ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Διερεύνηση και Ανάλυση του Ρίσκου Κυβερνοεπιθέσεων με Βάση τον Ανθρώπινο Παράγοντα σε έναν Οργανισμό

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Χριστίνα Λούζο

Επιβλέπων : Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2020

Διερεύνηση και Ανάλυση του Ρίσκου Κυβερνοεπιθέσεων με Βάση τον Ανθρώπινο Παράγοντα σε έναν Οργανισμό

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Διερεύνηση και Ανάλυση του Ρίσκου Κυβερνοεπιθέσεων με Βάση τον Ανθρώπινο Παράγοντα σε έναν Οργανισμό

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Χριστίνα Λούζο

Επιβλέπων : Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 27η Οκτωβρίου 2020.

.....	.....	.....
Δημήτριος Ασκούνης	Ιωάννης Ψαρράς	Χρυσόστομος Δούκας
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Επίκουρος Καθηγητής Ε.Μ.Π.

Διερεύνηση και Ανάλυση του Ρίσκου Κυβερνοεπιθέσεων με Βάση τον Ανθρώπινο Παράγοντα σε έναν Οργανισμό

Αθήνα, Οκτώβριος 2020

.....
Χριστίνα Λούζο

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Διερεύνηση και Ανάλυση του Ρίσκου Κυβερνοεπιθέσεων με Βάση τον Ανθρώπινο Παράγοντα σε έναν Οργανισμό

ΠΕΡΙΛΗΨΗ:

Η παρούσα διπλωματική προσπαθεί να διασυνδέσει τις διαστάσεις και τα χαρακτηριστικά της ψυχολογίας και της συμπεριφοράς των εργαζομένων με τις Κυβερνοεπιθέσεις που απειλούν τους Οργανισμούς και ευδοκιμούν εξαιτίας του ανθρώπινου σφάλματος. Αρχικά αναλύεται η σημασία της Κυβερνασφάλειας και τα αποτελέσματα του αυξανόμενου αριθμού των Κυβερνοεπιθέσεων. Στη συνέχεια, αναφέρονται και αναλύονται οι πιο συχνές κατηγορίες Κυβερνοεπιθέσεων, καθώς και οι κατηγορίες που εξαρτώνται από τον ανθρώπινο παράγοντα. Παρουσιάζονται τα στατιστικά στοιχεία που δείχνουν την επίδραση των Κυβερνοεπιθέσεων και έπειτα αναλύεται η συμπεριφορά των ανθρώπων, και συγκεκριμένα των εργαζομένων σε Οργανισμούς και τα στάδια ανάπτυξης της συμπεριφοράς τους και οι προδιαγραφές του ISO / IEC 27002 που προτείνεται να ακολουθούνται από τους Οργανισμούς. Στο τέλος συνδέονται τα χαρακτηριστικά της συμπεριφοράς των εργαζομένων με τις κατηγορίες των Κυβερνοεπιθέσεων που εξαρτώνται από τον ανθρώπινο παράγοντα και προτείνονται οι διαδικασίες για την αποφυγή και εξάλειψή τους.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ:

Κυβερνοχώρος, Κυβερνοεπίθεση, Κυβερνοασφάλεια, κοινωνική μηχανική, ανθρώπινο σφάλμα, παραβίαση δεδομένων, συμπεριφορά ασφάλειας πληροφοριών, διαδικασίες ασφάλειας πληροφοριών

ABSTRACT:

This diploma thesis attempts to link the dimensions and characteristics of employees' psychology and behavior towards Cyberattacks that threaten the Organizations and thrive on human error. Initially, we analyze the importance of Cybersecurity and the effects of the growing number of Cyberattacks. Then, we enlist and analyze the most common categories of Cyberattacks, as well as the categories that depend on the human factor. Statistics show the impact of Cyberattacks and then we analyze the behavior of people, specifically employees in organizations and the stages of development of their behavior and the specifications of ISO / IEC 27002 that are proposed to be followed by the organizations. In the end, we connect the characteristics of the employees' behavior with the categories of Cyber-attacks that depend on the human factor and we propose the procedures in order Cyber attacks to be avoided and eliminated.

KEYWORDS:

Cyberspace, Cyber Attack, Cyber Security, Social Engineering, human error, ISB – Information Security Behavior, ISP – Information Security Procedures, data breach

ΕΥΧΑΡΙΣΤΙΕΣ:

Με την ολοκλήρωση της διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όλους όσους συνέβαλλαν στην εκπόνησή της.

Ευχαριστώ θερμά τον επιβλέπων καθηγητή μου, κύριο Δημήτρη Ασκούνη, για την εμπιστοσύνη που μου έδειξε εξ' αρχής, αναθέτοντάς μου το συγκεκριμένο θέμα, την επιστημονική του καθοδήγηση και τις υποδείξεις του.

Επιπλέον, ιδιαίτερες ευχαριστίες θα ήθελα να απευθύνω στον υποψήφιο διδάκτορα Κανάρη Μπούνα για τη συνεχή υποστήριξη και βοήθειά του, καθ' όλη τη διάρκεια της ερευνητικής διαδικασίας.

Τέλος, θα ήθελα εκφράσω την ευγνωμοσύνη μου στην οικογένειά μου για όλη τη στήριξη, τη συμπαράσταση και την κατανόησή τους, καθ' όλη τη διάρκεια των σπουδών μου.

Περιεχόμενα

ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ

Κεφάλαιο 1: ΕΙΣΑΓΩΓΗ

Ένα από τα προβλήματα που αντιμετωπίζουν οι Οργανισμοί στη σύγχρονη ψηφιακή εποχή είναι ο κίνδυνος της ασφάλειας των πληροφοριών που διαθέτουν. Για να μπορέσουν οι Οργανισμοί να αντιμετωπίσουν αυτό το πρόβλημα και να διαφυλάξουν τις πληροφορίες τους, επενδύουν στην Κυβερνοασφάλεια.

Η Κυβερνοασφάλεια είναι η πρακτική της προστασίας συστημάτων, δικτύων και προγραμμάτων από ηλεκτρονικές επιθέσεις. Αυτές οι ηλεκτρονικές επιθέσεις στοχεύουν συνήθως στην πρόσβαση, την αλλαγή ή την καταστροφή ευαίσθητων πληροφοριών, την απόσπαση χρημάτων από χρήστες ή τη διακοπή των κανονικών επιχειρηματικών διαδικασιών.

Η εφαρμογή αποτελεσματικών μέτρων ασφάλειας στον κυβερνοχώρο είναι ιδιαίτερα δύσκολη σήμερα, επειδή υπάρχουν περισσότερες συσκευές από τους ανθρώπους και οι επιτιθέμενοι γίνονται πιο καινοτόμοι.

Η ασφάλεια πληροφοριών, που συχνά αναφέρεται ως InfoSec, αναφέρεται στις διαδικασίες και τα εργαλεία που έχουν σχεδιαστεί και αναπτυχθεί για την προστασία ευαίσθητων επιχειρηματικών πληροφοριών από τροποποιήσεις, διαταραχές, καταστροφή και επιθεώρηση.

Για τη διασφάλιση της ασφάλειας των πληροφοριών όμως, μεγάλο μέρος ευθύνης έχουν και οι εργαζόμενοι των Οργανισμών, τα σφάλματα των οποίων οδηγούν σε διέρευση των απόρρητων πληροφοριών του Οργανισμού.

Με βάση τις γνωστές Κυβερνοεπιθέσεις που απειλούν τους Οργανισμούς και τα χαρακτηριστικά της ψυχολογίας και της συμπεριφοράς των εργαζομένων, η παρούσα εργασία συνδέει αυτά τα δύο στοιχεία, εφόσον για να μπορέσει να αντιμετωπισθεί το πρόβλημα των Κυβερνοεπιθέσεων πρέπει να διερευνηθούν οι παράγοντες που τις ενισχύουν.

