια υποσχόμενη ανταμοιβή ή κάτι ελκυστικό (π.χ. δωρεάν λογισμικό, μουσική, ή ένα ξεχασμένο USB stick «τυχαία» σε κοινό χώρο), που όμως κρύβει κακόβουλο περιεχόμενο. Στις επιθέσεις quid pro quo, προσφέρεται κάποια υπηρεσία ή όφελος σε αντάλλαγμα για πληροφορίες όπως για παράδειγμα αν ο δράστης παριστάνει τον τεχνικό που υπόσχεται να διορθώσει έναν υπολογιστή με αντάλλαγμα τους κωδικούς πρόσβασης του χρήστη
  (Salahdine & Kaabouch, 2019, Kushwaha et al., 2024).
- **Tailgating (Ανεπίτρεπτη Είσοδος):** Μία φυσική μορφή κοινωνικής μηχανικής, όπου ένας επιτιθέμενος εκμεταλλεύεται την ευγένεια ή απροσεξία για να εισέλθει σε χώρους με ελεγχόμενη πρόσβαση. Για παράδειγμα, μπορεί να ακολουθήσει έναν υπάλληλο σε μια ασφαλή είσοδο πριν κλείσει η πόρτα ή να προσποιηθεί τον διανομέα για να περάσει από τη ρεσεψιόν. Αν και φυσική μέθοδος, συχνά προηγείται ηλεκτρονική συλλογή πληροφορίας (OSINT) για να γνωρίζει ο δράστης το περιβάλλον, τους υπαλλήλους ή τις διαδικασίες του οργανισμού-στόχου (Adu-Manu et al., 2022).

Οι παραπάνω κατηγορίες δεν είναι ανεξάρτητες συχνά οι επιτιθέμενοι συνδυάζουν τεχνικές. Για παράδειγμα, μια επίθεση Business Email Compromise (BEC) μπορεί να ξεκινήσει με spear phishing ώστε ο δράστης να αποκτήσει πρόσβαση σε έναν εταιρικό λογαριασμό email, και στη συνέχεια να στείλει *vishing* τηλεφωνικές εντολές σε λογιστήριο για μεταφορά χρημάτων. Το κοινό στοιχείο είναι ότι όλες εκμεταλλεύονται την ανθρώπινη εμπιστοσύνη και άγνοια ως μονοπάτι προς την παραβίαση ασφαλείας (Papathanasiou et al., 2023).

2.3 Ο «Κύκλος» της Κοινωνικής Μηχανικής και Ψυχολογία Θύματος

Οι περισσότερες επιθέσεις κοινωνικής μηχανικής ακολουθούν μια παρόμοια διαδικαστική προσέγγιση, γνωστή και ως **κύκλος ζωής επίθεσης κοινωνικής μηχανικής**. Συμφωνα με τους Naz et al., (2024) και Lalit et al. (2023) σε γενικές γραμμές, ένας τέτοιος κύκλος περιλαμβάνει τα εξής στάδια:

1. **Αναγνώριση και Έρευνα (Reconnaissance):** Ο επιτιθέμενος επιλέγει στόχο και συγκεντρώνει πληροφορίες για αυτόν. Αυτό το στάδιο συχνά περιλαμβάνει εκτεταμένη χρήση OSINT όπως αναζήτηση στο διαδίκτυο για δημόσια προφίλ, στοιχεία επικοινωνίας, εταιρικές δομές, ακόμη και τεχνικές πληροφορίες όπως τομέα email του οργανισμού, προηγούμενες παραβιάσεις δεδομένων κ.α.. Η έρευνα βοηθά τον δράστη να κατανοήσει ποιες προσεγγίσεις θα είναι πιο αποτελεσματικές και ποια πρόσωπα-κλειδιά μπορεί να στοχοποιήσει.
2. **Εγκαθίδρυση Σχέσης (Hook):** Σε αυτό το στάδιο, ο δράστης έρχεται σε επαφή με το θύμα υπό ψεύτικη πρόφαση. Αυτό μπορεί να είναι ένα email, τηλεφώνημα ή δια ζώσης επικοινωνία. Στόχος είναι να κερδίσει την εμπιστοσύνη του θύματος – συχνά αξιοποιώντας τις πληροφορίες από το προηγούμενο στάδιο για να φανεί αξιόπιστος. Για παράδειγμα, αν γνωρίζει από το LinkedIn του θύματος ότι συνεργάζεται με συγκεκριμένο πελάτη, μπορεί να προσποιηθεί τον εκπρόσωπο

αυτού του πελάτη. Η **ψυχολογική χειραγώγηση** παίζει κρίσιμο ρόλο: οι επιτιθέμενοι μπορεί να χρησιμοποιήσουν τακτικές ευγένειας, κολακείας, ή πίεσης (επείγοντος) για να *«αγκιστρώσουν»* το θύμα.

3. **Εκτέλεση (Play):** Αφού έχει κερδίσει αρκετή εμπιστοσύνη, ο επιτιθέμενος προβαίνει στην κύρια πράξη εξαπάτησης. Αυτό μπορεί να σημαίνει ότι ζητά από το θύμα να του δώσει συγκεκριμένες πληροφορίες, όπως κωδικούς, αριθμούς λογαριασμών, να ανοίξει ένα συνημμένο αρχείο που περιέχει κακόβουλο λογισμικό ή να κάνει κλικ σε έναν σύνδεσμο που θα εγκαταστήσει κάποιο malware. Σε άλλες περιπτώσεις, μπορεί να του ζητήσει να εκτελέσει μια ενέργεια όπως μεταφορά χρημάτων σε έναν «εγκεκριμένο» λογαριασμό. Η επιτυχία αυτής της φάσης εξαρτάται από το πόσο καλά προετοιμάστηκε το έδαφος νωρίτερα, ένα καλά μελετημένο πρόσχημα θα κάνει το αίτημα του δράστη να φαίνεται φυσιολογικό.

4. **Λήξη και Κάλυψη Ιχνών (Exit):** Αφού ο δράστης αποκτήσει ό,τι επιδιώκει, τερματίζει την επικοινωνία με τρόπο που να μην κινήσει υποψίες. Ιδανικά, το θύμα μπορεί να μην συνειδητοποιήσει ποτέ ότι εξαπατήθηκε, τουλάχιστον όχι μέχρι να φανεί κάποια συνέπεια (όπως μη εξουσιοδοτημένες συναλλαγές ή παραβίαση λογαριασμού). Οι ικανοί κοινωνικοί μηχανικοί συχνά παίρνουν μέτρα για να καλύψουν τα ίχνη τους ή να καθυστερήσουν την ανίχνευση όπως για παράδειγμα να ζητούν από το θύμα να μην μιλήσει σε κανέναν για το αίτημα «για λόγους ασφαλείας» ή εκμεταλλεύονται μηχανισμούς ανάκτησης δεδομένων που δεν αφήνουν άμεσα εμφανή σημάδια στον χρήστη.

3 Open Source Intelligence(OSINT)

3.1 Ορισμός και Πηγές Ανοιχτής Πληροφορίας

Ως Open Source Intelligence (OSINT) ορίζεται η συλλογή και ανάλυση πληροφοριών από διαθέσιμες ανοικτές πηγές, δηλαδή πηγές που είναι προσβάσιμες νόμιμα στο κοινό και δεν προστατεύονται από πνευματικά δικαιώματα ή απόρρητο . Οι ανοικτές πηγές περιλαμβάνουν ένα ευρύ φάσμα μέσων και δεδομένων συμπεριλαμβανομένων ιστοτόπων και μέσων κοινωνικής δικτύωσης, ειδησεογραφικών άρθρων, μητρώων επιχειρήσεων, δημοσίων εγγράφων κυβερνήσεων, βάσεων δεδομένων διαρροών, ακόμη και πληροφοριών από δορυφορικές εικόνες

ή forums στο σκοτεινό διαδίκτυο. Οτιδήποτε δηλαδή είναι διαθέσιμο στο ευρύ κοινό έστω και δυσεύρετο, θεωρείται όμως ανοικτή πληροφορία και μπορεί να αξιοποιηθεί για εξαγωγή χρήσιμων συμπερασμάτων. (Nobili, 2023)

Το περιεχόμενο των ανοικτών πληροφοριών είναι εξαιρετικά ποικιλόμορφο. Για παράδειγμα, μια φωτογραφία που ανεβάζει ένας χρήστης στα κοινωνικά δίκτυα μπορεί να αποκαλύψει την τοποθεσία του (μέσω γεωδεδομένων), την ημερομηνία και τις συνθήκες της δραστηριότητάς του, τους φίλους ή συνεργάτες που εμφανίζονται, αντικείμενα στο περιβάλλον (π.χ. μάρκες συσκευών) και άλλα μεταδεδομένα. Ένα απλό βιογραφικό σημείωμα στο LinkedIn μπορεί να προσφέρει πληροφορίες για το ιστορικό καριέρας ενός ατόμου, δεξιότητες, ακόμα και τις τεχνολογίες που γνωρίζει – στοιχεία που μπορούν να φανούν πολύτιμα σε κάποιον που σχεδιάζει στοχευμένη επίθεση. Δημόσια αρχεία επιχειρήσεων (π.χ. τα εταιρικά μητρώα, ισολογισμοί) μπορούν να αποκαλύψουν τη δομή και τους υπεύθυνους μιας εταιρείας. Ακόμη και φαινομενικά αθώες πληροφορίες, όπως αναρτήσεις σε φόρουμ τεχνικής υποστήριξης, μπορεί να *διαρρεύσουν* εκθετικά δεδομένα – π.χ. ένας υπάλληλος ζητά βοήθεια online για ένα

πρόβλημα λογισμικού, αποκαλύπτοντας έτσι ποιο λογισμικό χρησιμοποιεί η εταιρεία του και τι είδους προβλήματα αντιμετωπίζει (Nobili, 2023; Szymoniak & Foks, 2024).

Σύμφωνα με την ανασκόπηση Szymoniak & Foks (2024), οι πληροφορίες αυτές δεν είναι κατ' ανάγκην αξιόπιστες ή ακριβείς καθώς προέρχονται από δημόσιες πηγές και μπορεί να περιέχουν σφάλματα, παραπληροφόρηση ή να είναι ξεπερασμένες. Συνεπώς, ένα μέρος της OSINT διαδικασίας είναι και η επαλήθευση της ακρίβειας και αυθεντικότητας των συλλεγόμενων δεδομένων. Για παράδειγμα, έμπειροι αναλυτές OSINT θα εξετάσουν τα μεταδεδομένα μιας εικόνας για να βεβαιωθούν ότι δεν είναι επεξεργασμένη ή θα διασταυρώσουν μια είδηση με πολλαπλές πηγές. Παρά τις προκλήσεις αυτές, η αξία του OSINT έγκειται στο ότι μπορεί να παράσχει έγκαιρη και πλουσιότατη πληροφόρηση με ελάχιστο κόστος, αξιοποιώντας κυρίως ανοιχτά διαθέσιμα εργαλεία

Μερικές από τις πιο κοινές κατηγορίες ανοικτών πηγών περιλαμβάνουν:

- **Μηχανές Αναζήτησης και Διαδίκτυο:** Η αναζήτηση στο Google (και σε εξειδικευμένες μηχανές όπως Shodan για συσκευές ή Censys για υπηρεσίες) μπορεί να αποκαλύψει τεράστιο όγκο δεδομένων. Ακόμα και προχωρημένες τεχνικές αναζήτησης (*Google dorks*) επιτρέπουν τον εντοπισμό ευαίσθητων πληροφοριών που δεν είναι άμεσα ορατές (Rajamäki et al., 2024).
- **Μέσα Κοινωνικής Δικτύωσης (Social Media):** Πλατφόρμες όπως το Facebook, το Twitter (X), το Instagram, το LinkedIn είναι θησαυροί προσωπικών και επαγγελματικών δεδομένων. Δημόσιες αναρτήσεις, λίστες φίλων/συνδεδεμένων, ομάδες και σελίδες, ακόμα και σχόλια, δίνουν εικόνα για τις συνήθειες, τις προτιμήσεις και το κοινωνικό δίκτυο ενός ατόμου. Για οργανισμούς, τα κοινωνικά δίκτυα μπορεί να αποκαλύψουν ονόματα υπαλλήλων, εταιρικές εκδηλώσεις, τεχνολογίες που επιδεικνύουν σε δημοσιεύσεις, κ.ά. (Van Puyvelde & Rienzi, 2025).
- **Δημόσια Μητρώα και Βάσεις Δεδομένων:** Περιλαμβάνονται κυβερνητικά αρχεία όπως μητρώα εταιρειών, ονόματα τομέων/DNS, καταχωρήσεις WHOIS για domain names και IP διευθύνσεις, εμπορικά μητρώα, πιστοποιήσεις SSL και άλλες τεχνικές εγγραφές. Αυτά μπορούν να δείξουν ποιος κατέχει έναν ιστότοπο, ποια υποδομή δικτύου χρησιμοποιεί ένας οργανισμός ή τι θυγατρικές/εταιρικές σχέσεις έχει.

Διαρροές Δεδομένων (Data Leaks/Breaches): Δυστυχώς, τα τελευταία χρόνια τεράστιες βάσεις δεδομένων με διευθύνσεις email, κωδικούς πρόσβασης και άλλα προσωπικά δεδομένα έχουν διαρρεύσει στο διαδίκτυο. Ιστότοποι όπως το *Have I Been Pwned* επιτρέπουν την αναζήτηση αν συγκεκριμένα emails έχουν εκτεθεί. Αυτά τα δεδομένα – αν και δεν προέρχονται από «επίσημες» ανοικτές πηγές αλλά από παραβιάσεις – γίνονται ουσιαστικά OSINT μόλις δημοσιοποιηθούν, και οι επιτιθέμενοι τα χρησιμοποιούν εντατικά για να διευκολύνουν περαιτέρω επιθέσεις (π.χ. password spraying με γνωστούς κωδικούς). (*The Data Revolution: OSINT's Role in the Digital Age*, 2023)

- **Τύπος και Ειδήσεις:** Άρθρα ειδήσεων, ανακοινώσεις Τύπου, περιοδικά κ.λπ., μπορεί να περιέχουν κρίσιμες πληροφορίες. Για παράδειγμα, μια συνέντευξη στελέχους μπορεί να αποκαλύψει τα μελλοντικά σχέδια μιας εταιρείας ή μια είδηση για συνεργασία εταιρειών μπορεί να δώσει στοιχεία σε έναν επιτιθέμενο για να προετοιμάσει ένα σχετικό pretext

  (πρόσχημα). (Saundatikar & Seth, 2020)

- **Δορυφορικές και Street View Εικόνες:** Υπηρεσίες όπως το Google Earth και το Google Street View παρέχουν πρόσβαση σε οπτικό υλικό εγκαταστάσεων. Κάποιος μπορεί να μελετήσει την τοπογραφία και την περίμετρο ενός κτιρίου-στόχου, να εντοπίσει κάμερες ή σημεία εισόδου, βοηθώντας πιθανή φυσική διείσδυση.
- **Forums, Blogs, και Αποθετήρια Κώδικα:** Σε διαδικτυακά forums ή σε πλατφόρμες προγραμματιστών όπως το GitHub, μπορεί να βρεθούν πληροφορίες που διέρρευσαν κατά λάθος – π.χ. προγραμματιστής που ανέβασε κώδικα με σκληροκωδικοποιημένους κωδικούς πρόσβασης ή κλειδιά API. Αυτά παρέχουν άμεσους τεχνικούς δρόμους επίθεσης αν εντοπιστούν από κακόβουλους.

