



Ο άνθρωπος στο στόχαστρο των εισβολών

Ο όρος Κοινωνική Μηχανική (Social Engineering) αναφέρεται σε συγκεκριμένη μέθοδο ηλεκτρονικής επίθεσης, η οποία χαρακτηρίζεται από πολλούς ως η μεγαλύτερη απειλή για την ασφάλεια των δικτύων. Ο λόγος είναι απλός: στόχος της κοινωνικής μηχανικής είναι ο ίδιος ο ανυποψίαστος χρήστης και όχι το σύστημα ασφάλειας και οι τεχνικές δυνάμεις του.

Οι επιτιθέμενοι που χρησιμοποιούν τις μεθόδους της κοινωνικής μηχανικής αλληλεπιδρούν με τους χρήστες του διαδικτύου με σκοπό να τους ξεγελάσουν, να κερδίσουν την εμπιστοσύνη τους και να παραβιάσουν το εκάστοτε σύστημα με τις πληροφορίες που «αλέυσαν», χωρίς απαραίτητα τη χρήση τεχνικών μέσων.

Τα βήματα που ακολουθεί ένας εισβολέας για να επιτύχει να εισβάλει σε ένα δίκτυο υπολογιστών με μεθόδους κοινωνικής μηχανικής, είναι τα εξής:

- Προσεγγίζει με κάποιο τρόπο ένα άτομο που έχει εξουσιοδοτημένη πρόσβαση στο δίκτυο.
- Παρουσιάζει τον εαυτό του ως άτομο εμπιστοσύνης.
- Προσπαθεί να αποσπάσει από το άτομο που προσέγγισε, πληροφορίες που θέτουν σε κίνδυνο την ασφάλεια του δικτύου.

Η βασική αδυναμία που εκμεταλλεύεται η κοινωνική μηχανική, είναι η ολιγωρία των ανθρώπων ως προς την υιοθέτηση μια τακτικής συνεχούς επαγρύπνησης όσον αφορά την ασφάλεια των πληροφοριών. Οι περισσότεροι χρήστες δε συνειδητοποιούν τη μεγάλη σπουδαιότητα των πληροφοριών που διαχειρίζονται και ως εκ τούτου δεν τηρούν τα απαραίτητα μέτρα προστασίας, με αποτέλεσμα να πέφτουν συχνά θύματα ηλεκτρονικών επιθέσεων. Εξίσου αρνητικός παράγοντας είναι η συνήθεια αρκετών χρηστών να επιλέγουν απλούς κωδικούς πρόσβασης, τους οποίους εύκολα μπορεί να μαντέψει κάποιος εισβολέας.



Ποιοί επηρεάζονται από επιθέσεις κοινωνικής μηχανικής;

Στόχος τέτοιων επιθέσεων είναι συνήθως οι επιχειρήσεις και συνεκδοχικά το ανθρώπινο δυναμικό τους. Κάθε άνθρωπος που σχετίζεται με μια επιχείρηση, είτε ως εργαζόμενος, είτε ως μέρος του εξωτερικού της περιβάλλοντος, έχει ευθύνη για την ακεραιότητά της. Ο εξοπλισμός για την ασφάλεια μιας εταιρείας μπορεί να κοστίζει εκατομμύρια, παρόλα αυτά, ένα και μόνο λάθος ενός ατόμου αρκεί για να θέσει σε μεγάλο κίνδυνο την ασφάλεια ολόκληρης της επιχείρησης. Προκειμένου να αποφευχθεί κάτι τέτοιο, κρίνεται απαραίτητο να πραγματοποιούνται τακτικές εκπαιδευτικές του προσωπικού της εταιρείας σε θέματα ασφάλειας πληροφοριών.