Κεφάλαιο 2: ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ

2.1. Η σημασία της Κυβερνοασφάλειας

Η ασφάλεια στον κυβερνοχώρο είναι σημαντική διότι περιλαμβάνει όλα όσα σχετίζονται με την προστασία των ευαίσθητων δεδομένων μας, των προσωπικά αναγνωρίσιμων πληροφοριών (PII), των προστατευόμενων πληροφοριών για την υγεία (PHI), των προσωπικών πληροφοριών, της πνευματικής ιδιοκτησίας, των δεδομένων και των κυβερνητικών και βιομηχανικών συστημάτων πληροφοριών, από κλοπή και ζημία που επιχειρούν εγκληματίες και αντίπαλοι.

Ο κίνδυνος ασφάλειας στον κυβερνοχώρο αυξάνεται, καθοδηγούμενος από την παγκόσμια συνδεσιμότητα και τη χρήση υπηρεσιών cloud, όπως το Amazon Web Services, για την αποθήκευση ευαίσθητων δεδομένων και προσωπικών πληροφοριών. Η εκτεταμένη κακή διαμόρφωση των υπηρεσιών cloud σε συνδυασμό με τους όλο και πιο εξελιγμένους εγκληματίες στον κυβερνοχώρο, σημαίνει ότι αυξάνεται ο κίνδυνος να υποστεί ο οργανισμός μια επιτυχή επίθεση στον κυβερνοχώρο ή παραβίαση δεδομένων. (Upguard, 2020)

Πέρασαν οι μέρες του απλού τείχους προστασίας και του λογισμικού προστασίας από ιούς ως τα μοναδικά μέτρα ασφαλείας. Οι Οργανισμοί δεν μπορούν πλέον να αφήνουν την ασφάλεια πληροφοριών στους επαγγελματίες της Κυβερνοασφάλειας.

Οι απειλές στον κυβερνοχώρο μπορούν να προέρχονται από οποιοδήποτε επίπεδο του Οργανισμού. Είναι αναγκαίο να εκπαιδευτεί το προσωπικό σχετικά με τις απλές απάτες κοινωνικής μηχανικής, όπως το ηλεκτρονικό ψάρεμα (phishing) και πιο εξελιγμένες επιθέσεις στον κυβερνοχώρο από κακόβουλο λογισμικό που έχει σχεδιαστεί για την κλοπή πνευματικής ιδιοκτησίας ή προσωπικών δεδομένων.

Ο GDPR και άλλοι νόμοι σημαίνουν ότι η ασφάλεια στον κυβερνοχώρο δεν είναι πλέον κάτι που οι επιχειρήσεις οποιουδήποτε μεγέθους μπορούν να αγνοήσουν. Τα περιστατικά ασφαλείας επηρεάζουν τακτικά τις επιχειρήσεις όλων των μεγεθών, προκαλώντας συχνά μη αναστρέψιμη ζημία στη φήμη των εμπλεκόμενων εταιρειών.

Το γεγονός είναι ότι είτε σε ατομικό επίπεδο, είτε ένας μικρός, μεγάλος ή πολυεθνικός οργανισμός, όλοι βασίζονται σε συστήματα υπολογιστών κάθε μέρα. Σε συνδυασμό με την αύξηση των υπηρεσιών cloud, την κακή ασφάλεια των υπηρεσιών cloud, τα smartphones και το Internet of Things (IoT) υπάρχουν πολλές απειλές στην κυβερνοασφάλεια που δεν υπήρχαν πριν από μερικές δεκαετίες.

Οι κυβερνήσεις πλέον σε όλο τον κόσμο δίνουν μεγαλύτερη προσοχή στα εγκλήματα στον κυβερνοχώρο. Ο GDPR είναι ένα εξαιρετικό παράδειγμα, καθώς έχει γνωστοποιήσει τις επιπτώσεις από τις παραβιάσεις δεδομένων αναγκάζοντας όλους τους οργανισμούς που δραστηριοποιούνται στην ΕΕ:

- Να επικοινωνούν τις παραβιάσεις δεδομένων
- Να διορίσουν έναν υπεύθυνο προστασίας δεδομένων
- Να απαιτείται συναίνεση του χρήστη για την επεξεργασία πληροφοριών
- Να ανωνυμοποιηθούν δεδομένα για προστασία της ιδιωτικότητας

Η τάση για δημοσιοποίηση δεν περιορίζεται στην Ευρώπη. Ενώ δεν υπάρχουν εθνικοί νόμοι που εποπτεύουν την αποκάλυψη παραβιάσεων δεδομένων στις Ηνωμένες Πολιτείες, υπάρχουν νόμοι περί παραβίασης δεδομένων και στις 50 πολιτείες που περιλαμβάνουν:

- Απαίτηση κοινοποίησης όσων επηρεάζονται το συντομότερο δυνατό
- Ενημέρωση της κυβέρνησης το συντομότερο δυνατό
- Πληρωμή ενός προστίμου

Η Καλιφόρνια ήταν η πρώτη πολιτεία που ρύθμισε τις κοινοποιήσεις παραβιάσεων δεδομένων το 2003, απαιτώντας από άτομα ή επιχειρήσεις να ειδοποιήσουν τους πληγέντες «χωρίς εύλογη καθυστέρηση» και «αμέσως μετά την ανακάλυψη». Τα

θύματα μπορούν να μηνύσουν έως και 750 $ και στις εταιρείες μπορούν να επιβληθούν πρόστιμα έως 7.500 $ ανά θύμα.

Αυτό οδήγησε οργανισμούς όπως το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) να ανακοινώσουν πλαίσια και πρότυπα για να βοηθήσουν τους οργανισμούς να κατανοήσουν τους κινδύνους ασφάλειάς τους, να βελτιώσουν τα μέτρα ασφάλειας στον κυβερνοχώρο και να αποτρέψουν τις επιθέσεις στον κυβερνοχώρο.

2.2. Γιατί αυξάνεται το έγκλημα στον κυβερνοχώρο

Η κλοπή πληροφοριών είναι το πιο ακριβό και ταχύτερα αναπτυσσόμενο τμήμα του εγκλήματος στον κυβερνοχώρο. Κυρίως καθοδηγείται από την αυξανόμενη έκθεση πληροφοριών ταυτότητας στον Ιστό μέσω υπηρεσιών cloud. Αλλά δεν είναι ο μόνος στόχος. Οι βιομηχανικοί έλεγχοι που διαχειρίζονται ηλεκτρικά δίκτυα και άλλες υποδομές μπορούν να διαταραχθούν ή να καταστραφούν. Η κλοπή ταυτότητας δεν είναι ο μόνος στόχος, οι επιθέσεις στον κυβερνοχώρο μπορεί να στοχεύουν στην ακεραιότητα των δεδομένων με την καταστροφή ή την αλλαγή τους, για να δημιουργήσουν δυσπιστία σε έναν οργανισμό ή κυβέρνηση.

Οι εγκληματίες του κυβερνοχώρου γίνονται πιο περίπλοκοι, αλλάζουν οι στόχοι τους, ο τρόπος που επηρεάζουν τους οργανισμούς και οι μέθοδοι επίθεσής τους σε διαφορετικά συστήματα ασφαλείας.

Η κοινωνική μηχανική παραμένει η ευκολότερη μορφή επίθεσης στον κυβερνοχώρο με το ransomware και το ηλεκτρονικό ψάρεμα να είναι η ευκολότερη μορφή εισόδου. (Upguard, 2020) Άμεσοι εξωτερικοί προμηθευτές (third party) και έμμεσοι εξωτερικοί προμηθευτές (fourth party) που επεξεργάζονται τα δεδομένα πελατών και έχουν κακές πρακτικές ασφάλειας στον κυβερνοχώρο είναι ένας άλλος κοινός φορέας επίθεσης, καθιστώντας τη διαχείριση κινδύνου από τον προμηθευτή όλο και πιο σημαντική.