3.2 Εργαλεία και Μέθοδοι OSINT

Η συλλογή πληροφοριών OSINT μπορεί να πραγματοποιηθεί χειροκίνητα (manual), αλλά στην πράξη υπάρχει μια πληθώρα εργαλείων λογισμικού που αυτοματοποιούν και βελτιστοποιούν τη διαδικασία. Τέτοια εργαλεία είναι συχνά διαθέσιμα ελεύθερα ή ως ανοιχτού κώδικα, γεγονός

που σημαίνει ότι τόσο οι επαγγελματίες ασφαλείας όσο και οι επιτιθέμενοι μπορούν εύκολα να τα χρησιμοποιήσουν.

Παραδείγματα γνωστών εργαλείων OSINT παρουσιάζονται παρακάτω:

- Το **Maltego** είναι μια εφαρμογή που επιτρέπει τον συσχετισμό και την οπτικοποίηση πληροφοριών. Μπορεί, για παράδειγμα, να πάρει μια διεύθυνση email και να αυτοματοποιήσει την εύρεση σχετικών κοινωνικών προφίλ, καταχωρήσεων σε διαρροές, καταχωρήσεων DNS κ.ο.κ., παρουσιάζοντας ένα γράφημα συνδέσεων. (Maltego, 2023).
- Το **theHarvester** είναι ένα εργαλείο που συλλέγει emails, ονόματα υπαλλήλων, ονόματα υποτομέων και άλλα δεδομένα για έναν συγκεκριμένο τομέα (domain) από δημόσιες πηγές
  (Brown et al., 2016).
- Το **Shodan** αποκαλείται και «μηχανή αναζήτησης για IoT/Συσκευές». Επιτρέπει σε κάποιον να αναζητήσει ανοιχτές πόρτες και υπηρεσίες στο Διαδίκτυο. Για παράδειγμα, ένας αναλυτής ή επιτιθέμενος μπορεί να βρει όλες τις ευπαθείς κάμερες ασφαλείας ή servers με συγκεκριμένο λογισμικό εκτεθειμένους στο Internet. (Tundis et al., 2021)
- Το **Google Dorking** δεν είναι εργαλείο αλλά τεχνική: χρησιμοποιεί προηγμένες τελεστές στην Google για να βρει ευαίσθητες πληροφορίες όπως αρχεία με κωδικούς, λίστες χρηστών, backup databases που λανθασμένα έχουν αναρτηθεί δημόσια. Ένας *dork query* μπορεί λόγου χάρη να είναι: filetype:xls “password” για να βρει υπολογιστικά φύλλα που περιέχουν τη λέξη “password”. (Alabdulatif & Thilakarathne, 2025)
- **Social media scrapers**: Ειδικά scripts ή πλατφόρμες (όπως το snscrape) μπορούν να συλλέγουν δημοσιεύσεις από κοινωνικά δίκτυα κατά χρονική σειρά ή με βάση λέξεις-κλειδιά. Επίσης, εργαλεία όπως το CheckUsernames βοηθούν να βρεθεί αν ένα συγκεκριμένο username χρησιμοποιείται σε δεκάδες πλατφόρμες (χαρτογραφώντας έτσι την παρουσία ενός ατόμου στο διαδίκτυο).

Επιπλέον, υπάρχουν πλατφόρμες που συνδυάζουν δεδομένα από πολλές πηγές. Για παράδειγμα, ιστοσελίδες όπως η Intelligence X (εμπορικό εργαλείο) επιτρέπουν αναζήτηση σε ποικίλα αποθετήρια, συμπεριλαμβανομένου και του σκοτεινού διαδικτύου, με ένα ερώτημα. Το

Have I Been Pwned (HIBP) είναι υπηρεσία που συγκεντρώνει εκατοντάδες γνωστές διαρροές δεδομένων και απαντά αν ένα email ή username εμφανίζεται σε κάποια από αυτές. (Rajamäki, 2024)

Σύμφωνα με το *The Data Revolution: OSINT's Role in the Digital Age*, (2023), οι μέθοδοι OSINT γενικά ακολουθούν το μοντέλο του κύκλου πληροφοριών (intelligence cycle):

1. *Καθορισμός στόχου*: Τι πληροφορίες ψάχνουμε; (π.χ. "βρες όλα τα δημόσια στοιχεία για τον οργανισμό Χ").
2. *Συλλογή*: Χρήση εργαλείων και χειροκίνητων αναζητήσεων για απόκτηση δεδομένων από κάθε σχετική πηγή.
3. *Επεξεργασία*: Φιλτράρισμα, οργάνωση και συνδυασμός των ωμών δεδομένων. Εδώ μπορεί να περιλαμβάνεται και ο καθαρισμός θορύβου ή η επαλήθευση αξιοπιστίας.
4. *Ανάλυση*: Εξαγωγή νοήματος – τι μας λένε τα δεδομένα; Για παράδειγμα, από μια λίστα ονομάτων υπαλλήλων, μπορεί να εξαχθεί ποιοι ίσως έχουν κρίσιμους ρόλους. Από μεταδεδομένα ενός αρχείου pdf μπορεί να βρεθεί το όνομα του συγγραφέα και η εφαρμογή που χρησιμοποίησε (υπόδειξη για το λειτουργικό σύστημα του).
5. *Διάχυση/Αξιοποίηση*: Παρουσίαση των αποτελεσμάτων σε εκείνους που θα τα χρησιμοποιήσουν (π.χ. μια αναφορά για την ομάδα ασφάλειας ή, στην περίπτωση κακόβουλου φορέα, η απευθείας αξιοποίησή τους σε μια επίθεση).

Σημαντικό είναι ότι οι OSINT τεχνικές είναι διττής χρήσης: μπορούν να χρησιμοποιηθούν για θετικούς σκοπούς (π.χ. έλεγχος ασφαλείας, έρευνες δημοσιογράφων, εντοπισμός εγκληματιών από αρχές) αλλά και για κακόβουλους (συλλογή πληροφοριών για σχεδιασμό επίθεσης). Στα επόμενα κεφάλαια, εστιάζουμε στο πώς οι επιτιθέμενοι εκμεταλλεύονται το OSINT για κοινωνική μηχανική, ενώ στο Κεφάλαιο 6 θα δούμε πώς και οι αμυνόμενοι μπορούν να αξιοποιήσουν OSINT για καλύτερη προστασία.

3.3 OSINT και Κυβερνοασφάλεια: Ευκαιρίες και Προκλήσεις

Η άνθηση του OSINT έχει φέρει νέες ευκαιρίες αλλά και προκλήσεις στον χώρο της κυβερνοασφάλειας. Από τη μία πλευρά, οι υπεύθυνοι ασφάλειας μπορούν να χρησιμοποιούν

OSINT για εντοπισμό απειλών και αυτοψία του αποτυπώματος της εταιρείας τους στο διαδίκτυο. Για παράδειγμα, είναι πλέον σύνηθες μια εταιρεία να διενεργεί *OSINT αναγνώριση στον εαυτό της*: δηλαδή να ψάχνει τι πληροφορίες σχετικές με αυτήν κυκλοφορούν δημόσια (ονόματα και emails υπαλλήλων στο LinkedIn, τεχνικές λεπτομέρειες σε forums, διαρροές credentials κ.ο.κ.) και να αξιολογεί έτσι το επίπεδο έκθεσής της. Αυτή η πρακτική βοηθά στο να προληφθούν επιθέσεις κοινωνικής μηχανικής – αν ξέρω ποιες πληροφορίες για τον οργανισμό μου είναι εκεί έξω, μπορώ να εκπαιδεύσω το προσωπικό να μην εμπιστεύεται αβασάνιστα αιτήματα που τις αναφέρουν. Από την άλλη πλευρά, οι επιτιθέμενοι έχουν πλέον στη διάθεσή τους μια πρωτοφανή ποσότητα δεδομένων για τους στόχους τους. Το OSINT λειτουργεί ως πολλαπλασιαστής δύναμης: ένας επιτιθέμενος με περιορισμένους πόρους μπορεί, χάρη σε δημόσια διαθέσιμα εργαλεία και δεδομένα, να εκτελέσει αναγνώριση που παλαιότερα θα απαιτούσε εκ των έσω πληροφορίες. Μάλιστα, η εξέλιξη των τεχνολογιών (web 2.0, big data) σημαίνει ότι ολοένα και περισσότερες προσωπικές λεπτομέρειες βρίσκονται δημοσίως. Η κουλτούρα της συνεχούς κοινοποίησης (π.χ. στα κοινωνικά δίκτυα) έχει θολώσει τα όρια μεταξύ δημόσιου και ιδιωτικού, με αποτέλεσμα άτομα και εταιρείες συχνά άθελά τους να αποκαλύπτουν κρίσιμες πτυχές, όπως:

- Την υποδομή IT που χρησιμοποιούν (αναρτώντας αγγελίες για θέσεις IT όπου ζητούν εμπειρία σε συγκεκριμένα συστήματα – έτσι ο επιτιθέμενος μαθαίνει τι συστήματα υπάρχουν).
- Τις συνήθειες του προσωπικού (π.χ. φωτογραφίες από το γραφείο μπορεί να δείχνουν κάρτες πρόσβασης ή σημειώσεις με κωδικούς στον πίνακα).
- Κλειδιά πρόσβασης που διαρρέουν από ανθρώπινο λάθος (π.χ. προγραμματιστής ανεβάζει κώδικα στο GitHub με κωδικό πρόσβασης embeded, ή κάποιος απαντά σε forum υποστήριξης και χωρίς να προσέξει περιλαμβάνει ευαίσθητα στοιχεία στο screenshot).

Οι νομικές και ηθικές παράμετροι αποτελούν επίσης πρόκληση. Ενώ το OSINT αξιοποιεί *νόμιμα* προσβάσιμες πληροφορίες, υπάρχει μια γραμμή όπου η συλλογή δεδομένων μπορεί να θεωρηθεί παραβίαση της ιδιωτικότητας ή κατασκοπεία. Οι οργανισμοί πρέπει να εξισορροπούν την ανοιχτή φύση των δεδομένων με την ανάγκη για προστασία ευαίσθητων πληροφοριών. Στο πλαίσιο αυτό, έχουν αρχίσει να θεσπίζονται κανονισμοί και καλύτερες πρακτικές για τη διαχείριση του ψηφιακού αποτυπώματος (digital footprint) – ουσιαστικά, να εκπαιδεύονται οι χρήστες και οι επιχειρήσεις να περιορίζουν τί μοιράζονται δημοσίως. Συνολικά, το OSINT έχει καταστεί αναπόσπαστο κομμάτι της σύγχρονης κυβερνοασφάλειας. Παρέχει μεν πολύτιμη

γνώση και στους αμυνόμενους (π.χ. για έγκαιρη προειδοποίηση απειλών), αλλά εξίσου εξοπλίζει και τους επιτιθέμενους με προσβάσιμα μέσα κατασκοπείας. Η διαθεσιμότητα πληροφοριών απαιτεί από όλους αυξημένη εγρήγορση: όπως χαρακτηριστικά σημειώνεται, *οποιαδήποτε πληροφορία κοινοποιείται ανοικτά, μπορεί δυνητικά να χρησιμοποιηθεί κακόβουλα*. Το επόμενο κεφάλαιο εξετάζει ακριβώς πώς οι επιτιθέμενοι αξιοποιούν το OSINT για να διευκολύνουν και να ενισχύσουν τις επιθέσεις κοινωνικής μηχανικής.

4 Εκμετάλλευση OSINT σε επιθέσεις κοινωνικής μηχανικής

4.1 Συλλογή Πληροφοριών και Προφίλ Στόχου μέσω OSINT

Η πρώτη φάση κάθε καλά σχεδιασμένης επίθεσης κοινωνικής μηχανικής είναι η αναγνώριση (reconnaissance) δηλαδή η σχολαστική συλλογή πληροφοριών για το υποψήφιο θύμα ή τον οργανισμό-στόχο. Στη σύγχρονη εποχή, το μεγαλύτερο μέρος αυτής της αναγνώρισης γίνεται μέσω OSINT. Οι επιτιθέμενοι εκμεταλλεύονται κάθε διαθέσιμη ανοικτή πηγή για να σκιαγραφήσουν ένα λεπτομερές προφίλ του στόχου τους. (Nobili, 2023)

Όσον αφορά το προφίλ ατόμου (θύματος), σύμφωνα με τους Cascavilla et al. (2016) **έ**νας επιτιθέμενος μπορεί να ξεκινήσει με το όνομα και το email ενός υπαλλήλου. Χρησιμοποιώντας OSINT εργαλεία, θα αναζητήσει αυτό το όνομα σε κοινωνικά δίκτυα (LinkedIn, Facebook, Twitter κλπ.) ώστε να βρει θέσεις εργασίας, ενδιαφέροντα, σχέσεις και πρόσφατες αναρτήσεις. Για παράδειγμα, αν το θύμα έχει δημόσιο προφίλ στο LinkedIn, ο επιτιθέμενος θα μάθει τον ρόλο του στην εταιρεία, τους συνεργάτες του, ίσως και τα έργα στα οποία συμμετέχει. Μέσω Facebook Instagram μπορεί να αντλήσει προσωπικές πληροφορίες – γενέθλια, οικογενειακή κατάσταση, χόμπι, αγαπημένα μέρη. Ακόμη και λεπτομέρειες όπως η κατοικία ή ο αριθμός κινητού συχνά μπορούν να βρεθούν είτε άμεσα είτε έμμεσα (π.χ. από μητρώα τηλεφώνων ή προηγούμενες online

καταχωρίσεις). Για παράδειγμα οι δράστες του περιστατικού του Twitter (2020) έκαναν έρευνα για να εντοπίσουν ονόματα, ρόλους και στοιχεία επικοινωνίας υπαλλήλων της εταιρείας, χρησιμοποιώντας πιθανότατα δημόσια δεδομένα από LinkedIn και άλλα sites. Έτσι ήξεραν ποιον να στοχεύσουν και πώς να εμφανιστούν πειστικοί.