Τι πρέπει να κάνετε εάν έχετε πτέσει «θύμα» κοινωνικής μηχανικής;

- Αν έχετε αποκαλύψει ευαίσθητα δεδομένα για την επιχείρηση που εργαζόσαστε, θα πρέπει να το αναφέρετε άμεσα στους υπεύθυνους ασφάλειας της εταιρείας. Έτσι, θα είναι έτοιμοι να δράσουν σε περίπτωση που ανιληρθθούν κάποια ύποπτη συμπεριφορά.
- Αν πιστεύετε ότι κάποιος χρηματοπιστωτικός σας λογαριασμός κινδυνεύει, επικοινωνήστε αμέσως με την τράπεζά σας, για να κλείσετε τους λογαριασμούς αυτούς.
- Ελέγξτε τις χρεώσεις των λογαριασμών σας, μήπως ανακαλύψετε κινήσεις που δεν έχουν γίνει από εσάς.
- Αν έχετε αποκαλύψει κάποιον κωδικό πρόσβασης, φροντίστε αμέσως να τον αλλάξετε σε όλους τους λογαριασμούς που τον χρησιμοποιείτε. Επίσης μην τον ξαναχρησιμοποιήσετε στο μέλλον.
- Αναφέρετε σε κάθε περίπτωση οποιαδήποτε επίθεση στη Δίωξη Ηλεκτρονικού Εγκλήματος.

Τι πρέπει να κάνουν οι εταιρείες για να προστατέψουν τα δεδομένα τους;

Οι Ειδικό σε θέματα Ασφάλειας ενημερώνουν και προειδοποιούν:

- Η αξία των πληροφοριών και των δεδομένων είναι ανυπολόγιστη. Για το λόγο αυτό, οι επιθέσεις κοινωνικής μηχανικής συνιστούν τις μεγαλύτερες απειλές για τα συστήματα ασφάλειας.
- Ένα πολύ δυνατό όπλο ενάντια σε επιθέσεις κοινωνικής μηχανικής είναι η πρόληψη, η εκπαίδευση δηλαδή των χρηστών σχετικά με την αξία των δεδομένων και η κατάρτισή τους για την προστασία τους.
- Σε ορισμένες περιπτώσεις, «επιθέσεις» κοινωνικής μηχανικής χρησιμοποιούνται από Εταιρείες Ασφάλειας Πληροφοριών ως μέρος μιας διαδικασίας ελέγχου της ασφάλειας των πληροφοριακών συστημάτων που αξιολογούνται: ειδικοί τεχνικοί προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα συστήματα μιας επιχείρησης, όχι με τη χρήση τεχνικών μέσων, αλλά εκμεταλλευόμενοι τα λάθη των εργαζομένων.
- Ο έλεγχος με τη χρήση τεχνικών κοινωνικής μηχανικής είναι ζωτικής σημασίας για την αξιολόγηση της ασφάλειας ενός οργανισμού, καθότι προσδιορίζει τις αδυναμίες που υπάρχουν στο επίπεδο του ανθρώπινου χρήστη, οι οποίες δε μπορούν να εντοπιστούν από τον τεχνικό εξοπλισμό των συστημάτων ασφάλειας (πχ. τα τείχη προστασίας [firewalls]). Με αυτόν τον τρόπο αξιολογούνται οι γνώσεις του προσωπικού σε θέματα ασφάλειας και η αποτελεσματικότητα των εκπαιδευτικών προγραμμάτων ασφάλειας.

Αντίστροφη Κοινωνική Μηχανική

Είναι μια νέα μέθοδος που χρησιμοποιούν οι χάκερς για να αποσπάσουν πολύτιμες πληροφορίες από επιχειρήσεις και οργανισμούς. Σε αυτή ο εισβολέας παρουσιάζει τον εαυτό του ως άτομο με κάποια ιδιαίτερη γνώση ή ικανότητα και περιμένει από τους υπαλλήλους να τον ρωτήσουν πληροφορίες ή να ζητήσουν τη βοήθειά του. Η επίθεση με τη μέθοδο της αντίστροφης κοινωνικής μηχανικής γίνεται με τα ακόλουθα βήματα:

- Δολοφθορά: Ο επιτιθέμενος αρχικά δημιουργεί κάποιο πρόβλημα στον υπολογιστή ή το δίκτυο του θύματος.
- Διαφήμιση: Έπειτα διαφημίζει τον εαυτό του ως τον ειδικό να λύσει αυτό το πρόβλημα.
- Εξυπηρέτηση: Εάν το θύμα πειστεί και ζητήσει τη βοήθεια του εισβολέα, εκείνος με το πρόσχημα της τεχνικής υποστήριξης μπορεί να έχει πρόσβαση στα δεδομένα που επιθυμεί.

Αληθινές Ιστορίες

«Σας καλώ από το τμήμα εξυπηρέτησης πελατών...»