Σύμφωνα με την Ένατη Ετήσια Μελέτη για το Έγκλημα στον Κυβερνοχώρο από την Accenture (Accenture, 2019) και το Ponemon Institute, το μέσο κόστος του εγκλήματος στον κυβερνοχώρο για έναν οργανισμό έχει αυξηθεί κατά 1,4 εκατομμύρια δολάρια το προηγούμενο έτος αγγίζοντας τα 13,0 εκατομμύρια δολάρια και ο μέσος αριθμός

παραβιάσεων δεδομένων αυξήθηκε κατά 11% αγγίζοντας τις 145. Η διαχείριση του κινδύνου πληροφοριών είναι πιο σημαντική από ποτέ.

Οι παραβιάσεις δεδομένων μπορεί να περιλαμβάνουν οικονομικές πληροφορίες όπως αριθμούς πιστωτικών καρτών ή στοιχεία τραπεζικού λογαριασμού, προστατευόμενες πληροφορίες υγείας (PHI), προσωπικά αναγνωρίσιμες πληροφορίες (PII), εμπορικά μυστικά, πνευματική ιδιοκτησία και άλλους στόχους βιομηχανικής κατασκοπείας. Άλλοι όροι για παραβιάσεις δεδομένων περιλαμβάνουν ακούσια αποκάλυψη πληροφοριών, διαρροή δεδομένων, διαρροή cloud, διαρροή πληροφοριών ή διαρροή δεδομένων.

Άλλοι παράγοντες που οδηγούν την ανάπτυξη του εγκλήματος στον κυβερνοχώρο περιλαμβάνουν:

- Την κατανεμημένη φύση του Διαδικτύου
- Την ικανότητα των κυβερνοεγκληματιών να επιτίθενται σε στόχους εκτός της δικαιοδοσίας τους καθιστώντας την αστυνόμευση εξαιρετικά δύσκολη
- Την αυξανόμενη κερδοφορία και την ευκολία του εμπορίου στο dark web

(Upguard, 2020)

2.3. Κυβερνοεπιθέσεις και κοινωνική μηχανική

Η κοινωνική μηχανική είναι μια τεχνική χειραγώγησης που εκμεταλλεύεται το ανθρώπινο λάθος για να αποκτήσει ιδιωτικές πληροφορίες, πρόσβαση ή τιμαλφή. Στο έγκλημα στον κυβερνοχώρο, αυτές οι απάτες «ανθρώπινης πειρατείας» τείνουν να παρασύρουν τους ανυποψίαστους χρήστες να εκθέσουν δεδομένα, να διαδώσουν μολύνσεις από κακόβουλα προγράμματα ή να έχουν πρόσβαση σε περιορισμένα συστήματα.

Οι απάτες που βασίζονται στην κοινωνική μηχανική, βασίζονται στον τρόπο που σκέφτονται και ενεργούν οι άνθρωποι. Ως εκ τούτου, οι επιθέσεις κοινωνικής μηχανικής είναι ιδιαίτερα χρήσιμες για τον χειρισμό της συμπεριφοράς ενός χρήστη. Μόλις ένας εισβολέας καταλάβει τι παρακινεί τις ενέργειες ενός χρήστη, μπορεί να εξαπατήσει και να χειριστεί τον χρήστη αποτελεσματικά.

Επιπλέον, οι αντίπαλοι προσπαθούν να εκμεταλλευτούν την έλλειψη γνώσεων ενός χρήστη. Χάρη στην ταχύτητα της τεχνολογίας, πολλοί χρήστες και εργαζόμενοι δεν γνωρίζουν συγκεκριμένες απειλές που υπάρχουν στον Κυβερνοχώρο. Οι χρήστες ενδέχεται επίσης να μην συνειδητοποιήσουν την πλήρη αξία των προσωπικών δεδομένων, όπως τον αριθμό τηλεφώνου τους. Ως αποτέλεσμα, πολλοί χρήστες δεν γνωρίζουν με ποιον τρόπο να προστατεύσουν καλύτερα τον εαυτό τους και τις πληροφορίες τους. (Kaspersky, n.d.)

2.4. Ο αντίκτυπος του εγκλήματος στον κυβερνοχώρο

Η έλλειψη εστίασης στην Κυβερνοασφάλεια μπορεί να βλάψει έναν οργανισμό με τους εξής τρόπους:

- Οικονομικό κόστος: Κλοπή πνευματικής ιδιοκτησίας και εταιρικών πληροφοριών, διαταραχές στο εμπόριο και κόστος επισκευής κατεστραμμένων συστημάτων

- Κόστος φήμης: Απώλεια εμπιστοσύνης καταναλωτή, απώλεια τρεχόντων και μελλοντικών πελατών και κακή κάλυψη των μέσων ενημέρωσης

- Ρυθμιστικό κόστος: Ο νόμος GDPR και άλλοι νόμοι περί παραβίασης δεδομένων σημαίνουν ότι ο οργανισμός ενδέχεται να υποστεί κανονιστικά πρόστιμα ή κυρώσεις ως αποτέλεσμα εγκλημάτων στον κυβερνοχώρο.
  (Cisco, 2020) , (Upguard, 2020)

Όλες οι επιχειρήσεις, ανεξάρτητα από το μέγεθός τους, πρέπει να διασφαλίσουν ότι όλο το προσωπικό κατανοεί τις απειλές για την ασφάλεια στον κυβερνοχώρο και πώς να τις μετριάσει. Αυτό θα πρέπει να περιλαμβάνει τακτική εκπαίδευση και ένα πλαίσιο για να συνεργαστεί με αυτό να στοχεύει στη μείωση του κινδύνου διαρροών δεδομένων ή παραβιάσεων δεδομένων.

Δεδομένης της φύσης του εγκλήματος στον κυβερνοχώρο και πόσο δύσκολο είναι να εντοπιστεί, είναι δύσκολο να κατανοήσουμε το άμεσο και έμμεσο κόστος πολλών παραβιάσεων ασφαλείας. (Cisco, 2020) , (Upguard, 2020)

Κεφάλαιο 3: ΟΙ ΠΙΟ ΣΥΝΗΘΙΣΜΕΝΕΣ ΚΑΤΗΓΟΡΙΕΣ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ

3.1. Επίθεση άρνησης υπηρεσίας (DoS) και επίθεση κατανεμημένης άρνησης υπηρεσίας(DDoS)

Μια επίθεση άρνησης υπηρεσίας κατακλύζει τους πόρους ενός συστήματος, ώστε να μην μπορεί να ανταποκριθεί σε αιτήματα υπηρεσίας. Μια επίθεση DDoS είναι επίσης μια επίθεση στους πόρους του συστήματος, αλλά ξεκινά από έναν μεγάλο αριθμό άλλων μηχανών υποδοχής που έχουν μολυνθεί από κακόβουλο λογισμικό που ελέγχεται από τον εισβολέα.

Σε αντίθεση με τις επιθέσεις που έχουν σχεδιαστεί για να επιτρέψουν στον εισβολέα να αποκτήσει ή να αυξήσει την πρόσβαση, η άρνηση υπηρεσίας δεν παρέχει άμεσα οφέλη για τους εισβολείς. Για μερικούς από αυτούς, αρκεί η ικανοποίηση της άρνησης υπηρεσίας. Ωστόσο, εάν ο πόρος που δέχεται επίθεση ανήκει σε επιχειρηματικό ανταγωνιστή, τότε το όφελος για τον εισβολέα μπορεί να είναι αρκετά σημαντικό. Ένας άλλος σκοπός μιας επίθεσης DoS μπορεί να είναι να θέσει ένα σύστημα εκτός σύνδεσης έτσι ώστε να ξεκινήσει ένα διαφορετικό είδος επίθεσης, με κοινό παράδειγμα την πειρατεία συνεδριών.