Το προφίλ περιλαμβάνει επίσης την χαρτογράφηση σχέσεων του θύματος και περιλαμβάνει ερωτήσεις όπως «Ποιος είναι ο προϊστάμενός του;» «Με ποιους άλλους αλληλεπιδρά συχνά;» «Αν ένας επιτιθέμενος γνωρίζει, για παράδειγμα, ότι το υποψήφιο θύμα έχει στενή συνεργασία με τον διευθυντή Χ σε ένα τρέχον project (γιατί το είδε σε μια ανάρτηση ή σε δελτίο τύπου),

μπορεί αργότερα να προσποιηθεί τον διευθυντή Χ στην επίθεση.» Επιπλέον, το προφίλ μπορεί να καλύψει και τεχνικές γνώσεις του θύματος – αν από δημόσιες ομιλίες ή άρθρα φαίνεται ότι το άτομο έχει επίγνωση των βασικών αρχών ασφαλείας, ο δράστης θα χρειαστεί πιο προσεκτική προσέγγιση.(Cascavilla et al. 2016)

Παράλληλα με το άτομο, οι επιτιθέμενοι συνθέτουν και την εικόνα, δηλαδή το προφίλ του οργανισμού στον οποίο ανήκει. Αυτό περιλαμβάνει:

- Τη **δομή** του οργανισμού (τμήματα, διευθύνσεις, ονόματα βασικών στελεχών) – πληροφορίες συχνά διαθέσιμες στην ιστοσελίδα της εταιρείας ή σε επαγγελματικά δίκτυα.
- Το **πεδίο δραστηριότητας** και λεξιλόγιο: ένας επιτιθέμενος θέλει να μιλήσει στη γλώσσα της εταιρείας. Αν η εταιρεία έχει συγκεκριμένη ορολογία για τους πελάτες της ή τα έργα της (πληροφορία από δελτία τύπου), ο δράστης θα την υιοθετήσει για να ακούγεται αυθεντικός.
- **Τεχνολογικό προφίλ:** Μέσω OSINT μπορεί κάποιος να μάθει τι τεχνολογίες χρησιμοποιεί ένας οργανισμός. Π.χ., με ένα απλό query στο Shodan μπορεί να βρει ποιο web server λογισμικό «τρέχει» ο δημόσιος ιστότοπός του, ή με αναζήτηση εργασιακών αγγελιών να δει τι λογισμικά ζητούνται. Υπάρχουν και ειδικά site (όπως το BuiltWith) που δίνουν πληροφορίες για τις τεχνολογίες ενός website. Αν ένας οργανισμός χρησιμοποιεί, π.χ., Microsoft 365, ο επιτιθέμενος θα το μάθει και έτσι θα μπορούσε να στείλει ένα ψεύτικο email ειδοποίησης Microsoft στοχευμένα.
- **Πολιτισμός και κανόνες:** Από κοινωνικά δίκτυα ή Glassdoor μπορεί κανείς να αντλήσει πληροφόρηση για τον εσωτερικό κανονισμό της εταιρείας, ωράρια, ακόμα και ονόματα εορτών ή εκδηλώσεων. Όλα αυτά μπορούν να βοηθήσουν στο να κάνει ο δράστης *κλικ* με το θύμα – π.χ. αναφέροντας «Είδα τις φωτογραφίες από το πρόσφατο εταιρικό event σας, συγχαρητήρια για την επέτειο των 20 χρόνων» (πληροφορία δημοσιευμένη στο Facebook) δημιουργεί αίσθημα οικειότητας.

Συνολικά, το OSINT προσφέρει στους δράστες την απαραίτητη “πρώτη ύλη” για να σχεδιάσουν μια επίθεση κοινωνικής μηχανικής. Όσο περισσότερες σχετικές πληροφορίες συγκεντρωθούν, τόσο πιο *αόρατο* και πιστευτό μπορεί να γίνει το σενάριο της απάτης. Στην εποχή μας, οι πιο

εξελιγμένες επιθέσεις όπως Advanced Persistent Threats από κρατικά καθοδηγούμενες ομάδες επενδύουν μεγάλο μέρος χρόνου στην OSINT φάση, πριν καν επιχειρήσουν οποιαδήποτε προσέγγιση προς το θύμα. Είναι χαρακτηριστικό ότι ομάδες όπως οι Exotic Lily και Cobalt Dickens που έχουν στοχεύσει οργανισμούς υψηλής αξίας, αφιέρωσαν χρόνο σε εκτενή έρευνα OSINT για τα θύματά τους, ώστε να φτιάξουν απολύτως αληθοφανή μηνύματα και ψεύτικες εταιρικές οντότητες για την εξαπάτηση (Stolyarov, 2022; (*Silent Librarian, TA407, COBALT DICKENS, Group G0122 | MITRE ATT&CK®*, n.d.).

4.2 Σχεδιασμός και εξατομίκευση επίθεσης βάσει OSINT

Μετά τη φάση της συλλογής πληροφοριών, οι δράστες περνούν στον σχεδιασμό της επίθεσης, χρησιμοποιώντας τα ευρήματα του OSINT για να μεγιστοποιήσουν τις πιθανότητες επιτυχίας. Δύο είναι τα βασικά πλεονεκτήματα που τους δίνει το OSINT σε αυτή τη φάση: (α) η εξατομίκευση (personalization) της επίθεσης όπου οι πληροφορίες που συλλέγονται μέσω OSINT επιτρέπουν τη δημιουργία μηνυμάτων που ανταποκρίνονται στο προφίλ του θύματος(Xu et al., 2022) και (β)

ή παράκαμψη μέτρων ασφαλείας μέσω γνώσης εκ των έσω όπου το OSINT διευκολύνει την κατανόηση και εκμετάλλευση αμυντικών μηχανισμών, όπως για παράδειγμα αναφορές περιγράφουν περιπτώσεις όπου, μετά από spear-phishing, οι επιτιθέμενοι έπεισαν τα θύματα να αποδεχτούν push MFA ειδοποιήσεις, επικαλούμενοι ανάγκη από την ομάδα IT (“Implementing Phishing-Resistant MFA,” 2022). Οι πληροφορίες που συγκεντρώθηκαν επιτρέπουν στον επιτιθέμενο να δημιουργήσει ένα μήνυμα ή σενάριο επίθεσης που να *ταιριάζει απόλυτα* στο προφίλ του θύματος. Για παράδειγμα:

- Αν το OSINT έδειξε ότι το θύμα μόλις ανακοίνωσε στο LinkedIn ότι πήρε προαγωγή, ο δράστης μπορεί να του στείλει ένα phishing email που να φαίνεται σαν «συγχαρητήρια

e-card από τον CEO» της εταιρείας. Η φυσική περιέργεια και φιλοφρόνηση μπορεί να οδηγήσουν το θύμα να ανοίξει το συνημμένο που περιέχει κακόβουλο λογισμικό.

- Αν γνωρίζει από το Facebook ότι το θύμα πρόσφατα έκανε διακοπές σε ένα νησί, θα μπορούσε να στείλει SMS (smishing) που να προσποιείται την ακτοπλοϊκή εταιρεία, λέγοντας ότι «υπάρχει επιστροφή χρημάτων από ακυρωμένο δρομολόγιο» με έναν σύνδεσμο για καταχώριση στοιχείων τράπεζας.

  Σε εταιρικό πλαίσιο, αν ο δράστης βρήκε ένα οργανόγραμμα με ονόματα, μπορεί να στείλει email στον υπάλληλο Α από τον «διευθυντή Β» (whaling attack) ζητώντας του επειγόντως κάποια στοιχεία. Επειδή τα ονόματα ταιριάζουν με πραγματικά πρόσωπα της εταιρείας, ο υπάλληλος Α δύσκολα θα αμφισβητήσει την γνησιότητα.

Βάσει πρόσφατων ερευνών, η στοχευμένη μορφή phishing, γνωστή ως *spear phishing*, θεωρείται εξαιρετικά αποτελεσματική, κυρίως λόγω της αξιοποίησης OSINT (Open Source Intelligence). Οι επιτιθέμενοι δεν χρησιμοποιούν δημόσιες πληροφορίες μόνο για να γεμίσουν τα μηνύματά τους με αληθοφανείς λεπτομέρειες, αλλά και για να επιλέξουν προσεκτικά τα πιο ευάλωτα θύματα. Για παράδειγμα, από μια λίστα εργαζομένων, μπορεί να στοχεύσουν τον πιο νέο ή λιγότερο έμπειρο υπάλληλο, θεωρώντας τον πιθανότερο να εξαπατηθεί, ή κάποιον από το τμήμα λογιστηρίου, γνωρίζοντας ότι έχει πρόσβαση σε ευαίσθητα οικονομικά συστήματα. Όπως περιγράφεται στη μελέτη των Burns et al. (2019) , οι επιτιθέμενοι επιλέγουν στόχους βασισμένοι σε πληροφορίες από το LinkedIn, αξιολογώντας τον ρόλο, την εμπειρία και την πιθανότητα επιτυχίας του δόλου. Παρόμοια ευρήματα παρουσιάζει και η Allodi et al. (2019), όπου τεκμηριώνεται η χρήση OSINT σε όλα τα στάδια προετοιμασίας της επίθεσης – από την αναγνώριση έως τη σύνθεση του μηνύματος. Οι αποφάσεις αυτές βασίζονται σε ακριβή γνώση που αποκτάται εξωτερικά, χωρίς να έχει παραβιαστεί το ίδιο το σύστημα του οργανισμού.

Εκτός από την πειστικότητα, το OSINT βοηθά τους δράστες να αποφύγουν ή να παρακάμψουν μηχανισμούς άμυνας. Ένας τρόπος είναι ο εξής: Αν γνωρίζουν ποια τεχνολογία ασφαλείας χρησιμοποιεί ο οργανισμός, μπορούν να *προσαρμόσουν* την επίθεσή τους. Για παράδειγμα, ας πούμε ότι ο OSINT αποκάλυψε πως ο οργανισμός χρησιμοποιεί **πολυπαραγοντικό έλεγχο ταυτότητας (MFA)** με push ειδοποιήσεις στο κινητό. Στο περιστατικό του Twitter 2020, οι δράστες το ήξεραν και κατάφεραν να το εκμεταλλευτούν – δημιούργησαν ψεύτικο login site,

πήραν το password των υπαλλήλων και όταν εμφανίστηκε η ειδοποίηση MFA στο κινητό, τους έπεισαν τηλεφωνικά ότι έπρεπε να την αποδεχτούν. Έτσι ουσιαστικά νίκησαν το MFA όχι τεχνικά, αλλά κοινωνικά, *χρησιμοποιώντας γνώση εκ των έσω ότι η εταιρεία στηριζόταν σε push MFA*.

Επίσης εστω ότι για παράδειγμα ένας οργανισμός καμαρώνει δημοσίως ότι εκπαιδεύει τους υπαλλήλους του στο phishing μέσω μηνυμάτων email, οι δράστες μπορεί να επιλέξουν το **vishing** ως εναλλακτική οδό, ξέροντας ότι οι υπάλληλοι είναι πιο υποψιασμένοι στα emails παρά στα τηλεφωνήματα. Ομοίως, αν μια εταιρεία ανακοινώνει ότι δεν θα ζητήσει ποτέ κωδικό μέσω email (πολλές το αναφέρουν στην πολιτική τους), ένας επιτιθέμενος θα αποφύγει να ζητήσει ευθέως κωδικό – μπορεί αντ' αυτού να ζητήσει άλλες πληροφορίες ή να πείσει το θύμα να εισάγει τον κωδικό σε μια «ασφαλή εταιρική σελίδα» (που στην πραγματικότητα ελέγχει ο δράστης).

Το OSINT μπορεί επίσης να αποκαλύψει κρίσιμες χρονικές συγκυρίες, τις οποίες οι επιτιθέμενοι εκμεταλλεύονται για τη διενέργεια χρονισμένων επιθέσεων επιχειρηματικής εξαπάτησης μέσω ηλεκτρονικής αλληλογραφίας (Timed Business Email Compromise – BEC attacks). Ενδεικτικά, μέσω πλατφορμών κοινωνικής δικτύωσης όπως το LinkedIn ή το Twitter, ένας επιτιθέμενος μπορεί να πληροφορηθεί ότι ο οικονομικός διευθυντής (CFO) μιας εταιρείας πρόκειται να παρευρεθεί σε συνέδριο, γεγονός που συνεπάγεται πιθανή απουσία ή περιορισμένη διαθεσιμότητα λόγω διαφοράς ώρας. Εκμεταλλευόμενος αυτό το παράθυρο ευκαιρίας, ο δράστης ενδέχεται να αποστείλει μήνυμα ηλεκτρονικού ταχυδρομείου σε υπάλληλο του λογιστηρίου, προσποιούμενος τον CFO, και να ζητήσει την άμεση εκτέλεση μιας χρηματικής συναλλαγής. Το αίτημα εμφανίζεται ως επείγον, και ο παραλήπτης αδυνατεί να επαληθεύσει την εγκυρότητά του με τον προϊστάμενό του, λόγω της χρονικής συγκυρίας. Πράγματι, πολλές επιθέσεις BEC βασίζονται σε δημόσια διαθέσιμες πληροφορίες, όπως ανακοινωμένα ταξίδια στελεχών ή προγραμματισμένες οικονομικές δραστηριότητες (π.χ. πλησίον της λήξης τριμήνου), προκειμένου να αυξήσουν την πιθανότητα επιτυχούς εξαπάτησης (Al-Musib et al., 2021).

Ακολουθούν παραδείγματα σχετικών επιθέσεων

1. Επίθεση στο Twitter - Ιούλιος 2020

Οι δραστηριότητες της επίθεσης περιλάμβαναν οργανωμένη συλλογή πληροφοριών για δομή help-desk και τίτλους στελεχών με χρήση OSINT (π.χ. LinkedIn, εταιρικοί κατάλογοι). Οι επιτιθέμενοι παρουσίασαν ομιλία προσαρμοσμένη στη γλώσσα της εταιρείας, γεγονός που κατέστησε την επικοινωνία μέσω τηλεφώνου εξαιρετικά πειστική (*Twitter Investigation Report*, 2020).Το αποτέλεσμα ήταν πρόσβαση σε credentials & MFA tokens, χωρίς τεχνικό εύρημα – γνωστό ως “phone spear phishing” ή vishing attack (Szymoniak & Foks, 2024).

