Η Παγίδα της Ευγένειας

Όταν η Κοινωνική Μηχανική Ανοίγει τις Πόρτες

Nadia Liapi
Group Director
Governance, Risk & Compliance Services – SOC Services

SPACE

Classification ISO 27001: Public

www.space.gr

Η Ιστορία του "Τεχνικού Υποστήριξης"

Η Άφιξη του Άγνωστου Τεχνικού

- Ήταν ένα συνηθισμένο πρωινό στη "***DataSecure Inc.***", μια μεγάλη εταιρεία κυβερνοασφάλειας που προστάτευε δεδομένα χιλιάδων πελατών. Οι εργαζόμενοι κατέφταναν στα γραφεία τους, οι συζητήσεις γίνονταν γύρω από τον καφέ και το τμήμα IT προσπαθούσε να διαχειριστεί τα καθημερινά αιτήματα υποστήριξης.
- Στις 10:15 το πρωί, ένας άνδρας με μπλε πόλο μπλουζάκι και ένα ID badge που έγραφε **"Τεχνική Υποστήριξη – Συνεργάτης"** εμφανίστηκε στη ρεσεψιόν. Συστήθηκε ως **Μάριος Αντωνίου**, εξωτερικός τεχνικός της συνεργαζόμενης εταιρείας συντήρησης του Wi-Fi.

Η Άφιξη του Άγνωστου Τεχνικού

- Η ρεσεψιονίστ, χωρίς να έχει ενημερωθεί για προγραμματισμένη επίσκεψη, τηλεφώνησε στο IT.
  - *"Έχει έρθει ο τεχνικός για το Wi-Fi, να τον αφήσω να περάσει;"*
  - *"Wi-Fi; Δεν θυμάμαι κάποια προγραμματισμένη επίσκεψη, αλλά είχαμε αναφέρει πρόβλημα στο δίκτυο…*
  - *Άστον να περάσει, τον συνοδεύω εγώ," απάντησε ένας βιαστικός IT manager.*
- Ο **Μάριος** μπήκε στο κτίριο.

Η Καλοπροαίρετη Βοήθεια

- Ο **Μάριος** πέρασε την επόμενη ώρα περιεργαζόμενος τα δίκτυα, σημειώνοντας πληροφορίες και μιλώντας με υπαλλήλους. Ήταν φιλικός, έκανε αστεία και βοηθούσε ακόμη και σε μικροπροβλήματα με το ίντερνετ στους υπολογιστές.

- Στη διάρκεια της ημέρας, ένας εργαζόμενος του IT τον κάλεσε να ρίξει μια ματιά σε έναν server που φαινόταν να έχει θέμα με τις συνδέσεις. Ο **Μάριος** απλά χαμογέλασε, μπήκε στο δωμάτιο των servers και –χωρίς να το καταλάβει κανείς– τοποθέτησε μια μικρή USB συσκευή πίσω από μία συσκευή δικτύου. Η συσκευή αυτή παρείχε απομακρυσμένη πρόσβαση σε ευαίσθητα δεδομένα.

Η Κατάρρευση

- Μερικές ώρες αργότερα, περίεργη δραστηριότητα παρατηρήθηκε στο σύστημα. Δεδομένα πελατών άρχισαν να διαρρέουν σε περίεργους διακομιστές, οι υπάλληλοι έχασαν πρόσβαση σε αρχεία, ενώ emails με phishing links στάλθηκαν εσωτερικά εκ μέρους του CEO.
- Το IT τμήμα σήμανε συναγερμό, αλλά ήταν ήδη αργά. Οι hackers που συνεργάζονταν με τον Μάριο είχαν αποκτήσει πρόσβαση στο δίκτυο. Μία σειρά από επιθέσεις ransomware και διαρροές δεδομένων ξεκίνησαν, δημιουργώντας οικονομική και νομική καταστροφή για την εταιρεία.

Το Μεγάλο Λάθος

- Όταν ξεκίνησε η έρευνα, το μεγαλύτερο λάθος φάνηκε ξεκάθαρα: **κανείς δεν επιβεβαίωσε την ταυτότητα του "τεχνικού".** Δεν υπήρξε καμία δεύτερη επαλήθευση της επίσκεψης, και όλοι υπέθεσαν πως αν κάποιος "φαίνεται επαγγελματίας", τότε είναι αληθινός.
- Το χτύπημα κόστισε στην **DataSecure Inc.** εκατομμύρια ευρώ, αγωγές από πελάτες και ανεπανόρθωτη ζημιά στην φήμη της.

Κοινωνική Μηχανική

- Η **κοινωνική μηχανική** είναι η **εκμετάλλευση της ανθρώπινης ψυχολογίας** για να αποκτηθεί μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες, συστήματα ή φυσικούς χώρους.
- Αντί να "χακάρει" ένα σύστημα με τεχνικές μεθόδους, ένας επιτιθέμενος χρησιμοποιεί **χειραγώγηση, εξαπάτηση και ψυχολογικά κόλπα** για να κάνει κάποιον να αποκαλύψει εμπιστευτικές πληροφορίες ή να του δώσει πρόσβαση σε ασφαλείς περιοχές.

Τα Στάδια της Κοινωνικής Μηχανικής

- **Αναγνώριση (Research / Reconnaissance)**
  - Ο επιτιθέμενος συλλέγει πληροφορίες για το στόχο του (άτομα, οργανισμούς, διαδικασίες).
  - Αναζήτηση σε social media, εταιρικά sites και διαρροές δεδομένων.
  - Εντοπισμός αδύναμων σημείων (π.χ. νέοι υπάλληλοι, εξωτερικοί συνεργάτες).
- **Δημιουργία Σχέσης (Engagement / Pretexting)**
  - Ο επιτιθέμενος εμφανίζεται ως αξιόπιστο πρόσωπο (τεχνικός, προμηθευτής, ανώτερος υπάλληλος).
  - Δημιουργεί ψεύτικο σενάριο για να προκαλέσει εμπιστοσύνη.
  - Εκμεταλλεύεται την ανθρώπινη ευγένεια και την ανάγκη για βοήθεια.