Υπάρχουν διαφορετικοί τύποι επιθέσεων DoS και DDoS. Οι πιο συνηθισμένες είναι τα εξής: TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack και botnets.

3.2. Επίθεση TCP SYN Flood

Σε αυτήν την επίθεση, ένας εισβολέας εκμεταλλεύεται τη χρήση του χώρου του buffer κατά τη διάρκεια μιας χειραψίας προετοιμασίας περιόδου σύνδεσης Transmission Control Protocol (TCP). Η συσκευή του εισβολέα πλημμυρίζει τη μικρή ουρά του συστήματος στόχου με αιτήματα σύνδεσης, αλλά δεν αποκρίνεται όταν το σύστημα στόχος απαντά σε αυτά τα αιτήματα. Αυτό προκαλεί το time out του συστήματος

στόχου περιμένοντας την απόκριση από τη συσκευή του εισβολέα, γεγονός που προκαλεί την κατάρευση του συστήματος ή την αδυναμία χρήσης του όταν γεμίζει η ουρά σύνδεσης.

Υπάρχουν μερικά αντίμετρα για μια επίθεση πλημμύρας TCP SYN:

- Τοποθέτηση διακομιστών πίσω από ένα τείχος προστασίας που έχει ρυθμιστεί για να σταματά τα εισερχόμενα πακέτα SYN.
- Αύξηση του μεγέθους της ουράς σύνδεσης και μείωση του χρονικού ορίου στις ανοιχτές συνδέσεις.

3.3. Επίθεση Teardrop

Αυτή η επίθεση προκαλεί τα πεδία αντιστάθμισης μήκους και κατακερματισμού σε διαδοχικά πακέτα πρωτοκόλλου διαδικτύου (IP) να αλληλοεπικαλύπτονται στον επιτιθέμενο κεντρικό υπολογιστή. Το επιτιθέμενο σύστημα προσπαθεί να ανακατασκευάσει πακέτα κατά τη διάρκεια της διαδικασίας, αλλά αποτυγχάνει. Το σύστημα προορισμού στη συνέχεια μπερδεύεται και καταρρέει.

Εάν οι χρήστες δεν έχουν ενημερώσεις κώδικα για προστασία από αυτήν την επίθεση DoS, πρέπει να απενεργοποιήσουν το SMBv2 και να αποκλείσουν τις θύρες 139 και 445. (Melnick, 2020)

3.4. Επίθεση Smurf

Αυτή η επίθεση περιλαμβάνει τη χρήση πλαστογράφησης IP και του ICMP για κορεσμό ενός δικτύου προορισμού με κίνηση. Αυτή η μέθοδος επίθεσης χρησιμοποιεί ICMP αιτήματα ηχούς που στοχεύουν σε διευθύνσεις IP μετάδοσης. Αυτά τα αιτήματα ICMP προέρχονται από μια πλαστή διεύθυνση «θύματος». Για παράδειγμα, εάν η προοριζόμενη διεύθυνση θύματος είναι 10.0.0.10, ο εισβολέας θα πλαστογραφήσει ένα αίτημα ηχούς ICMP από 10.0.0.10 στη διεύθυνση εκπομπής 10.255.255.255. Αυτό το αίτημα θα πήγαινε σε όλα τα IP στην περιοχή, με όλες τις απαντήσεις να ξεκινούν έως τις 10.0.0.10, κατακλύζοντας το δίκτυο. Αυτή η διαδικασία είναι

επαναλαμβανόμενη και μπορεί να αυτοματοποιηθεί για να δημιουργήσει τεράστιες ποσότητες συμφόρησης δικτύου.

Για την προστασία των συσκευών από αυτήν την επίθεση, απαιτείται η απενεργοποίηση των εκπομπών που κατευθύνονται από IP στους δρομολογητές. Αυτό θα αποτρέψει το αίτημα εκπομπής ηχούς ICMP στις συσκευές δικτύου. Μια άλλη επιλογή είναι η διαμόρφωση των τερματικών συστημάτων ώστε να μην αποκρίνονται σε πακέτα ICMP από διευθύνσεις εκπομπής.

3.5. Επίθεση Ping of Death

Αυτός ο τύπος επίθεσης χρησιμοποιεί πακέτα IP για να κάνει ping σε ένα σύστημα στόχου με μέγεθος IP πάνω από το μέγιστο των 65.535 byte. Δεν επιτρέπονται πακέτα IP αυτού του μεγέθους, οπότε ο εισβολέας θρυμματίζει το πακέτο IP. Μόλις το σύστημα προορισμού επανασυναρμολογήσει το πακέτο, μπορεί να αντιμετωπίσει υπερχείλιση buffer και άλλα σφάλματα.

Οι επιθέσεις Ping of Death μπορούν να αποκλειστούν χρησιμοποιώντας ένα τείχος προστασίας που θα ελέγχει κατακερματισμένα πακέτα IP για μέγιστο μέγεθος.

3.6. Botnets

Τα botnets είναι τα εκατομμύρια των συστημάτων που έχουν μολυνθεί από κακόβουλο λογισμικό υπό έλεγχο χάκερ, προκειμένου να πραγματοποιήσουν επιθέσεις DDoS. Αυτά τα bots ή συστήματα ζόμπι χρησιμοποιούνται για τη διεξαγωγή επιθέσεων εναντίον των συστημάτων στόχων, συχνά κατακλύζουν το εύρος ζώνης και τις δυνατότητες επεξεργασίας του συστήματος στόχου. Αυτές οι επιθέσεις DDoS είναι δύσκολο να εντοπιστούν επειδή τα botnets βρίσκονται σε διαφορετικές γεωγραφικές τοποθεσίες.

Τα botnets μπορούν να μετριαστούν από:

- Το φιλτράρισμα RFC3704, το οποίο θα αρνηθεί την κυκλοφορία από πλαστογραφημένες διευθύνσεις και θα διασφαλίσει ότι η επισκεψιμότητα είναι

ανιχνεύσιμη στο σωστό δίκτυο προέλευσης. Για παράδειγμα, το φιλτράρισμα RFC3704 θα ρίξει πακέτα από διευθύνσεις λίστας bogon.

- Το φιλτράρισμα μαύρων οπών, το οποίο μειώνει την ανεπιθύμητη κίνηση πριν εισέλθει σε προστατευμένο δίκτυο. Όταν εντοπιστεί μια επίθεση DDoS, ο BGP (Border Gateway Protocol) host θα πρέπει να στέλνει ενημερώσεις δρομολόγησης σε δρομολογητές ISP, έτσι ώστε να δρομολογεί όλη την επισκεψιμότητα προς διακομιστές θύματος σε μια διεπαφή null0 στο επόμενο hop.