2. Πανεπιστημιακή επίθεση μέσω spear-phishing

Σύμφωνα με τους Heiding et al. (2024), hackers με τη χρήση OSINT από ακαδημαϊκά site η/ και άρθρα δημιούργησαν «πρόσκληση συνεργασίας» email απευθυνόμενη σε καθηγητές· χρησιμοποιώντας αναφορά σε πραγματικό συνεργάτη και έργο, αύξησαν σημαντικά την πειστικότητα του μηνύματος.Μια σχετική ποσοτική έρευνα σε πανεπιστημιακό περιβάλλον καταγράφει υψηλά click-through rates, ειδικά όταν τα μηνύματα περιέχουν προσωπικές και ερευνητικές πληροφορίες .

4.3 Φυσική Πρόσβαση και OSINT

Η αξιοποίηση πληροφοριών ανοικτών πηγών (OSINT) δεν περιορίζεται αποκλειστικά στο πεδίο των ψηφιακών απειλών· αντιθέτως, διαδραματίζει κρίσιμο ρόλο και σε επιθέσεις που προϋποθέτουν φυσική διείσδυση σε εγκαταστάσεις. Στο πλαίσιο αυτό, επιτιθέμενοι μπορούν να εντοπίσουν σχεδιαγράμματα κτιρίων, φωτογραφίες υποδομών, ακόμη και κρίσιμες λεπτομέρειες από αναρτήσεις σε υπηρεσίες όπως το Google Maps – π.χ. σχόλια που αναφέρουν την έλλειψη φύλαξης σε συγκεκριμένες εισόδους μετά από ορισμένη ώρα (Tundis, Nga, et al., 2021). Επιπλέον, δημόσια έγγραφα, όπως οικοδομικές άδειες ή συμβάσεις έργων που δημοσιεύονται από δημόσιους φορείς, ενδέχεται να αποκαλύπτουν διαρρυθμίσεις χώρων, συστήματα ασφαλείας ή στοιχεία εξωτερικών συνεργατών (*SEC587: Advanced Open-Source Intelligence (OSINT) Gathering and Analysis | SANS Institute*, n.d ; Nonum, Avwokuruaye, & Ezemonye, 2025).

Χαρακτηριστικό παράδειγμα αποτελεί η υπόθεση της Target (2013), όπου η αρχική πρόσβαση στο εσωτερικό δίκτυο της εταιρείας και κατ’ επέκταση η παραβίαση των συστημάτων σημείων

πώλησης (POS) φέρεται να πραγματοποιήθηκε μέσω μιας εξωτερικής εταιρείας HVAC (*Krebs on Security*, 2025). Είναι πιθανό οι επιτιθέμενοι να εντόπισαν την εν λόγω εταιρεία μέσω OSINT μεθόδων όπως από δημοσιευμένα έγγραφα ανάθεσης έργου) και στη συνέχεια να πραγματοποίησαν κοινωνική μηχανική με στόχο τους εργαζομένους της, επιτυγχάνοντας τελικά έμμεση πρόσβαση στο σύστημα του κύριου στόχου.

Το συγκεκριμένο παράδειγμα αναδεικνύει τον τρόπο με τον οποίο το OSINT μπορεί να λειτουργήσει ως εργαλείο προετοιμασίας για επιθέσεις κοινωνικής μηχανικής, ενισχύοντας τη ρεαλιστικότητα και την αποτελεσματικότητά τους. Συγκεκριμένα, η αξιοποίηση πληροφοριών από ανοικτές πηγές παρέχει στους επιτιθέμενους τη δυνατότητα να:

- Επιλέγουν κατάλληλα τον στόχο και τον χρονισμό της επίθεσης.
- Κατασκευάζουν αληθοφανή σενάρια που παρακάμπτουν τα φίλτρα υποψίας των χρηστών.
- Εντοπίζουν εσωτερικές αδυναμίες και παρακάμπτουν τεχνικά ή φυσικά μέτρα ασφαλείας
- Αυξάνουν τη συνολική πιθανότητα επιτυχίας, ακόμη και όταν ο στόχος είναι καλά εκπαιδευμένος.

Συνεπώς, στο σύγχρονο περιβάλλον απειλών, το OSINT αποτελεί βασικό παράγοντα σχεδιασμού και επιτυχίας σύνθετων επιθέσεων, συμπεριλαμβανομένων και εκείνων με φυσική διάσταση. Στο επόμενο κεφάλαιο εξετάζονται οι επιπτώσεις τέτοιων επιθέσεων, καθώς και τα είδη ρηγμάτων ασφαλείας που προκύπτουν, μέσα από αναλύσεις πραγματικών περιστατικών.

5 Ρήγματα Ασφαλείας και Επιπτώσεις από Επιθέσεις Κοινωνικής Μηχανικής

5.1 Επιχειρησιακές και Οικονομικές Επιπτώσεις

Οι επιθέσεις κοινωνικής μηχανικής που αξιοποιούν πληροφορίες από ανοικτές πηγές (OSINT) αποτελούν συχνά το αρχικό στάδιο παραβιάσεων ασφαλείας, οδηγώντας σε σοβαρές επιχειρησιακές, οικονομικές και νομικές συνέπειες. Στο εταιρικό περιβάλλον, μια τέτοια επίθεση συνήθως μεταφράζεται σε μη εξουσιοδοτημένη πρόσβαση σε κρίσιμα συστήματα ή ευαίσθητα δεδομένα, μέσω της παραπλάνησης ενός εργαζομένου (Hadnagy, 2018; Al-Musib et al., 2021). Οι επιπτώσεις διακρίνονται στις εξής βασικές κατηγορίες:

Οικονομικές Απώλειες: Οι ζημίες μπορεί να είναι άμεσες – όπως η απώλεια χρηματικών ποσών σε επιθέσεις τύπου BEC ή έμμεσες, όπως το κόστος αποκατάστασης, οι νομικές αμοιβές, τα πρόστιμα συμμόρφωσης και η απώλεια πελατειακής εμπιστοσύνης (*Cost of a Data Breach 2024 | IBM*, 2024). Σύμφωνα με τη σχετική ετήσια μελέτη της IBM, το μέσο κόστος μιας παραβίασης δεδομένων παγκοσμίως ανήλθε το 2022 σε 4,35 εκατομμύρια δολάρια, με το αντίστοιχο κόστος στις ΗΠΑ να υπερβαίνει τα 9,4 εκατομμύρια. Οι επιθέσεις κοινωνικής μηχανικής συμβάλλουν σημαντικά σε αυτό, είτε ως μέσο αρχικής εισόδου (π.χ. phishing email που οδηγεί σε εγκατάσταση ransomware) είτε ως όχημα εκβίασης.

Διακοπή Λειτουργιών: Σε περιπτώσεις όπου οι επιθέσεις καταλήγουν σε εγκατάσταση κακόβουλου λογισμικού ή καταστρατήγηση διαπιστευτηρίων, μπορεί να σημειωθεί προσωρινή αναστολή λειτουργιών. Ενδεικτικό είναι το περιστατικό με την Περιφέρεια Λάτσιο στην Ιταλία το

2021, όπου κακόβουλο λογισμικό (ransomware), πιθανώς εγκατεστημένο μέσω phishing, παρέλυσε για ημέρες το πληροφοριακό σύστημα υγείας, επηρεάζοντας κρίσιμες λειτουργίες όπως

ο προγραμματισμός εμβολιασμών COVID-19 (Check Point Research, 2025). Οι επιπτώσεις υπερέβησαν το οικονομικό κόστος, επεκτεινόμενες στον τομέα της δημόσιας υγείας και της εμπιστοσύνης των πολιτών.

Κλοπή Πληροφοριών και Κατασκοπεία: Οι επιθέσεις spear phishing συχνά αποσκοπούν στην απόκτηση διαπιστευτηρίων ή εμπιστευτικών πληροφοριών, με σκοπό τη βιομηχανική κατασκοπεία ή τη διαρροή δεδομένων (Grimes & Just, 2024). Οι πληροφορίες αυτές μπορούν να πωληθούν στο σκοτεινό διαδίκτυο ή να αξιοποιηθούν σε εκβιαστικά σενάρια. Η διαρροή εσωτερικών εγγράφων της Sony Pictures το 2014, η οποία ξεκίνησε πιθανώς από τεχνικές κοινωνικής μηχανικής, κατέδειξε τις πολιτικές και επιχειρησιακές επιπτώσεις τέτοιων επιθέσεων (Cieply & Barnes, 2014).

Νομικές και Κανονιστικές Συνέπειες: Η ύπαρξη αυστηρών κανονισμών προστασίας προσωπικών δεδομένων (π.χ. GDPR στην Ε.Ε., HIPAA στις ΗΠΑ) καθιστά τέτοιες παραβιάσεις νομικά επιζήμιες. Οι οργανισμοί υποχρεούνται να ενημερώσουν τις αρχές και τους χρήστες, γεγονός που συνεπάγεται υψηλό πρόστιμο και αρνητικό δημοσιογραφικό αντίκτυπο (Kesan & Hayes, 2017). Η απώλεια δεδομένων λόγω κοινωνικής μηχανικής μπορεί να οδηγήσει όχι μόνο σε χρηματικές κυρώσεις, αλλά και σε νομικές αγωγές ή απώλεια συμμόρφωσης με συμβατικές υποχρεώσεις.

Επιθέσεις στην Εφοδιαστική Αλυσίδα (Supply Chain Attacks): Όταν το θύμα της κοινωνικής μηχανικής είναι κάποιος τρίτος συνεργάτης – όπως προμηθευτής τεχνολογικών υπηρεσιών – οι επιπτώσεις μπορεί να επεκταθούν σε πολλαπλούς οργανισμούς. Το φαινόμενο αυτό, γνωστό ως supply chain compromise, έχει καταγράψει σημαντικές επιπτώσεις σε διάφορους τομείς, προκαλώντας πτώση αξίας μετοχών, ρήξη εταιρικών σχέσεων και απώλεια εμπιστοσύνης πελατών (ENISA, 2021).

Συμπερασματικά, ακόμη και ένα φαινομενικά ασήμαντο ανθρώπινο σφάλμα – όπως το πάτημα ενός κακόβουλου συνδέσμου μπορεί να αποτελέσει την αφετηρία ενός ευρύτερου επιχειρησιακού ρήγματος, με πολυεπίπεδες συνέπειες.

5.2 Παραδείγματα Πραγματικών Περιστατικών

Απάτη Business Email Compromise (BEC) – Crelan Bank (2016): Το συγκεκριμένο περιστατικό αξίζει αναφοράς ως κλασική περίπτωση BEC. Οι επιτιθέμενοι χρησιμοποίησαν πληροφορίες για την ιεραρχία της τράπεζας πιθανόν από δελτία Τύπου και κοινωνικά δίκτυα για να στείλουν email στον οικονομικό διευθυντή, προσποιούμενοι τον CEO, ζητώντας μεταφορά μεγάλου ποσού. Η τράπεζα έχασε ~70 εκατ. ευρώ. Το περιστατικό αυτό κατέδειξε πόσο επικερδείς μπορεί να είναι οι επιθέσεις κοινωνικής μηχανικής υψηλού επιπέδου και οδήγησε πολλές εταιρείες να αναθεωρήσουν τα πρωτόκολλα τους για χρηματικές μεταφορές. (Zorz, 2018)

Πανδημία COVID-19 και κοινωνική μηχανική: Οι κυβερνοεγκληματίες εκμεταλλεύτηκαν την αναταραχή και τον φόβο γύρω από την πανδημία. Αναφορές έδειξαν έκρηξη phishing emails που προσποιούνταν κυβερνητικούς φορείς υγείας ή εταιρείες διανομής εμβολίων. Σε μια περίπτωση, ένα email με θέμα “Λίστα για εμβολιασμό – συμπληρώστε τα στοιχεία σας” παρέσυρε χιλιάδες χρήστες. Μεγάλο μέρος των δεδομένων για το πού να στοχεύσουν (π.χ. email γιατρών, κλινικών) οι δράστες το άντλησαν από ανοιχτές πηγές όπως ιστοσελίδες νοσοκομείων και λίστες ιατρών. Το FBI και οι ευρωπαϊκές αρχές εξέδωσαν προειδοποιήσεις για αύξηση άνω του 200% στις επιθέσεις phishing εν μέσω πανδημίας. (*COVID-19 Exploited by Malicious Cyber Actors*, 2020; Federal Bureau of Investigation, 2020)

Ransomware μέσω Social Engineering – Colonial Pipeline (2021): Μια από τις μεγαλύτερες επιθέσεις σε κριτική υποδομή στις ΗΠΑ. Οι δράστες (ομάδα DarkSide) εισχώρησαν στο δίκτυο μέσω παραβιασμένων credentials VPN. Πιθανολογείται ότι αυτά αποκτήθηκαν είτε από προηγούμενη διαρροή είτε με phishing ενός υπαλλήλου. Το αποτέλεσμα ήταν να κλείσει για μέρες ο αγωγός καυσίμων της Ανατολικής Ακτής, προκαλώντας ελλείψεις. Η εταιρεία πλήρωσε λύτρα ~$4,4 εκατ. και υπέστη τεράστιο πλήγμα αξιοπιστίας. Η κοινωνική μηχανική δεν ήταν απλά ένα εργαλείο οικονομικής απάτης εδώ, αλλά όπλο διατάραξης ζωτικών λειτουργιών. (*The*

Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years, 2023)

Επίθεση στο Twitter (2020) – Bitcoin Scam: Το περιστατικό αυτό θα αναλυθεί εκτενώς στο επόμενο κεφάλαιο ως μελέτη περίπτωσης. Εν συντομία, έφηβοι χάκερ κατάφεραν με τηλεφωνικό phishing να παραβιάσουν εσωτερικά συστήματα του Twitter, να πάρουν τον έλεγχο λογαριασμών διασήμων και εταιρειών (Elon Musk, Apple, κ.ά.) και να δημοσιεύσουν μια απάτη κρυπτονομισμάτων. Μολονότι τα κίνητρα ήταν οικονομικά (συγκέντρωσαν ~118 χιλ. δολάρια σε Bitcoin), το περιστατικό κατέδειξε πόσο ευάλωτες είναι ακόμη και οι ισχυρότερες πλατφόρμες από απλές τεχνικές κοινωνικής μηχανικής – και πόσο *χειραγωγήσιμο* είναι το κοινό μέσω έγκυρων λογαριασμών. Οι ρυθμιστικές αρχές επενέβησαν (έκθεση NYDFS) και υπογράμμισαν την ανάγκη αυστηρών ελέγχων ακόμα και σε μη χρηματοπιστωτικές εταιρείες λόγω τέτοιων κινδύνων. (*Three Individuals Charged for Alleged Roles in Twitter Hack*, 2020)

Διαρροή Δεδομένων Facebook (2021): Αν και δεν ήταν κλασική κοινωνική μηχανική επίθεση, στοιχεία κοινωνικής μηχανικής φαίνονται στο πώς επιτήδειοι εκμεταλλεύτηκαν λειτουργίες της πλατφόρμας για να συλλέξουν προσωπικά δεδομένα ~533 εκατομμυρίων χρηστών (τηλέφωνα, emails). Αυτά τα δεδομένα δημοσιεύθηκαν σε hacking forums (OSINT για όλους τους υπόλοιπους hackers) και μέσα στο 2021-2022 παρατηρήθηκε αύξηση spam κλήσεων και phishing SMS αξιοποιώντας τα. Δείχνει πώς ένα *ρήγμα ασφαλείας* μετατρέπεται σε τροφοδότη κοινωνικής μηχανικής ευρείας κλίμακας. (BBC News, 2021)

Από τα παραπάνω παραδείγματα, φαίνεται ότι οι επιθέσεις κοινωνικής μηχανικής:

- **Δεν κάνουν διακρίσεις σε στόχους:** Ιδιώτες, επιχειρήσεις κάθε μεγέθους, κυβερνητικοί οργανισμοί – όλοι μπορούν να πέσουν θύματα.
- **Μπορούν να έχουν πολλαπλασιαστικές επιπτώσεις:** Ένα λάθος ενός χρήστη μπορεί να οδηγήσει σε αλυσιδωτές παραβιάσεις.
- **Εξελίσσονται με το πλαίσιο:** Εκμεταλλεύονται γεγονότα (π.χ. πανδημία), νέες τεχνολογίες (social media), και οτιδήποτε μπορεί να αυξήσει την πιθανότητα επιτυχίας.
- **Συχνά αποτελούν την αρχή μιας μεγαλύτερης επίθεσης:** Όπως τονίζεται στη βιβλιογραφία, η κοινωνική μηχανική συχνά είναι το πρώτο βήμα πολύπλοκων κυβερνοεπιχειρήσεων.