Τα Στάδια της Κοινωνικής Μηχανικής

- **Εκτέλεση Επίθεσης (Exploitation / Attack)**
  - Ο επιτιθέμενος εκμεταλλεύεται την εμπιστοσύνη του θύματος.
  - Μπορεί να ζητήσει κωδικούς, να αποκτήσει πρόσβαση σε κτίρια ή να εγκαταστήσει κακόβουλο λογισμικό.
  - Χρησιμοποιεί τεχνικές όπως phishing, tailgating ή baiting.
- **Απόσπαση Δεδομένων (Extraction / Execution)**
  - Ο επιτιθέμενος συλλέγει κρίσιμες πληροφορίες ή εκτελεί κακόβουλες ενέργειες.
  - Ενδέχεται να μεταφέρει δεδομένα σε εξωτερικούς servers ή να προκαλέσει λειτουργική διαταραχή.

Τα Στάδια της Κοινωνικής Μηχανικής

- **Διαφυγή (Exit & Cover-up)**
  - Ο επιτιθέμενος αποχωρεί χωρίς να αφήσει εμφανή ίχνη.
  - Καλύπτει τις κινήσεις του ώστε να καθυστερήσει η ανίχνευση.
  - Οι οργανισμοί συχνά καταλαβαίνουν την επίθεση όταν είναι ήδη αργά.

Η κοινωνική μηχανική δεν απαιτεί πολύπλοκες τεχνικές hacking – μόνο την ανθρώπινη τάση να εμπιστευόμαστε κάποιον που φαίνεται "κανονικός"

Προστασία από την Κοινωνική Μηχανική: Μέτρα Πρόληψης & Αντίδρασης

- Γιατί είναι κρίσιμη η ασφάλεια φυσικής και ψηφιακής πρόσβασης;
- Πώς μπορούμε να αποτρέψουμε επιθέσεις σαν αυτή που είδαμε;

Έλεγχος Πρόσβασης

- Η Ασφάλεια Ξεκινά από την Πόρτα
  - Υποχρεωτικός έλεγχος ταυτότητας επισκεπτών
  - Αυστηρός έλεγχος για εργολάβους, προμηθευτές & επισκέπτες
  - Κατάλληλες πολιτικές για την πρόσβαση σε κρίσιμες υποδομές

Εκπαίδευση Προσωπικού

- Ο Ανθρώπινος Παράγοντας: Το Μεγαλύτερο Ρίσκο & Η Μεγαλύτερη Προστασία
  - Σεμινάρια για αναγνώριση τακτικών κοινωνικής μηχανικής
  - Ενθάρρυνση της καχυποψίας απέναντι σε "φιλικές" απάτες
  - Ενημέρωση ασφαλούς διαχείρισης προσωπικών και επαγγελματικών δεδομένων
  - Δοκιμές προσομοίωσης κοινωνικής μηχανικής για να εντοπιστούν αδυναμίες

Ασφάλεια Δικτύου & Συσκευών

- Η Ψηφιακή Πλευρά της Απειλής
  - Πολιτική καθαρών γραφείων (Clean Desk Policy) – δεν αφήνουμε έγγραφα εκτεθειμένα
  - Απαγόρευση χρήσης μη εγκεκριμένων USB και φορητών συσκευών
  - Τακτικές αναβαθμίσεις λογισμικού και έλεγχοι ασφαλείας
  - Χρήση ασφαλών συνδέσεων Wi-Fi και VPN για απομακρυσμένη πρόσβαση

Ανίχνευση & Αντίδραση σε Υποψίες Παραβίασης

- Όταν Κάτι Δεν Φαίνεται Σωστό, Μην το Αγνοείς
  - Πρωτόκολλα αναφοράς ύποπτων συμπεριφορών
  - Εφαρμογή συστημάτων παρακολούθησης με κάμερες ασφαλείας και καταγραφικά
  - Απομόνωση πιθανών παραβιάσεων και γρήγορη απόκριση
  - Διερεύνηση περιστατικών με βάση προκαθορισμένα πλάνα

Πολιτική Ασφάλειας & Συνεχής Αξιολόγηση

- Η Ασφάλεια είναι μία Διαρκής Διαδικασία
  - Δημιουργία και τήρηση αυστηρών πολιτικών ασφαλείας
  - Συχνές εσωτερικές και εξωτερικές αξιολογήσεις ασφάλειας
  - Διεξαγωγή δοκιμαστικών επιθέσεων (penetration testing & red teaming)
  - Καλλιέργεια κουλτούρας ασφάλειας μέσα στον οργανισμό

Η Κοινωνική Μηχανική Δεν Εξαρτάται από την Τεχνολογία – Αλλά από τους Ανθρώπους

Η Κοινωνική Μηχανική εξαρτάται από τους Ανθρώπους

- Δεν αρκεί η ύπαρξη πολιτικών, χρειάζεται **εκπαίδευση, επαγρύπνηση και προετοιμασία**
- Ένα μικρό λάθος μπορεί να οδηγήσει σε **καταστροφικές συνέπειες**
- Κάθε εργαζόμενος είναι μέρος της άμυνας – **οργανώστε την προστασία της επιχείρησης σας!**

Empowering
Your Digital Transformation Journey

Thank you!

SPACE

Classification : Confidential

www.space.gr