3.7. Επίθεση Man-in-the-Middle(MitM)

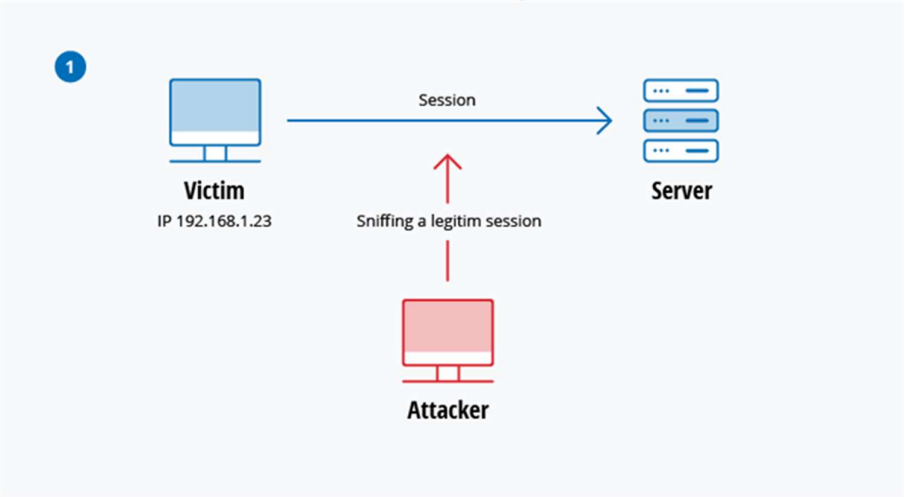
Μια επίθεση MitM συμβαίνει όταν ένας εισβολέας παρεμβάλλεται μεταξύ των επικοινωνιών ενός πελάτη και ενός διακομιστή. Ακολουθούν ορισμένοι κοινοί τύποι επιθέσεων man-in-the-middle:

Παραβίαση συνεδρίας:

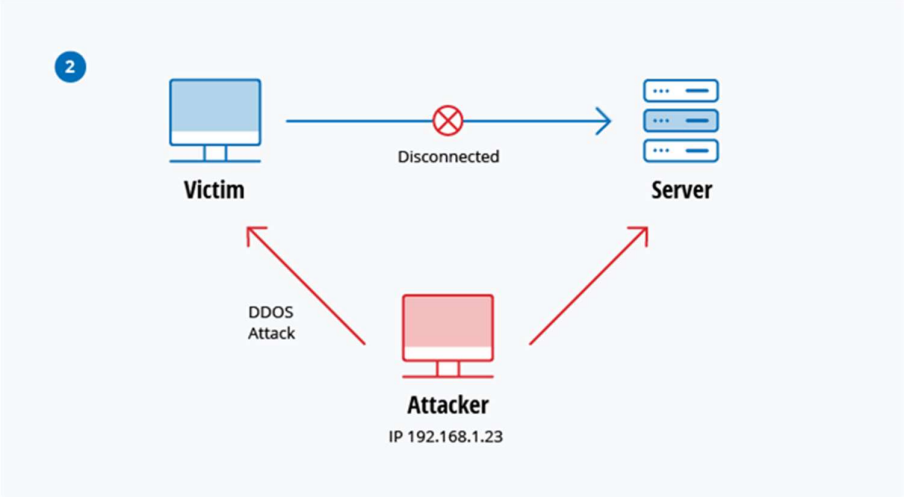
Σε αυτόν τον τύπο επίθεσης MitM, ένας εισβολέας εισβάλλει σε μια περίοδο σύνδεσης μεταξύ ενός αξιόπιστου πελάτη και ενός διακομιστή δικτύου. Ο επιτιθέμενος υπολογιστής αντικαθιστά με τη διεύθυνση IP του τη διεύθυνση IP του αξιόπιστου πελάτη, ενώ ο διακομιστής συνεχίζει τη συνεδρία, πιστεύοντας ότι επικοινωνεί με τον πελάτη. Για παράδειγμα, η επίθεση μπορεί να ξεδιπλωθεί ως εξής:

- Ένας πελάτης συνδέεται με έναν διακομιστή.
- Ο υπολογιστής του εισβολέα αποκτά τον έλεγχο του πελάτη.
- Ο υπολογιστής του εισβολέα αποσυνδέει τον πελάτη από το διακομιστή.
- Ο υπολογιστής του εισβολέα αντικαθιστά τη διεύθυνση IP του πελάτη με τη δική του διεύθυνση IP και
- πλαστογραφεί τους αριθμούς ακολουθίας του πελάτη.
- Ο υπολογιστής του εισβολέα συνεχίζει το διάλογο με τον διακομιστή και ο διακομιστής πιστεύει ότι εξακολουθεί να επικοινωνεί με τον πελάτη.

Εικόνα 1: Επίθεση DoS



Εικόνα 2: Επίθεση DDoS



3.8. IP Spoofing

Το IP spoofing χρησιμοποιείται από έναν εισβολέα για να πείσει ένα σύστημα ότι επικοινωνεί με μια γνωστή, αξιόπιστη οντότητα και παρέχει στον εισβολέα πρόσβαση στο σύστημα. Ο εισβολέας στέλνει ένα πακέτο με τη διεύθυνση προέλευσης IP ενός γνωστού, αξιόπιστου κεντρικού υπολογιστή αντί της δικής του διεύθυνσης προέλευσης IP σε έναν κεντρικό υπολογιστή προορισμού. Ο κεντρικός υπολογιστής στόχος μπορεί να αποδεχτεί το πακέτο και να ενεργήσει πάνω του. (Melnick, 2020)

3.9. Replay

Μια επίθεση επανάληψης εμφανίζεται όταν ένας εισβολέας παρεμποδίζει και αποθηκεύει παλιά μηνύματα και στη συνέχεια προσπαθεί να τα στείλει αργότερα, πλαστοπροσωπώντας έναν από τους συμμετέχοντες. Αυτός ο τύπος μπορεί να αντιμετωπιστεί εύκολα με χρονικές σημάνσεις περιόδου λειτουργίας ή nonce (ένας τυχαίος αριθμός ή μια συμβολοσειρά που αλλάζει με την ώρα).

Προς το παρόν, δεν υπάρχει μεμονωμένη τεχνολογία ή διαμόρφωση για την αποτροπή όλων των επιθέσεων MitM. Γενικά, η κρυπτογράφηση και τα ψηφιακά πιστοποιητικά παρέχουν μια αποτελεσματική προστασία έναντι επιθέσεων MitM, διασφαλίζοντας τόσο την εμπιστευτικότητα όσο και την ακεραιότητα των επικοινωνιών. Αλλά μια επίθεση man-in-the-middle μπορεί να εγχυθεί στη μέση των επικοινωνιών με τέτοιο τρόπο ώστε η κρυπτογράφηση να μην βοηθήσει - για παράδειγμα, ο εισβολέας "A" παρεμποδίζει το δημόσιο κλειδί του ατόμου "P" και το αντικαθιστά με το δικό του κοινό κλειδί. Στη συνέχεια, όποιος θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στο P χρησιμοποιώντας το δημόσιο κλειδί του P χρησιμοποιεί, εν αγνοία του, το δημόσιο κλειδί του A. Επομένως, ο A μπορεί να διαβάσει το μήνυμα που προορίζεται για το P και στη συνέχεια να στείλει το μήνυμα στο P, κρυπτογραφημένο στο πραγματικό δημόσιο κλειδί του P και ο P δεν θα παρατηρήσει ποτέ ότι το μήνυμα έχει παραβιαστεί. Επιπλέον, ο A θα μπορούσε επίσης να τροποποιήσει το μήνυμα προτού το στείλει ξανά στο P. Όπως μπορείτε να δείτε, ο P χρησιμοποιεί κρυπτογράφηση και πιστεύει ότι οι πληροφορίες του προστατεύονται αλλά δεν είναι, λόγω της επίθεσης MitM.

Για να λυθεί το πρόβλημα επιβεβαίωσης του ότι το δημόσιο κλειδί του P ανήκει στο P και όχι στο A δημιουργήθηκαν οι αρχές έκδοσης πιστοποιητικών και οι λειτουργίες κατακερματισμού. Όταν το άτομο 2 (P2) θέλει να στείλει ένα μήνυμα στο P και το P θέλει να είναι σίγουρο ότι το A δεν θα διαβάσει ή θα τροποποιήσει το μήνυμα και ότι το μήνυμα προήλθε πραγματικά από το P2, πρέπει να χρησιμοποιηθεί η ακόλουθη μέθοδος:

- Ο P2 δημιουργεί ένα συμμετρικό κλειδί και το κρυπτογραφεί με το δημόσιο κλειδί του P.
- Ο P2 στέλνει το κρυπτογραφημένο συμμετρικό κλειδί στο P.
- Ο P2 υπολογίζει μια συνάρτηση κατακερματισμού του μηνύματος και το υπογράφει ψηφιακά.