Αυτός είναι ο λόγος που η **αντιμετώπιση** τους θεωρείται πλέον υψίστης σημασίας. Στο επόμενο κεφάλαιο, θα συζητήσουμε τα μέτρα και τις στρατηγικές που προτείνονται και εφαρμόζονται για την πρόληψη και άμβλυνση τέτοιων επιθέσεων – από την εκπαίδευση των χρηστών έως τεχνικές λύσεις και πολιτικές ασφαλείας.

6 Μέτρα Κυβερνοασφάλειας και Αντιμετώπισης

6.1 Εκπαίδευση και Ευαισθητοποίηση Χρηστών

Η εκπαίδευση των χρηστών αναγνωρίζεται ομόφωνα ως το πρώτο και σημαντικότερο ανάχωμα ενάντια στις επιθέσεις κοινωνικής μηχανικής. Δεδομένου ότι αυτές οι επιθέσεις στοχεύουν ανθρώπους, η ενδυνάμωση των ανθρώπων να τις αναγνωρίζουν και να αντιδρούν σωστά είναι κλειδί. Οι οργανισμοί θα πρέπει να διεξάγουν τακτικά προγράμματα ευαισθητοποίησης (security awareness training) για όλους τους εργαζομένους, ανεξαρτήτως ρόλου. Τα προγράμματα αυτά πρέπει να καλύπτουν:

- Τις βασικές μορφές κοινωνικής μηχανικής (phishing, vishing, κλπ) και **ενδείξεις** που τις προδίδουν (περίεργες διευθύνσεις email, ορθογραφικά λάθη, αιτήματα για ευαίσθητες πληροφορίες, κ.ά.).
- Συγκεκριμένα σενάρια που αφορούν τον εκάστοτε οργανισμό. Π.χ. ένας τραπεζικός οργανισμός θα εκπαιδεύσει το προσωπικό του να είναι καχύποπτο σε αιτήματα μεταφοράς χρημάτων που έρχονται μόνο με email, ειδικά αν δηλώνουν επείγοντα χαρακτήρα.
- Τις **διαδικασίες αναφοράς**: οι υπάλληλοι πρέπει να γνωρίζουν πού και πώς να αναφέρουν μια ύποπτη απόπειρα κοινωνικής μηχανικής. Ένα ταχύ σύστημα αναφοράς βοηθά τον οργανισμό να αντιδράσει προτού κλιμακωθεί ένα περιστατικό.
- Τις ιδιαιτερότητες του **απομακρυσμένου εργασιακού περιβάλλοντος** (remote work).

  Όπως σημειώνει έκθεση, κατά την μετάβαση στην εξ αποστάσεως εργασία αυξήθηκαν οι ευκαιρίες για social engineering (π.χ. χρήστες στο σπίτι που δεν μπορούν να επιβεβαιώσουν εύκολα με έναν συνάδελφο αν ένα αίτημα είναι νόμιμο). Η εκπαίδευση πρέπει να καλύπτει θέματα όπως: επιβεβαίωση

ταυτότητας καλούντος, μη εμπιστοσύνη σε ανεπίσημα κανάλια επικοινωνίας, κλπ.

Επιπλέον, **δοκιμές phishing** (phishing simulations) είναι μια καθιερωμένη πρακτική: οι ομάδες ασφαλείας στέλνουν περιοδικά ελεγχόμενα ψεύτικα phishing emails στο προσωπικό για να αξιολογήσουν την αντίδρασή του και να εντοπίσουν αδυναμίες. Σύμφωνα με ειδικούς, οι ασκήσεις αυτές είναι πιο αποτελεσματικές όταν **ενσωματώνουν ρεαλιστικά στοιχεία OSINT** – δηλαδή είναι τόσο πειστικές όσο και οι πραγματικές επιθέσεις. Έτσι οι υπάλληλοι εκπαιδεύονται σε *πραγματικές συνθήκες*, π.χ. λαμβάνοντας ένα phishing email που περιλαμβάνει το όνομα ενός πραγματικού πελάτη ή συνεργάτη (στοιχεία που θα μπορούσε να βρει ένας hacker). Οι επιτυχείς ή αποτυχημένες αντιδράσεις στις δοκιμές χρησιμοποιούνται για στοχευμένη επανεκπαίδευση.

Η κουλτούρα της **συνεχούς εγρήγορσης** πρέπει να καλλιεργηθεί. Ο στόχος είναι οι εργαζόμενοι να σκέφτονται κριτικά πριν εμπιστευτούν ένα απρόσμενο αίτημα. Όπως συνιστούν οι ρυθμιστικές αρχές, οι οργανισμοί οφείλουν να εξηγούν στο προσωπικό:

- *«Πώς θα επικοινωνήσει πραγματικά η εταιρεία μαζί σας για ζητήματα λογαριασμού ή ασφαλείας;»* (π.χ. δεν θα σας ζητήσει ποτέ κωδικό με email).
- *«Ποιές πρακτικές να ακολουθείτε όταν εργάζεστε απομακρυσμένα;»* (π.χ. χρήση VPN,

  επιβεβαίωση προτού δώσετε πληροφορίες στο τηλέφωνο).
- *«Πώς να αναφέρετε ύποπτες δραστηριότητες;»*.

εμπειρία έχει δείξει ότι εταιρείες που είχαν επενδύσει σε τέτοια εκπαίδευση απέτρεψαν μεγάλες ζημιές. Για παράδειγμα, αρκετές από τις μεγάλες εταιρείες κρυπτονομισμάτων στόχοι στην επίθεση του Twitter 2020 **δεν εξαπατήθηκαν** από τους δράστες, διότι διέθεταν μηχανισμούς επιβεβαίωσης σε live χρόνο (τηλεφωνική επιβεβαίωση συναλλαγής) και καλά εκπαιδευμένους υπαλλήλους που υποψιάστηκαν την απάτη.

6.2 Περιορισμός Ψηφιακού Αποτυπώματος και Έλεγχος Πληροφοριών

Αφού μεγάλο μέρος της επιτυχίας των επιθέσεων βασίζεται στο OSINT, ένα προληπτικό μέτρο είναι ο περιορισμός των ευαίσθητων πληροφοριών που είναι προσβάσιμες δημοσίως. Οι οργανισμοί πρέπει να ελέγχουν το ψηφιακό τους αποτύπωμα:

- **Πολιτική Κοινοποίησης:** Θέσπιση κανόνων για το τι μπορούν να δημοσιεύουν οι υπάλληλοι σε δημόσια fora και social media σχετικά με τη δουλειά τους. Π.χ. να αποφεύγεται η ανάρτηση φωτογραφιών από τον χώρο εργασίας που μπορεί να αποκαλύπτουν εξοπλισμό ή διαδικασίες ασφαλείας.

  Αποφυγή Υπερβολικής Διαμοίρασης: Περιορισμός των πληροφοριών που δίνονται σε δελτία Τύπου ή στο εταιρικό site. Δεν είναι απαραίτητο να βρίσκονται όλα τα ονόματα του προσωπικού online. Κάποιες εταιρείες μετά από BEC επιθέσεις αποφάσισαν να **αφαιρέσουν τη λίστα των στελεχών και email τους** από τις ιστοσελίδες τους, παρέχοντας αντ' αυτού μια γενική φόρμα επικοινωνίας.
- **Ψευδωνυμοποίηση δημόσιων λογαριασμών:** Για παράδειγμα, αντί ο διαχειριστής συστημάτων να έχει email *admin@company.com* (ευκολότατο για επιθέσεις), μπορεί να χρησιμοποιείται ένα πιο πολύπλοκο alias. Παρομοίως, οι εσωτερικές δομές (ονόματα servers, διευθύνσεις URL intranet) καλό είναι να μην διαρρέουν σε δημόσια repos ή αρχεία.
- **Τακτικός OSINT έλεγχος (OSINT auditing):** Όπως αναφέρθηκε, εταιρείες μπορούν να προσλάβουν ειδικούς ή να χρησιμοποιήσουν εργαλεία για να δουν τι δεδομένα τους υπάρχουν δημόσια. Για παράδειγμα, μπορεί να διαπιστωθεί ότι κάποιο αρχείο ευαίσθητο βρίσκεται στο Google Index και να ζητηθεί η απόσυρσή του, ή ότι προσωπικά δεδομένα υπαλλήλων εμφανίζονται σε απρόσμενα μέρη (π.χ. μια παρουσίαση ενός συνεδρίου με στοιχεία επικοινωνίας).

- **Κατέβασμα παλιών πληροφοριών:** Παλαιά υποδομές (π.χ. παλιός ιστότοπος, παλιό subdomain) που δεν χρησιμοποιούνται, καλό είναι να αποσύρονται ώστε να μην γίνονται στόχος ούτε πηγή πληροφορίας. Για παράδειγμα, παλιό site του 2010 μπορεί να έχει ακόμη μια σελίδα “Επικοινωνία” με ονόματα υπαλλήλων που έχουν φύγει – κι όμως οι hackers να τη χρησιμοποιήσουν για phishing προσποιούμενοι έναν από αυτούς.

Επιπλέον, **διαχείριση διαρροών δεδομένων**: Επειδή πολλές πληροφορίες OSINT προέρχονται από διαρροές (π.χ. αν διέρρευσε μια λίστα πελατών, γίνεται εργαλείο phishers), οι εταιρείες πρέπει να παρακολουθούν το dark web και τα fora για ενδείξεις ότι **δεδομένα τους έχουν διαρρεύσει**. Υπάρχουν υπηρεσίες threat intelligence που ειδοποιούν “τα emails της εταιρείας σας εμφανίστηκαν σε νέα διαρροή”. Έτσι μπορούν να λαμβάνονται άμεσα μέτρα (reset passwords, ενημέρωση χρηστών να προσέχουν στοχευμένα phishing που θα ακολουθήσουν).

Στο ατομικό επίπεδο, η **εκπαίδευση των χρηστών** περιλαμβάνει και πτυχές “ψηφιακής ιδιωτικότητας”: να εκπαιδεύεται το προσωπικό να προσέχει τι μοιράζεται δημόσια (είτε έχει σχέση με τη δουλειά είτε προσωπικά). Π.χ. ένας υπάλληλος που ποστάρει στο LinkedIn “Πω πω, δούλευα όλο το Σαββατοκύριακο για το project X, είμαι κομμάτια” μπορεί άθελά του να ενημερώνει πιθανούς δράστες για εσωτερικό έργο και την κούρασή του – ιδανικό timing να του στείλει κάποιος ένα phishing Δευτέρα πρωί, όταν δεν είναι σε εγρήγορση.

6.3 Τεχνικά Μέτρα Προστασίας

Παράλληλα με τον ανθρώπινο παράγοντα, τα τεχνικά μέτρα ασφαλείας μπορούν να μειώσουν σημαντικά την πιθανότητα επιτυχίας ή το εύρος ζημιάς μιας κοινωνικής μηχανικής επίθεσης:

- **Πολυπαραγοντικός Έλεγχος Ταυτότητας (MFA):** Η χρήση MFA σε όλες τις κρίσιμες προσβάσεις (email, VPN, χρηματοοικονομικά συστήματα) κάνει δυσκολότερο για έναν δράστη που απέσπασε κωδικό να τον αξιοποιήσει.

Ωστόσο, όπως φάνηκε και στο Twitter hack, δεν επαρκεί οποιαδήποτε μορφή MFA: οι εταιρείες πρέπει να υιοθετούν **ισχυρές μορφές MFA**, όπως φυσικά κλειδιά ασφαλείας (U2F) ή τουλάχιστον εφαρμογές OTP, ώστε να μη μπορούν να παρακαμφθούν εύκολα μέσω social engineering.

- **Περιορισμός Πρόσβασης & Δικαιωμάτων:** Εφαρμογή της αρχής του ελάχιστου προνομίου (least privilege). Έτσι, ακόμα κι αν ένας υπάλληλος εξαπατηθεί και δώσει τα στοιχεία του, οι δράστες να μη μπορούν να κάνουν πολλά αν αυτός ο λογαριασμός έχει περιορισμένα δικαιώματα. Στο Twitter hack, ο πρώτος συμβιβασμένος λογαριασμός δεν είχε πρόσβαση στα εσωτερικά εργαλεία, γεγονός που περιόρισε αρχικά τους δράστες. Η καθυστέρηση αυτή έδωσε ευκαιρία σε μερικούς υπαλλήλους να αναφέρουν ύποπτες κλήσεις, αν και τελικά δεν απέτρεψε την κλιμάκωση. Αυτό δείχνει ότι **segmentation δικαιωμάτων** μπορεί να περιορίσει ζημιές.
- **Email Security Filters:** Η χρήση προηγμένων φίλτρων για phishing (SEG – Secure Email Gateway, ή και AI-based detection) μπορεί να μπλοκάρει ένα ποσοστό κακόβουλων μηνυμάτων προτού φτάσουν στους χρήστες. Αν και οι πολύ στοχευμένες επιθέσεις ενίοτε περνούν (λόγω craft επιμέλειας), τα φίλτρα κόβουν την “μαζική” εκστρατεία phishing, μειώνοντας την έκθεση.