Μια γυναίκα έλαβε ένα τηλεφώνημα από κάποιον άγνωστο τη στιγμή που εργαζόταν, ο οποίος ισχυρίστηκε ότι έπαιρνε από την εξυπηρέτηση πελατών του τοπικού της υποκαταστήματος.

Της είπε ότι ο λόγος που τηλεφωνούσε ήταν ένα σφάλμα στο σύστημα διαχείρισης δεδομένων, το οποίο είχε προκαλέσει τη διαγραφή ορισμένων από τα στοιχεία των πελατών.

Ζήτησε λοιπόν από το θύμα να του υπαγορεύσει ξανά τα στοιχεία της (ονοματεπώνυμο, αριθμό πιστωτικής κάρτας, διεύθυνση χρέωσης και αριθμό κοινωνικής ασφάλισης).

Μετά από 20 μέρες, όταν το θύμα έλαβε τον αναλυτικό λογαριασμό χρέωσης της πιστωτικής κάρτας, εντόπισε εκπληκτική αγοράς αξίας 2.500 δολαρίων. Στις αγορές περιλαμβάνονταν μια ψηφιακή βιντεοκάμερα, ένας φορητός υπολογιστής, τρία mp3 και δύο dvd players.

Η ίδια δεν είχε κάνει καμία από αυτές τις αγορές, αλλά έπρεπε να τις πληρώσει όλες! Το μήνυμα αυτής της ιστορίας είναι πολύ σημαντικό: Ένας χάκερ δεν επιτίθενται πάντα από τον υπολογιστή του, ένα τηλεφώνημα ίσως να είναι αρκετό.

Υπουργικές ανέσεις με ένα τηλεφώνημα

Ένας νεαρός Τσέχος ονόματι Lukas Kohout, στοχημάτισε με τους φίλους του ότι μπορεί να ξεγελάσει την κυβέρνηση της Τσεχίας και να παρουσιαστεί ως εκπρόσωπος του υπουργού, για να χρησιμοποιήσει το κυβερνητικό αεροπλάνο.

Έπειτα από μερικές μέρες έρευνας, αφού μελέτησε πληροφορίες που αφορούσαν την ταυτική κυβέρνηση, τηλεφώνησε με σκοπό να προγραμματίσει μια πτήση για Σρι Λάνκα, υποδουμένος τον εκπρόσωπο ενός υπουργού.

Έμεινε εκπληκτος όταν το αεροπλάνο τέθηκε στη διάθεσή του και η πτήση προγραμματίστηκε όπως είχε ζητήσει. Αμέσως μετά τηλεφώνησε σε μία τοπική εταιρεία ασφάλειας (Samcora) και ζήτησε 5 σωματοφύλακες για το ταξίδι.

Ο νεαρός ισχυρίζεται ότι είναι εκπρόσωπος υπουργού, χρησιμοποιώντας ένα αριθμό ταυτότητας που είχε βρει κατά τη διάρκεια της έρευνάς του.



Ο Lukas συνέχισε την μέθοδο αυτή επί 1,5 χρόνο και ταξίδευε στο εξωτερικό χωρίς να πληρώνει. Ζήτησε επίσης χρήματα από την πρεσβεία της Τσεχίας και όταν του αρνήθηκαν είπε: "Είμαι εκπρόσωπος του Jan Kasal και ο αριθμός ταυτότητάς μου είναι OSN87" και έτσι κατόρθωσε να λάβει και μετρητά.

Τελικά, η απάτη αποκαλύφθηκε κατά τη διάρκεια ενός ταξιδιού στην Ινδία, καθώς δε διέθετε πράσινη κάρτα. Ύστερα από παραπομπή, καταδικάστηκε σε 6 μήνες φυλάκιση και υποχρεώθηκε να καταβάλει 30.000€, το συνολικό ποσό που είχε καταχραστεί.

Trust-IT



Η Trust-IT παρέχει Επιχειρηματικές Λύσεις Ασφάλειας και Τεχνολογίας Πληροφοριών και δραστηριοποιείται στον τομέα της Ευφυούς Ασφάλειας των Πληροφοριών (IT Security Intelligence).

Στοιχεία Επικοινωνίας

Trust-IT

Λ. Μεσογείων 176-178

155 61, Χολαργός

Τηλ. 210 6520660

E-mail: info@trust-it.gr

URL: <http://www.trust-it.gr>

Ακολουθήστε την Trust-IT