- Ο P2 κρυπτογραφεί το μήνυμά του και το υπογεγραμμένο hash του μηνύματος χρησιμοποιώντας το συμμετρικό κλειδί και στέλνει ολόκληρο το πράγμα στον P.

Ο P μπορεί να λάβει το συμμετρικό κλειδί από το P2 επειδή έχει το ιδιωτικό κλειδί για την αποκρυπτογράφηση της κρυπτογράφησης.
Μόνο ο P μπορεί να αποκρυπτογραφήσει το συμμετρικά κρυπτογραφημένο μήνυμα και το υπογεγραμμένο κατακερματισμό επειδή έχει το συμμετρικό κλειδί.
Είναι σε θέση να επαληθεύσει ότι το μήνυμα δεν έχει αλλάξει επειδή μπορεί να υπολογίσει το hash του ληφθέντος μηνύματος και να το συγκρίνει με ένα ψηφιακά υπογεγραμμένο.
Ο P είναι επίσης σε θέση να αποδείξει στον εαυτό του ότι ο P2 ήταν ο αποστολέας, επειδή μόνο ο P2 μπορεί να υπογράψει τον κατακερματισμό έτσι ώστε να επαληθευτεί με το δημόσιο κλειδί P2.

3.10. Επίθεση Ηλεκτρονικού Ψαρέματος (Phishing και Spear Phishing)

Η επίθεση ηλεκτρονικού "ψαρέματος" είναι η πρακτική της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχονται από αξιόπιστες πηγές με στόχο την απόκτηση προσωπικών πληροφοριών ή την επιρροή των χρηστών να κάνουν κάτι. Συνδυάζει την κοινωνική μηχανική και την τεχνική απάτη. Θα μπορούσε να περιλαμβάνει ένα συνημμένο σε ένα email που φορτώνει κακόβουλο λογισμικό στον υπολογιστή. Θα μπορούσε επίσης να είναι ένας σύνδεσμος προς έναν παράνομο ιστότοπο έτσι ώστε ο χρήστης να κατεβάσει κακόβουλο λογισμικό ή να παραδώσει τα προσωπικά του στοιχεία.

Το spear phishing είναι ένας πολύ στοχευμένος τύπος δραστηριότητας phishing. Οι επιτιθέμενοι αφιερώνουν χρόνο για να πραγματοποιήσουν έρευνα σε στόχους και να δημιουργήσουν μηνύματα που είναι προσωπικά και σχετικά. Εξαιτίας αυτού, το ηλεκτρονικό ψάρεμα μπορεί να είναι πολύ δύσκολο να εντοπιστεί και ακόμη πιο δύσκολο για τον χρήστη να αμυνθεί. Ένας από τους απλούστερους τρόπους με τους οποίους ένας εισβολέας μπορεί να πραγματοποιήσει επίθεση spear phishing είναι η πλαστογράφηση ηλεκτρονικού ταχυδρομείου, κάνοντας τις πληροφορίες να φαίνονται σαν να προέρχονται από γνωστό αποστολέα. Μια άλλη τεχνική είναι η κλωνοποίηση

ιστότοπων για την εισαγωγή προσωπικών στοιχείων αναγνώρισης (PII) ή διαπιστευτηρίων σύνδεσης.

Τεχνικές για τη μείωση του κινδύνου ψαρέματος:

- Κριτική σκέψη

3.11. Επίθεση σε Κωδικό Πρόσβασης

Επειδή οι κωδικοί πρόσβασης είναι ο πιο συχνά χρησιμοποιούμενος μηχανισμός για τον έλεγχο ταυτότητας των χρηστών σε ένα σύστημα πληροφοριών, η απόκτηση κωδικών πρόσβασης είναι μια κοινή και αποτελεσματική προσέγγιση επίθεσης. Μπορεί κάποιος να αποκτήσει πρόσβαση στον κωδικό πρόσβασης ενός ατόμου κοιτάζοντας γύρω από το γραφείο του ατόμου, κάνοντας «sniffing» στη σύνδεση με το δίκτυο για να αποκτήσει μη κρυπτογραφημένους κωδικούς πρόσβασης, χρησιμοποιώντας την κοινωνική μηχανική, μπορεί να αποκτήσει πρόσβαση σε μια βάση δεδομένων κωδικών πρόσβασης ή να μαντέψει τον κωδικό πρόσβασης. Η τελευταία προσέγγιση μπορεί να γίνει είτε με τυχαίο είτε με συστηματικό τρόπο:

- Η εικασία κωδικού πρόσβασης με βίαιο τρόπο σημαίνει χρήση τυχαίας προσέγγισης δοκιμάζοντας διαφορετικούς κωδικούς πρόσβασης που σχετίζονται με το όνομα του ατόμου, τον τίτλο εργασίας, τα χόμπι ή παρόμοια αντικείμενα.

- Σε μια επίθεση λεξικού, ένα λεξικό κοινών κωδικών πρόσβασης χρησιμοποιείται για την απόπειρα πρόσβασης στον υπολογιστή και στο δίκτυο ενός χρήστη. Μια προσέγγιση είναι η αντιγραφή ένός κρυπτογραφημένου αρχείου που περιέχει τους κωδικούς πρόσβασης, να εφαρμοστεί η ίδια κρυπτογράφηση σε ένα λεξικό των κοινώς χρησιμοποιούμενων κωδικών πρόσβασης και να γίνει σύγκριση των αποτελεσμάτων.

Για την προστασία από επιθέσεις λεξικού ή βίαιης επίθεσης, πρέπει να εφαρμοστεί μια πολιτική κλειδώματος λογαριασμού που θα κλειδώνει τον λογαριασμό μετά από μερικές άκυρες προσπάθειες εισόδου με κωδικό πρόσβασης. (Melnick, 2020)

3.12. Επίθεση SQL Injection

Η SQL injection έχει γίνει ένα κοινό πρόβλημα σε ιστότοπους που βασίζονται σε βάση δεδομένων. Εμφανίζεται όταν εκτελείται ένα ερώτημα SQL στη βάση δεδομένων μέσω των δεδομένων εισαγωγής από τον χρήστη στον διακομιστή. Οι εντολές SQL εισάγονται στην είσοδο επιπέδου δεδομένων για την εκτέλεση προκαθορισμένων εντολών SQL.

Μια επιτυχημένη εκμετάλλευση SQL injection μπορεί να διαβάσει ευαίσθητα δεδομένα από τη βάση δεδομένων, να τροποποιήσει με εισαγωγή, ενημέρωση ή διαγραφή δεδομένων βάσης δεδομένων, να εκτελέσει λειτουργίες διαχείρισης όπως τερματισμός λειτουργίας στη βάση δεδομένων, να ανακτήσει το περιεχόμενο ενός δεδομένου αρχείου και, σε ορισμένες περιπτώσεις, εκδίδει εντολές στο λειτουργικό σύστημα.

Για παράδειγμα, μια φόρμα ιστού σε έναν ιστότοπο ενδέχεται να ζητήσει το όνομα λογαριασμού ενός χρήστη και, στη συνέχεια, να τη στείλει στη βάση δεδομένων για να συγκεντρώσει τις σχετικές πληροφορίες λογαριασμού χρησιμοποιώντας δυναμική SQL όπως αυτή:

"SELECT * FROM users WHERE account =" "+ userProvidedAccountNumber +" ";"

Ενώ αυτό λειτουργεί για χρήστες που εισάγουν σωστά τον αριθμό λογαριασμού τους, αφήνει ένα κενό για τους εισβολείς. Για παράδειγμα, αν κάποιος αποφάσισε να παράσχει έναν αριθμό λογαριασμού "" ή "1" = "1" ", αυτό θα είχε ως αποτέλεσμα μια σειρά ερωτημάτων:

“SELECT * FROM users WHERE account = ‘’ or ‘1’ = ‘1’;”

Επειδή το «1» = «1» αξιολογείται πάντα σε TRUE, η βάση δεδομένων θα επιστρέφει τα δεδομένα για όλους τους χρήστες αντί για έναν μόνο χρήστη.