  Anti-impersonation Controls: Υπάρχουν ρυθμίσεις όπως DMARC, SPF, DKIM για τα domain names που δυσκολεύουν τους επιτιθέμενους να στείλουν email προσποιούμενοι ένα εταιρικό domain (θα πάνε στα spam). Επίσης, ορισμένα εργαλεία μπορούν να επισημαίνουν αν ένα εισερχόμενο email προέρχεται από εξωτερικό αποστολέα, ακόμα κι αν το όνομα εμφανίζεται ίδιο με κάποιου εσωτερικού (π.χ. [EXTERNAL] tag στη θεματική γραμμή).
- **Web Proxies & DNS filters:** Μπορούν να αποτρέψουν εργαζόμενους από το να επισκεφθούν γνωστά phishing sites ή να κατεβάσουν κακόβουλα αρχεία, ακόμη κι αν αυτοί κλικάρουν το σύνδεσμο. Η δυναμική ενημέρωση τέτοιων συστημάτων (Threat intelligence feeds) είναι κρίσιμη, γιατί τα phishing sites συχνά εμφανίζονται και εξαφανίζονται μέσα σε ώρες.
- **Monitoring & Anomaly Detection:** Ένας οργανισμός με καλό σύστημα παρακολούθησης μπορεί να **εντοπίσει ασυνήθιστη δραστηριότητα** που ίσως

υποδηλώνει επιτυχή social engineering. Για παράδειγμα, αν ένας υπάλληλος που ποτέ δεν έχει κάνει μεγάλες μεταφορές ξαφνικά ζητά μεταφορά €100k, το σύστημα να σημάνει συναγερμό. Ή ένα SIEM μπορεί να δει ότι ένας λογαριασμός έκανε login από μια νέα χώρα και μετά ξεκίνησε μαζική λήψη δεδομένων – ένδειξη ότι ίσως τα διαπιστευτήρια έχουν παραβιαστεί.

- **Incident Response Plan:** Παρά τις καλύτερες προσπάθειες, πρέπει να υπάρχει σχέδιο για

  το *όταν* συμβεί περιστατικό. Δηλαδή: άμεσο κλείδωμα λογαριασμών αν υπάρξει υποψία παραβίασης, ενημέρωση ομάδας διαχείρισης κρίσεων, εφεδρικές επικοινωνίες αν οι κύριες έχουν παραβιαστεί (π.χ. εναλλακτικά κανάλια να ενημερωθούν οι πελάτες σε περίπτωση που οι δράστες πάρουν τον έλεγχο των social media της εταιρείας όπως στο Twitter hack).

6.4 Πολιτικές, Διαδικασίες και Κανονισμοί

Η τεχνολογία και η εκπαίδευση πρέπει να υποστηρίζονται από σαφείς πολιτικές ασφαλείας εντός του οργανισμού:

- **Επαλήθευση Δυσανθρώπων Αιτημάτων:** Θεσπίστε πολιτική ότι καμία χρηματοοικονομική συναλλαγή ή αποκάλυψη κρίσιμων δεδομένων δεν γίνεται απλά με ένα email. Πρέπει να υπάρχει δεύτερος παράγοντας επιβεβαίωσης (π.χ. τηλεφωνική ή δια ζώσης επιβεβαίωση με τον αιτούντα). Αυτό έχει αποδειχθεί αποτελεσματικό σε αποτροπή BEC – πολλές εταιρείες σώθηκαν επειδή ο υπάλληλος τηλεφώνησε στον αφεντικό του για να επιβεβαιώσει μια περίεργη εντολή και αποδείχθηκε απάτη.
- **Διαχωρισμός Καθηκόντων:** Ιδιαίτερα για κρίσιμες ενέργειες (μεταφορές χρημάτων, έγκριση πρόσβασης), να απαιτείται τουλάχιστον δύο άτομα να συμφωνήσουν. Έτσι μια κοινωνική μηχανική πρέπει να παραπλανήσει δύο ανθρώπους παρά έναν, αυξάνοντας τη δυσκολία.
- **Κατευθυντήριες γραμμές για απομακρυσμένη εργασία:** Π.χ. πολιτική ότι το IT ποτέ δεν θα ζητήσει κωδικό μέσω τηλεφώνου, ή ότι οι εργαζόμενοι δεν πρέπει

να αποκαλύπτουν διαπιστευτήρια μέσω email. Αυτά πρέπει να επικοινωνούνται συχνά.

- **Διαχείριση Ανθρώπινου Δυναμικού:** Όταν ένας υπάλληλος αποχωρεί, αμέσως να αφαιρούνται τα στοιχεία του από δημόσιες πηγές και να απενεργοποιούνται οι λογαριασμοί. Οι επιτιθέμενοι αγαπούν να υποδύονται πρώην υπαλλήλους ("ήμουν στην ομάδα μέχρι πρόσφατα και έχασα πρόσβαση, βοηθήστε με με Χ…"). Πρόσφατα αποχωρήσαντες μπορεί και οι ίδιοι να αποτελέσουν στόχο κοινωνικής μηχανικής (π.χ. να τους ζητηθεί από "το νέο τους αφεντικό" να δώσουν παλιούς φακέλους).
- **Κανονιστική Συμμόρφωση:** Αν και οι κανονισμοί (GDPR, ISO 27001, NIST κ.ά.) σπάνια αναφέρουν ρητά την "κοινωνική μηχανική", εντούτοις καλύπτουν τις απαιτήσεις που σχετίζονται: εκπαίδευση προσωπικού, έλεγχοι πρόσβασης, διαχείριση περιστατικών. Η συμμόρφωση με αυτά τα πλαίσια βοηθά έμμεσα στην θωράκιση έναντι κοινωνικής μηχανικής. Για παράδειγμα, το πρότυπο **ISO 27001:2013** απαιτεί επίσημα προγράμματα awareness – συμμορφούμενος κανείς, στην ουσία υλοποιεί το 6.1.
- **Oversight και Έλεγχοι:** Ορισμένοι κλάδοι έχουν αρχίσει να απαιτούν περισσότερα. Η έκθεση του NYDFS πρότεινε **ρυθμιστική εποπτεία των social media εταιρειών** αντίστοιχη με των τραπεζών, λόγω του κινδύνου που συνιστούν επιθέσεις σαν του Twitter. Στο μέλλον, δεν αποκλείεται να δούμε νόμους που να υποχρεώνουν τις εταιρείες να λαμβάνουν συγκεκριμένα μέτρα κατά του phishing, ή να εκπαιδεύουν υποχρεωτικά το προσωπικό τους σε τακτά χρονικά διαστήματα.

Τέλος, αξίζει να σημειωθεί η σημασία της **συνεργασίας και ανταλλαγής πληροφοριών** στον κλάδο. Επειδή οι επιθέσεις κοινωνικής μηχανικής τείνουν να επαναλαμβάνονται σε μοτίβα (π.χ. ίδια phishing emails σε πολλούς οργανισμούς), το να υπάρχει ένας μηχανισμός προειδοποίησης (είτε CERT ανά κλάδο, είτε απλή επικοινωνία μεταξύ εταιρειών) βοηθά. Για παράδειγμα, μια τράπεζα αν δει ένα κύμα επιθέσεων vishing σε πελάτες, ενημερώνει αμέσως και τις υπόλοιπες να έχουν το νου τους. Η ανάπτυξη

κουλτούρας *“security community”* λειτουργεί ως δύναμη πολλαπλασιαστική στην άμυνα έναντι αυτών των ευέλικτων και ανθρωποκεντρικών απειλών.

7. Μελέτη Περίπτωσης: Η Παραβίαση του Twitter το 2020 μέσω Social Engineering

Το **περιστατικό παραβίασης του Twitter τον Ιούλιο 2020** αποτελεί ένα από τα πιο προβεβλημένα παραδείγματα επιτυχημένης επίθεσης κοινωνικής μηχανικής με αξιοποίηση OSINT. Οι δράστες – μια ομάδα νεαρών hackers – κατάφεραν να αποκτήσουν πρόσβαση στα εσωτερικά εργαλεία διαχείρισης του Twitter, επιτρέποντάς τους να ελέγξουν δεκάδες διάσημους λογαριασμούς (μεταξύ των οποίων των Elon Musk, Jeff Bezos, Barack Obama, Apple, κ.ά.) και να αναρτήσουν απατηλά μηνύματα που ζητούσαν από τους ακόλουθους να στείλουν Bitcoin. Μέσα σε λίγες ώρες, είχαν εξαπατήσει χρήματα από χιλιάδες χρήστες, προτού η απάτη εντοπιστεί και το Twitter απενεργοποιήσει προσωρινά όλους τους επιβεβαιωμένους λογαριασμούς για να ανακτήσει τον έλεγχο. Η επίθεση ανέδειξε με εκκωφαντικό τρόπο την ισχύ της κοινωνικής μηχανικής: δεν χρησιμοποιήθηκε κάποιο περίπλοκο malware ή exploit λογισμικού – οι hackers *χειραγώγησαν ανθρώπους* για να εισβάλουν σε ένα από τα μεγαλύτερα social media του κόσμου.

7.1 Ιστορικό και Στόχοι των Επιτιθέμενων

Το Twitter, ως πλατφόρμα κοινωνικής δικτύωσης με εκατοντάδες εκατομμύρια χρήστες, είχε αναπτύξει εσωτερικά εργαλεία για τη διαχείριση λογαριασμών (account administration). Αυτά τα εργαλεία επιτρέπουν σε εξουσιοδοτημένους υπαλλήλους να αλλάζουν ρυθμίσεις λογαριασμών, να επαναφέρουν email, να ενεργοποιούν/απενεργοποιούν τον έλεγχο ταυτότητας δύο παραγόντων (MFA), κλπ. Προφανώς, η πρόσβαση σε αυτά τα εργαλεία είναι εξαιρετικά ευαίσθητη, διότι δίνει τη

δυνατότητα ανάληψης οποιουδήποτε λογαριασμού στην πλατφόρμα. Οι επιτιθέμενοι στοχοποίησαν ακριβώς αυτή την εσωτερική πρόσβαση.

Κίνητρο των δραστών φαίνεται πως ήταν αρχικά οικονομικό (το Bitcoin scam), αλλά ενδεχομένως και η φήμη/πρόκληση του να χακάρουν μεγάλους λογαριασμούς (μερικοί λογαριασμοί "OG" με μικρά username επίσης κλάπηκαν απλώς για επίδειξη). Η επίθεση εξελίχθηκε σε τρεις φάσεις

1. **Εισβολή στο εσωτερικό δίκτυο του Twitter** μέσω κοινωνικής μηχανικής (social engineering) – φάση κατά την οποία απέκτησαν διαπιστευτήρια υπαλλήλων.
2. **Κατάληψη λεγόμενων "OG" λογαριασμών** (αυτοί είναι παλαιοί λογαριασμοί με πολύ σύντομα ονόματα χρήστη, που έχουν μεγάλη αξία στην underground κοινότητα). Αυτή η φάση κράτησε λίγες ώρες και οι δράστες πούλησαν ή διαφήμισαν την πρόσβαση σε μερικούς.
3. **Μαζική επίθεση στους επιβεβαιωμένους (verified) λογαριασμούς** και ανάρτηση του μηνύματος απάτης για Bitcoin.

Κεντρικός στόχος λοιπόν ήταν το *πρώτο βήμα*: η είσοδος στα πληροφοριακά συστήματα του Twitter. Για να το πετύχουν, οι δράστες χρειάζονταν στοιχεία σύνδεσης υπαλλήλων με δικαιώματα πρόσβασης. Κι εδώ μπαίνει σε εφαρμογή η **κοινωνική μηχανική με χρήση OSINT**.

7.2 Μέθοδοι Επίθεσης και Χρήση OSINT

Οι hackers δεν είχαν εσωτερική γνώση της υποδομής του Twitter εκ των προτέρων. Ωστόσο, αξιοποιώντας ανοικτές πηγές και λογική, συνέλεξαν κάποιες κρίσιμες πληροφορίες:

- Γνώριζαν (ενδεχομένως από δημόσιες ανακοινώσεις ή διαρροές) ότι, λόγω COVID-19, το Twitter είχε μεταβεί σχεδόν πλήρως σε καθεστώς τηλεργασίας από τον Μάρτιο 2020. Αυτό σήμαινε ότι οι υπάλληλοι συνδέονταν στα

εσωτερικά συστήματα μέσω VPN. Επίσης, είχαν σημειωθεί προβλήματα με το VPN που ίσως είχαν αναφερθεί σε τεχνικά φόρουμ ή social media.

- Γνώριζαν πιθανώς ποια λύση VPN χρησιμοποιούσε το Twitter και ότι εφαρμοζόταν πολυπαραγοντικός έλεγχος (MFA) στις συνδέσεις αυτές. Αυτές οι πληροφορίες θα μπορούσαν να είχαν εξαχθεί από αγγελίες εργασίας του Twitter (ζητούμενη εμπειρία σε συγκεκριμένο VPN λογισμικό) ή γενική πληροφόρηση στον κλάδο.
- Μέσω LinkedIn, εντόπισαν ονόματα και θέσεις προσωπικού στο τμήμα IT/helpdesk ή άλλες σχετικές θέσεις. Το footnote [53] της έκθεσης NYDFS αναφέρει ότι οι δράστες *«έκαναν έρευνα για βασικές λειτουργίες και τίτλους των υπαλλήλων του Twitter»* πιθανώς συλλέγοντας πληροφορίες από δημόσια social media και προσωπικές ιστοσελίδες. Αυτό τους επέτρεψε να καταλάβουν ποιον πρέπει να στοχεύσουν (υπαλλήλους με πρόσβαση) και πώς να παρουσιαστούν.

Με αυτά τα δεδομένα, οι δράστες έστησαν την επίθεσή τους ως εξής:

- Ξεκίνησαν τηλεφωνώντας (vishing) σε πολλαπλούς υπαλλήλους του Twitter, παριστάνοντας ότι τηλεφωνούν από το εσωτερικό help desk της εταιρείας. Επικαλέστηκαν ένα κοινό πρόβλημα: “Ζήτημα με το VPN”. Γνώριζαν ότι λόγω τηλεργασίας αυτό θα ήταν πιστευτό – πράγματι, πολλοί υπάλληλοι αντιμετώπιζαν VPN προβλήματα στην καθημερινότητά τους, όπως σημειώνει η έκθεση.
- Κατεύθυναν τον κάθε υπάλληλο σε ένα phishing website που είχαν στήσει, το οποίο ήταν ίδιο εμφανισιακά με την πραγματική σελίδα εισόδου του Twitter VPN. Η διεύθυνση του phishing site ήταν παρεμφερής (typo-squatting domain).
- Όταν ο ανυποψίαστος υπάλληλος πληκτρολογούσε τα στοιχεία του στον ψεύτικο ιστότοπο, οι δράστες τα εισήγαγαν σε πραγματικό χρόνο στη νόμιμη σελίδα. Αυτό πυροδότησε την αποστολή push ειδοποίησης MFA στο κινητό του υπαλλήλου (εφόσον το

  Twitter χρησιμοποιούσε app-based MFA).