Η ευπάθεια σε αυτόν τον τύπο επίθεσης ασφάλειας στον κυβερνοχώρο εξαρτάται από το γεγονός ότι η SQL δεν κάνει πραγματική διάκριση μεταξύ των επιπέδων ελέγχου

και δεδομένων. Επομένως, οι SQL injectios λειτουργούν κυρίως εάν ένας ιστότοπος χρησιμοποιεί δυναμική SQL. Επιπλέον, η SQL injection είναι πολύ συχνή στις εφαρμογές PHP και ASP λόγω της επικράτησης παλαιότερων λειτουργικών διεπαφών. Οι εφαρμογές J2EE και ASP.NET είναι λιγότερο πιθανό να έχουν εκμεταλλευτεί εύκολα τις SQL injections λόγω της φύσης των διαθέσιμων προγραμματικών διεπαφών.

Για την προστασία από επιθέσεις SQL injection, πρέπει να εφαρμοστεί το μοντέλο ελάχιστων δικαιωμάτων (PoLP) στις βάσεις δεδομένων, οι διαδικασίες δε θα πρέπει να περιλαμβάνουν δυναμική SQL παραμετροποιημένα ερωτήματα. Ο κώδικας που εκτελείται στη βάση δεδομένων πρέπει να είναι αρκετά ισχυρός για να αποτρέπονται οι επιθέσεις με injection. Επιπλέον, πρέπει να επικυρώνονται τα δεδομένα εισαγωγής σε μια λευκή λίστα σε επίπεδο εφαρμογής.

3.13. Επίθεση Διασταυρούμενου Σεναρίου (XSS)

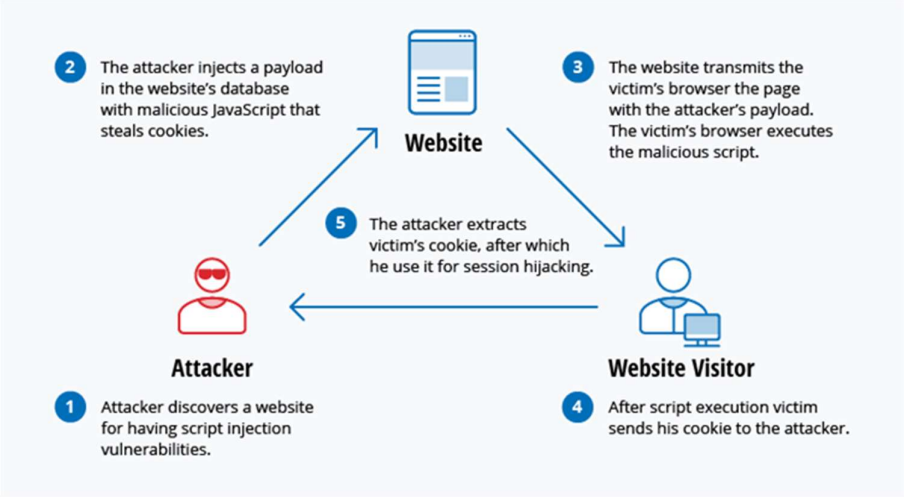
Οι επιθέσεις XSS χρησιμοποιούν πόρους ιστού τρίτων για την εκτέλεση σεναρίων στο πρόγραμμα περιήγησης ιστού του θύματος ή σε εφαρμογή με δυνατότητα δέσμης ενεργειών. Συγκεκριμένα, ο εισβολέας εισάγει ωφέλιμο φορτίο με κακόβουλη JavaScript στη βάση δεδομένων ενός ιστότοπου. Όταν το θύμα ζητά μια σελίδα από τον ιστότοπο, ο ιστότοπος μεταδίδει τη σελίδα, με το ωφέλιμο φορτίο του εισβολέα ως μέρος του σώματος HTML στο πρόγραμμα περιήγησης του θύματος, το οποίο εκτελεί το κακόβουλο σενάριο.

Για παράδειγμα, ενδέχεται να στείλει το cookie του θύματος στον διακομιστή του εισβολέα και ο εισβολέας μπορεί να το εξαγάγει και να το χρησιμοποιήσει για παραβίαση συνεδρίας. Οι πιο επικίνδυνες συνέπειες συμβαίνουν όταν το XSS χρησιμοποιείται για την εκμετάλλευση πρόσθετων τρωτών σημείων. Αυτές οι ευπάθειες μπορούν να επιτρέψουν σε έναν εισβολέα να μην κλέψει μόνο cookie, αλλά και να καταγράψει κτυπήματα πλήκτρων, να τραβήξει στιγμιότυπα οθόνης, να ανακαλύψει και να συλλέξει πληροφορίες δικτύου και να αποκτήσει πρόσβαση και να ελέγξει από απόσταση τη μηχανή του θύματος.

Ενώ το XSS μπορεί να επωφεληθεί μέσα σε VBScript, ActiveX και Flash, η πιο διαδεδομένη κατάχρηση είναι αυτή της JavaScript - κυρίως επειδή η JavaScript υποστηρίζεται ευρέως στον ιστό.

Για την προστασία από τις επιθέσεις XSS, οι προγραμματιστές μπορούν να ελέγχουν την εισαγωγή δεδομένων από χρήστες σε ένα αίτημα HTTP. Όλα τα δεδομένα πρέπει να έχουν επικυρωθεί, φιλτραριστεί ή διαγραφεί πριν επιστραφεί οτιδήποτε στον χρήστη, όπως οι τιμές των παραμέτρων ερωτήματος κατά τη διάρκεια των αναζητήσεων. Πρέπει να μετατραπούν οι ειδικοί χαρακτήρες όπως?, &, /, <,> και κενά διαστήματα στα αντίστοιχα κωδικοποιημένα HTML ή URL αντίστοιχα.

Εικόνα 3: Επίθεση XSS



3.14. Ανακάλυψη Πολιτικής Κωδικού Πρόσβασης

Οι πολιτικές κωδικού πρόσβασης για δίκτυα είναι ένας τρόπος επιβολής σύνθετων κωδικών πρόσβασης που είναι δύσκολο να σπάσουν μέσω του Brute Force. Ένας αντίπαλος μπορεί να επιχειρήσει να αποκτήσει πρόσβαση σε λεπτομερείς πληροφορίες σχετικά με την πολιτική κωδικού πρόσβασης που χρησιμοποιείται σε ένα εταιρικό δίκτυο. Αυτό θα βοηθούσε τον αντίπαλο να δημιουργήσει μια λίστα κοινών κωδικών πρόσβασης και να ξεκινήσει επιθέσεις λεξικού ή Brute Force που συμμορφώνεται με την πολιτική.

Οι πολιτικές κωδικού πρόσβασης μπορούν να οριστούν και να ανακαλυφθούν σε συστήματα Windows, Linux και macOS.

Windows

- net accounts
- net accounts/domain

Linux

- cat /etc/pam.d/common-password
- macOS
- pwpolicy getaccountpolicies

3.15. Επίθεση Γενεθλίων

Οι επιθέσεις γενεθλίων γίνονται εναντίον αλγορίθμων κατακερματισμού που χρησιμοποιούνται για την επαλήθευση της ακεραιότητας ενός μηνύματος, λογισμικού ή ψηφιακής υπογραφής. Ένα μήνυμα που υποβάλλεται σε επεξεργασία από μια συνάρτηση κατακερματισμού παράγει μια σύνοψη μηνυματος (MD: Message Digest) σταθερού μήκους, ανεξάρτητα από το μήκος του μηνύματος εισόδου. Αυτή η MD χαρακτηρίζει μοναδικά το μήνυμα.