- Οι δράστες, όντας ακόμη σε τηλεφωνική γραμμή με τον υπάλληλο, τον καθυσήχασαν/παρότρυναν να αποδεχτεί την MFA ειδοποίηση στο κινητό του, πιθανότατα λέγοντας κάτι όπως «επειδή κάνουμε reset, θα λάβεις έναν κωδικό, πάτα ναι για να λυθεί το πρόβλημα». Σε τουλάχιστον μία περίπτωση, ο υπάλληλος πράγματι πάτησε αποδοχή, δίνοντας έτσι πρόσβαση στους εισβολείς.

Εδώ βλέπουμε το συνδυασμό: OSINT γνώση (καθεστώς VPN + ονόματα) + social engineering (vishing + phishing site). Οι δράστες *δεν θα μπορούσαν να είχαν πείσει* χωρίς να ξέρουν το context του στόχου:

- Αν έλεγαν κάτι άσχετο, ο υπάλληλος θα το καταλάβαινε. Είπαν όμως “είμαστε από IT, σε καλούμε για το VPN πρόβλημα” – μια απόλυτα λογικοφανή ιστορία στο περιβάλλον τηλεργασίας.
- Αν δεν είχαν αντιγραφή την ακριβή σελίδα VPN, ο υπάλληλος ίσως αμφέβαλλε. Η προσοχή στη λεπτομέρεια έκανε το ψεύτικο site να φαίνεται γνήσιο.
- Αν δεν ήξεραν τα ονόματα/τίτλους, δεν θα έφταναν καν στους σωστούς ανθρώπους. Προφανώς στόχευσαν υπαλλήλους που να έχουν τουλάχιστον κάποιου είδους πρόσβαση στο εσωτερικό δίκτυο.

Με αυτό τον τρόπο, απέκτησαν τα διαπιστευτήρια αρκετών υπαλλήλων. Σύμφωνα με την έρευνα,

ο πρώτος συμβιβασμένος λογαριασμός ανήκε σε υπάλληλο που δεν είχε άμεσα πρόσβαση στα ευαίσθητα εργαλεία. Ωστόσο, οι δράστες χρησιμοποίησαν αυτόν τον λογαριασμό σαν ορμητήριο: περιηγήθηκαν στο εσωτερικό δίκτυο του Twitter (Intranet) και βρήκαν έγγραφα/σελίδες που περιέγραφαν πώς να αποκτήσει κανείς πρόσβαση σε άλλα συστήματα. Δηλαδή, ουσιαστικά διάβασαν το *manual* της εταιρείας που έλεγε ποιες ομάδες έχουν πρόσβαση πού και πώς γίνεται η διαδικασία. Αυτή η πληροφορία τους βοήθησε να στοχεύσουν στη συνέχεια συγκεκριμένους υπαλλήλους που είχαν τα κατάλληλα δικαιώματα για τα εργαλεία account admin.

Τη δεύτερη ημέρα, 15 Ιουλίου 2020, οι δράστες εστίασαν στους εν λόγω υπαλλήλους-κλειδιά. Κάλεσαν μερικούς από αυτούς με τον ίδιο τρόπο. Οι πληροφορίες που είχαν πλέον – τόσο από OSINT όσο και από την εσωτερική αναγνώριση της προηγούμενης ημέρας – τους έκαναν ακόμα πιο πειστικούς. Οι συνομιλίες τους πιθανώς εμπλουτίστηκαν με *"εσωτερικούς όρους"* που έμαθαν από το intranet, κάνοντάς τους να ακούγονται ακριβώς όπως ένα γνήσιο μέλος του IT του Twitter. Με αυτές τις κλήσεις, κατάφεραν να εξαπατήσουν τουλάχιστον έναν υπάλληλο με διοικητική πρόσβαση στα εργαλεία διαχείρισης λογαριασμών.

Μόλις είχαν αυτά τα credentials, μπόρεσαν να συνδεθούν στα εσωτερικά εργαλεία. Από εκεί, το μονοπάτι ήταν ανοιχτό: άρχισαν να πάρουν τον έλεγχο λογαριασμών. Αρχικά, όπως αναφέρθηκε, έβαλαν στόχο "OG" usernames (π.χ. @6, @VIP, κ.λπ.) τα οποία στην underground αγορά πωλούνται ακριβά. Μετέπειτα, προχώρησαν στο κύριο σχέδιο: υπέκλεψαν λογαριασμούς γνωστών προσώπων και εταιρειών (οι οποίοι ήταν verified, δηλ. με το μπλε τικ) και δημοσίευσαν tweets που καλούσαν τον κόσμο να στείλει Bitcoin σε ένα πορτοφόλι, με την υπόσχεση ότι θα τους επιστραφεί το διπλάσιο ποσό – κλασική απάτη giveaway. Μέσα σε λίγες ώρες, χάρη στην πειστικότητα (οι αναρτήσεις προέρχονταν από επίσημους λογαριασμούς), συγκέντρωσαν Bitcoins αξίας περίπου $118.000.

Είναι αξιοσημείωτο ότι κατά τη διάρκεια της τρίτης φάσης, οι επιτιθέμενοι κατόρθωσαν επίσης να χρησιμοποιήσουν τις παραβιασμένες προσβάσεις για να κατεβάσουν τα λεγόμενα "Your Twitter Data" αρχεία για ορισμένους στόχους (7 λογαριασμοί), τα οποία περιέχουν όλο το ιστορικό του λογαριασμού (DMs, media, κλπ). Αυτό δείχνει ότι είχαν πλήρη δικαιώματα ελέγχου λογαριασμών και ίσως στόχευαν να αποκομίσουν και πληροφορίες πέραν του άμεσου χρηματικού οφέλους.

Όλη η επίθεση συνέβη μέσα σε 24 ώρες. Το Twitter αντέδρασε κατόπιν εορτής απενεργοποιώντας προσωρινά τη δυνατότητα όλων των verified accounts να αναρτούν tweets, ενώ ξεκίνησε έρευνα.

ζημιά σε χρήστες ήταν σχετικά περιορισμένη (από οικονομική άποψη, $118k δεν είναι τεράστιο ποσό για το εύρος του Twitter). Όμως, η ζημιά στην αξιοπιστία του Twitter

ήταν σημαντική, καθώς φάνηκε πόσο ευάλωτη ήταν η πλατφόρμα. Επίσης, εγέρθηκαν σοβαρές ανησυχίες για το τί θα μπορούσαν να είχαν κάνει πιο κακόβουλοι παράγοντες: οι λογαριασμοί πολιτικών και επιχειρήσεων θα μπορούσαν να χρησιμοποιηθούν για διάδοση ψευδών ειδήσεων, χρηματιστηριακή χειραγώγηση, ακόμη και πρόκληση γεωπολιτικών εντάσεων.

7.3 Αποτελέσματα και Διδάγματα

Η ανάλυση του περιστατικού, κυρίως από την έρευνα του Τμήματος Οικονομικών Υπηρεσιών της Νέας Υόρκης (NYDFS), κατέδειξε πολλά σημαντικά σημεία:

- **Η απλότητα και αποτελεσματικότητα της κοινωνικής μηχανικής:** Οι δράστες «χάκαραν» το Twitter χωρίς να αγγίξουν κώδικα ή συστήματα ασφαλείας. *Εκμεταλλεύτηκαν τον άνθρωπο*. Όπως αναφέρει η έκθεση, “the Hackers relied on a simple tactic: social engineering... one-third of incidents reported in that period involved phishing or vishing”. Καμία εταιρεία, όσο τεχνολογικά προηγμένη, δεν είναι ασφαλής εάν το προσωπικό της δεν είναι προετοιμασμένο να αντιμετωπίσει τέτοιες επιθέσεις.
- **OSINT και προετοιμασία:** Το γεγονός ότι οι δράστες γνώριζαν για τα προβλήματα VPN, τους τίτλους υπαλλήλων, κ.ο.κ., δείχνει ότι έκαναν κατ’ ελάχιστον μια δομημένη συλλογή ανοικτών πληροφοριών πριν δράσουν. Αυτό τους έδωσε μεγάλη αξιοπιστία στα μάτια των θυμάτων. Δίδαγμα: Οι εταιρείες πρέπει να περιορίσουν τί πληροφορίες διαρρέουν προς τα έξω για την εσωτερική τους λειτουργία και να υποθέτουν ότι οι επιτιθέμενοι γνωρίζουν ή μπορούν να μάθουν πολλά για αυτές.
- **Σφάλματα του Twitter:** Μετά την επίθεση, αποκαλύφθηκε ότι το Twitter δεν είχε εφαρμόσει κάποιες βασικές αρχές:
    - Δεν διέθετε καθολικό μηχανισμό ειδοποίησης αν ένας λογαριασμός διαχειριστή έκανε ασυνήθιστες ενέργειες (π.χ. να πάρει πολλούς λογαριασμούς σε λίγο χρόνο).

- Η μετάβαση στο remote work δεν συνοδεύτηκε από πρόσθετα μέτρα ασφαλείας. Όπως αναφέρει η έκθεση, παρά τις προειδοποιήσεις (π.χ. από το FBI και το ίδιο το

  NYDFS) λόγω πανδημίας, το Twitter *«δεν υλοποίησε σημαντικούς αντισταθμιστικούς ελέγχους μετά τον Μάρτιο 2020 για να μετριάσει τον αυξημένο*

  κίνδυνο για το απομακρυσμένο προσωπικό του». Αυτό ήταν ένα κενό που οι δράστες εκμεταλλεύτηκαν.

- Η χρήση application-based MFA αντί για hardware keys ήταν ένα αδύναμο σημείο. Ένα φυσικό κλειδί πιθανότατα θα είχε σταματήσει την επίθεση, διότι δεν μπορεί να "αποσπαστεί" μέσω τηλεφώνου όπως μια push ειδοποίηση. Μετά την επίθεση, το Twitter ανακοίνωσε ότι στρέφεται σε χρήση security keys για τους διαχειριστές
  του.

- Η εκπαίδευση του προσωπικού αποδείχθηκε ανεπαρκής στο να σταματήσει έγκαιρα την απάτη, αν και κάποιοι υπάλληλοι ανέφεραν όντως ύποπτες κλήσεις (δυστυχώς όχι αρκετά γρήγορα). Αυτό τονίζει πως χρειάζεται συνεχής ενίσχυση της εγρήγορσης και πρακτική εξάσκηση μέσω δοκιμών, ειδικά όταν αλλάζουν οι συνθήκες εργασίας.

- **Αντίμετρα και βέλτιστες πρακτικές:** Το NYDFS στη συνέχεια δημοσίευσε βέλτιστες πρακτικές, όπως:
  1. Εκτενής εκπαίδευση για social engineering με έμφαση στη νέα πραγματικότητα της τηλεργασίας (το «νέο φυσιολογικό» όπως το αποκάλεσαν).
  2. Πρότυπα επικοινωνίας: ενημέρωση των υπαλλήλων πώς θα τους ζητούνται ποτέ πληροφορίες (π.χ. "ποτέ το IT δεν θα ζητήσει τον κωδικό σου").
  3. Άσκηση phishing/vishing tests τακτικά για τον έλεγχο ετοιμότητας.
  4. Προωθημένη παρακολούθηση (monitoring): ώστε αν συμβεί κάτι, να ανιχνευτεί άμεσα και να σταματήσει. Στην περίπτωση του Twitter, ένα

σύστημα SIEM θα μπορούσε να είχε δει ότι ξαφνικά έγιναν πολλές αλλαγές email σε λογαριασμούς

5. VIP, κάτι ανήκουστο σε κανονικές συνθήκες, και να σημάνει συναγερμό.

   Αυστηροποίηση προσβάσεων: π.χ. κάποιοι πρότειναν το Twitter να υιοθετήσει "IP allowlisting" για διαχειριστικές προσβάσεις – δηλαδή μόνο εταιρικές διευθύνσεις IP να μπορούν να τις χρησιμοποιούν, ώστε αν κάποιος συνδεθεί από οικιακό internet (όπως έγινε εδώ) να μπλοκαριστεί.

Συμπέρασμα της μελέτης περίπτωσης: Το hack του Twitter 2020 αποτέλεσε "μάθημα" για όλο τον κλάδο. Επιβεβαίωσε ότι

1. η κοινωνική μηχανική με OSINT μπορεί να διαπεράσει ακόμη και εταιρείες-γίγαντες τεχνολογίας,
2. τα βασικά προληπτικά μέτρα (MFA, training, monitoring) πρέπει να εφαρμόζονται σωστά και να προσαρμόζονται στις συνθήκες (π.χ. remote), και
3. σε επίπεδο macro, απαιτείται μια προσέγγιση all-hazard: όλοι οι οργανισμοί, όχι μόνο οι τράπεζες, έχουν πλέον στον πυρήνα του κινδύνου τους τον ανθρώπινο παράγοντα.

Συμπεράσματα

Η παρούσα εργασία ανέδειξε τις πολύπλευρες διαστάσεις των τεχνικών OSINT σε επιθέσεις κοινωνικής μηχανικής και τις συνέπειές τους, καθώς και τις άμυνες που μπορούν να αναπτυχθούν. Στα κύρια σημεία που εξετάστηκαν περιλαμβάνονται:

- **Η φύση της κοινωνικής μηχανικής:** Ένας εξελισσόμενος κίνδυνος που εκμεταλλεύεται ανθρώπινες αδυναμίες και χρησιμοποιεί την παραπληροφόρηση και την ψυχολογική επιρροή ως "όπλα" αντί για κακόβουλο κώδικα. Διαπιστώθηκε ότι η πλειονότητα των κυβερνοεπιθέσεων σήμερα εμπεριέχει ένα στοιχείο κοινωνικής μηχανικής ή ανθρώπινου λάθους, γεγονός

που καταδεικνύει πόσο κρίσιμο είναι να εστιάσουμε στην ανθρωποκεντρική ασφάλεια.

- **Ο ρόλος του OSINT:** Η πληθώρα δημοσίων δεδομένων προσφέρει στους επιτιθέμενους ένα πλεονέκτημα χωρίς προηγούμενο. Πλέον, ακόμα και ένας μεμονωμένος hacker μπορεί να συγκεντρώσει πληροφορίες για έναν στόχο σε βάθος που παλαιότερα θα απαιτούσε ομάδες κατασκόπων. Από την άλλη πλευρά, οι ίδιες αυτές τεχνικές OSINT αποτελούν και εργαλείο των αμυνόμενων για αναγνώριση απειλών και αυτοαξιολόγηση της έκθεσής τους. Η ισορροπία μεταξύ ανοιχτής πληροφορίας και ιδιωτικότητας/ασφάλειας είναι λεπτή και απαιτεί συνεχή διαχείριση.
- **Επιπτώσεις και περιστατικά:** Είδαμε πώς πραγματικά περιστατικά – από οικονομικές απάτες (BEC) έως επιθέσεις σε υποδομές (ransomware) και πλατφόρμες κοινωνικών μέσων – μπορούν να προκληθούν ή να διευκολυνθούν από κοινωνική μηχανική που αξιοποιεί OSINT. Τα κόστη είναι τεράστια όχι μόνο χρηματικά αλλά και σε επίπεδο φήμης, εμπιστοσύνης κοινού και εθνικής ασφάλειας. Ειδικά η περίπτωση του Twitter το 2020 έδειξε ότι ακόμα και οι "τεχνολογικοί κολοσσοί" είναι τρωτοί, εντείνοντας τις φωνές για αυστηρότερη κυβερνορυθμίση και λογοδοσία.
- **Μέτρα αντιμετώπισης:** Η προσέγγιση άμυνας πρέπει να είναι ολιστική. **Οι άνθρωποι**

  είναι το κέντρο: εκπαίδευση, κουλτούρα ασφαλείας, εγρήγορση. **Οι διαδικασίες** έπονται: σαφείς κανόνες, διασταυρώσεις κρίσιμων ενεργειών, πολιτικές ελέγχου πληροφορίας. Και **η τεχνολογία** υποστηρίζει: MFA, ανιχνευτικά συστήματα, φιλτράρισμα, έλεγχοι πρόσβασης. Καμία από αυτές τις πτυχές μόνη της δεν αρκεί· απαιτείται συνδυασμός. Όπως εύστοχα τονίστηκε, *«η πρώτη γραμμή άμυνας είναι η ενημέρωση όλων των εργαζομένων για τις απειλές»*, αλλά χωρίς παράλληλα τεχνικά στηρίγματα, ένας ανθρώπινος στιγμιαίος εφησυχασμός μπορεί να οδηγήσει σε breach.

Σε μια προοπτική προς το μέλλον, καθώς οι τεχνολογίες εξελίσσονται, αναδύονται και νέες μορφές απειλών κοινωνικής μηχανικής – π.χ. deepfakes φωνής/εικόνας που

μπορούν να κάνουν μια απάτη ακόμα πιο πειστική ή η χρήση AI chatbots από επιτιθέμενους για να εξαπατούν θύματα με αυτοματοποιημένες συνομιλίες. Παράλληλα, όμως, και η άμυνα εξοπλίζεται με AI για ανίχνευση ανωμαλιών συμπεριφοράς, προηγμένα προγράμματα εκπαίδευσης με προσομοιώσεις κ.ά. Η “κούρσα εξοπλισμών” στον τομέα αυτό είναι σε πλήρη εξέλιξη.

Το σίγουρο είναι ότι η *επίγνωση* παραμένει θεμέλιος λίθος: επίγνωση από πλευράς χρηστών ότι οι πληροφορίες που μοιράζονται μπορεί να αξιοποιηθούν εναντίον τους, επίγνωση από πλευράς οργανισμών των αδυναμιών τους και επίγνωση από πλευράς κοινωνίας ότι η εμπιστοσύνη στο ψηφιακό οικοσύστημα εξαρτάται και από την ανθρωπινή συμπεριφορά. Τελικά, επαληθεύεται η ρήση πως "η ασφάλεια είναι τόσο ισχυρή όσο ο πιο αδύναμος κρίκος της", και στις σύγχρονες επιχειρήσεις αυτός ο κρίκος είναι συχνά ο άνθρωπος. Η επένδυση στην ενδυνάμωση αυτού του κρίκου – μέσω γνώσης, εργαλείων και κουλτούρας – αποτελεί μονόδρομο για την μείωση των ρηγμάτων ασφαλείας στο παρόν και το μέλλον.

Βιβλιογραφία

Adu-Manu, K. S., Ahiable, R. K., Appati, J. K., & Mensah, E. E. (2022). Phishing Attacks in Social Engineering: A review. *Journal of Cyber Security*, *4*(4), 239–267. https://doi.org/10.32604/jcs.2023.041095

Alabdulatif, A., & Thilakarathne, N. N. (2025). Hacking exposed: leveraging Google Dorks, Shodan, and Censys for cyber attacks and the defense against them. *Computers*, *14*(1), 24. https://doi.org/10.3390/computers14010024

Allodi, L., Chotza, T., Panina, E., & Zannone, N. (2019). The need for new antiphishing measures against Spear-Phishing attacks. *IEEE Security & Privacy*, *18*(2), 23–34. https://doi.org/10.1109/msec.2019.2940952

Al-Musib, N. S., Al-Serhani, F. M., Humayun, M., & Jhanjhi, N. (2021). Business email compromise (BEC) attacks. *Materials Today Proceedings*, *81*, 497–503. https://doi.org/10.1016/j.matpr.2021.03.647

BBC News. (2021, April 14). *Facebook faces investigation over data breach*. https://www.bbc.com/news/technology-56745734

Bonnie, E. (2024, December 31). 60+ Social Engineering Statistics [Updated 2025]. *Secureframe*. https://secureframe.com/blog/social-engineering-statistics

Brown, M. B., Townsend, J. T., & Baird, L. B. (2016). The Harvester. In *GitHub*.

Burns, A. J., Johnson, M. E., & Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 24–39. https://doi.org/10.1080/10919392.2019.1552745

Cascavilla, G., Beato, F., Burattin, A., Conti, M., & Mancini, L. V. (2016). OSSINT - Open Source Social Network Intelligence An efficient and effective way to uncover “private” information in OSN profiles. *arXiv (Cornell University)*.

https://doi.org/10.48550/arxiv.1611.06737

Check Point Research. (2025, June 25). *CPR - Check point research*.

https://research.checkpoint.com/

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. *Procedia Computer Science*, *198*, 656–661. https://doi.org/10.1016/j.procs.2021.12.302

Cieply, M. C., & Barnes, B. B. (2014, December 30). Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm. *New York Times*. https://www.ny-times.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html

Cost of a data breach 2024 | IBM. (2024). https://www.ibm.com/reports/data-breach *COVID-19 exploited by malicious cyber actors*. (2020, April 8). CISA. Retrieved June 25, 2025, from https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-099a

Federal Bureau of Investigation. (2020). FBI alert: Enhanced threat of cyber fraud tied to COVID-19. In *Cybersecurity & Data Privacy* (pp. 1–3).

Grimes, R. A., & Just, Dr. J. N. (2024). *Fighting phishing*. John Wiley & Sons, Inc. Hadnagy, C. (2018). *Social engineering*. https://doi.org/10.1002/9781119433729 Heiding, F., Lermen, S., Kao, A., Schneier, B., & Vishwanath, A. (2024). Evaluating large language models' capability to launch fully automated spear phishing campaigns: validated on human subjects. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2412.00586

Implementing Phishing-Resistant MFA. (2022). In *CISA | DEFEND TODAY, SECURE TOMORROW*. https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

Kesan, J. P., & Hayes, C. M. (2017). Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2924854

Krebs on security. (2025, June 12). Retrieved June 25, 2025, from https://krebsonsecurity.com/

Kushwaha, A., Singh, P., & Waoo, A. A. (2024). REVIEW ON SOCIAL ENGINEERING ATTACKS AND DEFENSE MECHANISMS. *ShodhKosh Journal of Visual and Performing Arts*, *5*(5). https://doi.org/10.29121/shodhkosh.v5.i5.2024.1887

Lalit, R. L., Bhutani, P. B., Verma, N. V., & Marwah, S. M. (2023). Social engineering as a tool for Cyber-Attacks. *Acta Scientific COMPUTER SCIENCES*, *5*(9), 33–37. https://actascientific.com/ASCS/pdf/ASCS-05-0476.pdf

Maltego. (2023, September 12). *How to Conduct Operational Threat Intelligence Research with OSINT*. How to Conduct Operational Threat Intelligence Research With OSINT. Retrieved June 25, 2025, from https://www.maltego.com/blog/how-to-conduct-operational-threat-intelligence-research-with-osint/?utm_source

Mehta, A., Vora, D., Sachala, H., Khatri, J., & Gada, D. (2021). A Review of Social Engineering Attacks and their Mitigation Solutions [Journal-article]. *International Journal of Engineering Research & Technology (IJERT)*, 215. https://www.ijert.org/research/a-review-of-social-engineering-attacks-and-their-mitigation-solutions-IJERTV10IS100107.pdf

Mollazehi, A., Abuelezz, I., Barhamgi, M., Khan, K. M., & Ali, R. (2024). Do Cialdini's Persuasion Principles Still Influence Trust and Risk-Taking When Social Engineering is Knowingly Possible? In *Lecture notes in business information processing* (pp. 273–288). https://doi.org/10.1007/978-3-031-59465-6_17

Naz, A., Sarwar, M., Kaleem, M., Jr, Mushtaq, M. A., Rashid, S., University of Sargodha, & University of Lahore. (2024). [A comprehensive survey on social engineering-based attacks on social networks]. In *International Journal of Advanced and*

Applied Sciences (Vol. 11, Issue 4, pp. 139–154) [Journal-article]. https://doi.org/10.21833/ijaas.2024.04.016

Nobili, M. (2023). Review OSINT tool for social engineering. *Frontiers in Big Data*, *6*. https://doi.org/10.3389/fdata.2023.1169636

Nonum, N. E. O., Avwokuruaye, N. O., & Ezemonye, N. T. M. (2025). Role of Open Source intelligence (OSINT) in cybersecurity and threat analysis. *International Journal of Latest Technology in Engineering Management & Applied Science*, *14*(3), 189–200. https://doi.org/10.51583/ijltemas.2025.140300023

Nonum, N. E. O., Avwokuruaye, N. O., & Umar, N. a. M. (2025). SOCIAL ENGINEERING: UNDERSTANDING HUMAN FACTORS IN CYBER SECURITY. *International Journal of Convergent and Informatics Science Research*. https://doi.org/10.70382/hijcisr.v07i9.032

Papathanasiou, A., Liontos, G., Liagkou, V., & Glavas, E. (2023). Business Email Compromise (BEC) Attacks: Threats, Vulnerabilities and Countermeasures—A perspective on the Greek landscape. *Journal of Cybersecurity and Privacy*, *3*(3), 610–637. https://doi.org/10.3390/jcp3030029

Rajamäki, J. (2024). *Utilization and sharing of cyber threat intelligence produced by Open-Source Intelligence - ProQuest* [Digital / Online]. Proceedings of the 19th International Conference on Cyber Warfare and Security, ICCWS 2024. https://www.proquest.com/open-view/696622469e5ea6469c7fec946373fee3/1?pq-origsite=gscholar&cbl=396500

Rajamäki, J., McMenamin, S., & Tiitta, K. (2024). The importance of Open-Source intelligence in assessing risks of cyberattacks. *Information & Security an International Journal*, *55*(1), 15–31. https://doi.org/10.11610/isij.5511

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: a survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Saundatikar, R., & Seth, D. (2020). Review on OSNIT tools & techniques. In Jain Deemed-to-be University, *International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)* (Vol. 04, Issue 02, pp. 267–268).

Schmitt, M., & Flechais, I. (2024). Digital deception: generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*(12). https://doi.org/10.1007/s10462-024-10973-2

SEC587: Advanced Open-Source Intelligence (OSINT) Gathering and Analysis | SANS Institute. (n.d.). Retrieved June 25, 2025, from https://www.sans.org/cyber-security-courses/advanced-open-source-intelligence-gathering-analysis/

Silent Librarian, TA407, COBALT DICKENS, Group G0122 | MITRE ATT&CK®. (n.d.). Retrieved June 25, 2025, from https://attack.mitre.org/groups/G0122/

Stolyarov, V. (2022, March 31). Exposing initial access broker with ties to Conti. *Google*. https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti

Szymoniak, S., & Foks, K. (2024). Open Source Intelligence Opportunities and Challenges: a Review. *Advances in Science and Technology – Research Journal*, *18*(3), 123– 139. https://doi.org/10.12913/22998624/186036

The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. (2023, May 7). CISA. Retrieved June 25, 2025, from https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

The Data Revolution: OSINT's role in the Digital Age. (2023, December 21). American University. Retrieved June 25, 2025, from https://www.american.edu/sis/centers/security-technology/the-data-revolution-osints-role-in-the-digital-age.cfm

The Human Factor 2025: Vol. 1 Social Engineering | ProofPoint US. (2025, May 29). Proofpoint. Retrieved June 25, 2025, from https://www.proofpoint.com/us/resources/threat-reports/human-factor-social-engineering

Three individuals charged for alleged roles in Twitter hack. (2020, July 31). https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack

Tundis, A., Nga, E. M. M., & Mühlhäuser, M. (2021). An exploratory analysis on the impact of Shodan scanning tool on the network attacks. *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–10. https://doi.org/10.1145/3465481.3469197

Tundis, A., Ruppert, S., & Mühlhäuser, M. (2021). A feature-driven method for automating the assessment of OSINT cyber threat sources. *Computers & Security*, *113*, 102576. https://doi.org/10.1016/j.cose.2021.102576

Twitter investigation report. (2020, July 15). Department of Financial Services. Retrieved June 25, 2025, from https://www.dfs.ny.gov/Twitter_Report

Van Puyvelde, D., & Rienzi, F. T. (2025). The rise of open-source intelligence. *European Journal of International Security*, 1–15. https://doi.org/10.1017/eis.2024.61

Xu, T., Singh, K., & Rajivan, P. (2022). Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. *Applied Ergonomics*, *108*, 103908. https://doi.org/10.1016/j.apergo.2022.103908

Yu, J., Yu, Y., Wang, X., Lin, Y., Yang, M., Qiao, Y., & Wang, F. (2024, July 22). *The Shadow of Fraud: The Emerging Danger of AI-powered Social Engineering and its Possible Cure*. arXiv.org. https://arxiv.org/abs/2407.15912

Zorz, Z. (2018, October 15). *Belgian bank Crelan loses €70 million to BEC scammers - Help Net Security*. Help Net Security. https://www.helpnetsecurity.com/2016/01/26/belgian-bank-crelan-loses-e70-million-to-bec-scammers/