Η επίθεση γενεθλίων αναφέρεται στην πιθανότητα εύρεσης δύο τυχαίων μηνυμάτων που δημιουργούν την ίδια MD όταν υποβάλλονται σε επεξεργασία από μια συνάρτηση κατακερματισμού. Εάν ένας εισβολέας υπολογίσει την ίδια MD για το μήνυμά του με το χρήστη, μπορεί να αντικαταστήσει με ασφάλεια το μήνυμα του χρήστη με το δικό του και ο δέκτης δεν θα μπορεί να εντοπίσει την αντικατάσταση, ακόμη και αν συγκρίνει την MD. (Melnick, 2020)

3.16. Επίθεση από Κακόβουλο Λογισμικό

Το κακόβουλο λογισμικό μπορεί να περιγραφεί ως ανεπιθύμητο λογισμικό που είναι εγκατεστημένο σε ένα σύστημα χωρίς τη συγκατάθεσή του χρήστη. Μπορεί να προσκολληθεί σε νόμιμο κώδικα και να διαδωθεί. Μπορεί να παραμείνει σε χρήσιμες εφαρμογές ή να αναπαραχθεί στο Διαδίκτυο. Ακολουθούν ορισμένοι από τους πιο συνηθισμένους τύπους κακόβουλου λογισμικού

3.16.1. Ιοί Μακροεντολής

Αυτοί οι ιοί μολύνουν εφαρμογές όπως το Microsoft Word ή το Excel. Οι ιοί μακροεντολής συνδέονται με την ακολουθία αρχικοποίησης μιας εφαρμογής. Όταν ανοίγει η εφαρμογή, ο ιός εκτελεί οδηγίες πριν μεταφέρει τον έλεγχο στην εφαρμογή. Ο ιός αναπαράγεται και προσκολλάται σε άλλο κώδικα στο σύστημα του υπολογιστή.

3.16.2. Ιοί που μολύνουν τα Αρχεία

Οι ιοί που μολύνουν αρχεία συνήθως συνδέονται με εκτελέσιμο κώδικα, όπως αρχεία .exe. Ο ιός εγκαθίσταται όταν φορτώνεται ο κωδικός. Μια άλλη έκδοση ενός αρχείου που μολύνει συσχετίζεται με ένα αρχείο δημιουργώντας ένα αρχείο ιού με το ίδιο όνομα, αλλά μια επέκταση .exe. Επομένως, όταν ανοίξει το αρχείο, θα εκτελεστεί ο κώδικας ιού.

3.16.3. Ιοί που μολύνουν Συστήματα ή Εκκίνησης – Εντολής

Ένας ιός εγγραφής εκκίνησης συνδέεται με την κύρια εγγραφή εκκίνησης σε σκληρούς δίσκους. Όταν ξεκινήσει το σύστημα, θα κοιτάξει τον τομέα εκκίνησης και θα φορτώσει τον ιό στη μνήμη, όπου μπορεί να εξαπλωθεί σε άλλους δίσκους και υπολογιστές.

3.16.4. Πολυμορφικοί Ιοί

Αυτοί οι ιοί κρύβονται μέσα από διάφορους κύκλους κρυπτογράφησης και αποκρυπτογράφησης. Ο κρυπτογραφημένος ιός και μια σχετική μηχανή μετάλλαξης αποκρυπτογραφούνται αρχικά από ένα πρόγραμμα αποκρυπτογράφησης. Ο ιός προχωρά στη μόλυνση μιας περιοχής κώδικα. Η μηχανή μετάλλαξης στη συνέχεια

αναπτύσσει μια νέα ρουτίνα αποκρυπτογράφησης και ο ιός κρυπτογραφεί τη μηχανή μετάλλαξης και ένα αντίγραφο του ιού με έναν αλγόριθμο που αντιστοιχεί στη νέα ρουτίνα αποκρυπτογράφησης. Το κρυπτογραφημένο πακέτο μηχανής μετάλλαξης και ιού επισυνάπτεται σε νέο κώδικα και η διαδικασία επαναλαμβάνεται. Τέτοιοι ιοί είναι δύσκολο να εντοπιστούν αλλά έχουν υψηλό επίπεδο εντροπίας λόγω των πολλών τροποποιήσεων του πηγαίου κώδικα τους. Τα λογισμικά προστασίας από ιούς μπορούν να χρησιμοποιήσουν αυτήν τη δυνατότητα για να τα εντοπίσουν.

3.16.5. Ιοί Stealth

Οι ιοί Stealth καταλαμβάνουν τις λειτουργίες του συστήματος για να κρυφτούν. Το κάνουν αυτό διακυβεύοντας την ομαλή λειτουργία του λογισμικού εντοπισμού κακόβουλου λογισμικού, έτσι ώστε το λογισμικό να αναφέρει ότι μια μολυσμένη περιοχή δεν έχει μολυνθεί. Αυτοί οι ιοί αποκρύπτουν οποιαδήποτε αύξηση στο μέγεθος ενός μολυσμένου αρχείου ή αλλαγές στην ημερομηνία και την ώρα της τελευταίας τροποποίησης του αρχείου.

3.16.6. Trojans

Ένα Trojan ή Trojan Horse είναι ένα πρόγραμμα που κρύβεται σε ένα χρήσιμο πρόγραμμα και συνήθως έχει μια κακόβουλη λειτουργία. Μια σημαντική διαφορά μεταξύ ιών και Trojans είναι ότι οι Trojans δεν αυτοαντιγραφούνται. Εκτός από την έναρξη επιθέσεων σε ένα σύστημα, ένας Trojan μπορεί να δημιουργήσει μια πίσω πόρτα που μπορεί να αξιοποιηθεί από επιτιθέμενους. Για παράδειγμα, ένας Trojan μπορεί να προγραμματιστεί για να ανοίξει μια θύρα μεγάλου αριθμού, ώστε ο hacker να μπορεί να τη χρησιμοποιήσει για να ακούσει και στη συνέχεια να εκτελέσει μια επίθεση. (Melnick, 2020)

3.16.7. Λογικές Βόμβες

Μια λογική βόμβα είναι ένας τύπος κακόβουλου λογισμικού που προσαρτάται σε μια εφαρμογή και ενεργοποιείται από ένα συγκεκριμένο περιστατικό, όπως μια λογική συνθήκη ή μια συγκεκριμένη ημερομηνία και ώρα.

3.16.8. Worms

Τα worms διαφέρουν από τους ιούς στο ότι δεν συνδέονται σε ένα host αρχείο, αλλά είναι αυτόνομα προγράμματα που διαδίδονται σε δίκτυα και υπολογιστές. Τα worms εξαπλώνονται συνήθως μέσω συνημμένων email. Το άνοιγμα του προσαρτήματος ενεργοποιεί το πρόγραμμα worm. Ένα τυπικό worm εκμετάλλευσης περιλαμβάνει το worm που στέλνει ένα αντίγραφο του εαυτού του σε κάθε επαφή στη διεύθυνση email ενός μολυσμένου υπολογιστή. Εκτός από τη διεξαγωγή κακόβουλων δραστηριοτήτων, ένα worm που διαδίδεται στο Διαδίκτυο και υπερφορτώνει τους διακομιστές email μπορεί να οδηγήσει σε επιθέσεις άρνησης υπηρεσίας κατά κόμβων σε το δίκτυο.

3.16.9. Droppers

Το dropper είναι ένα πρόγραμμα που χρησιμοποιείται για την εγκατάσταση ιών σε υπολογιστές. Σε πολλές περιπτώσεις, το dropper δεν είναι δυνατό να εντοπιστεί από το λογισμικό σάρωσης ιών. Ένα dropper μπορεί επίσης να συνδεθεί στο Διαδίκτυο και να κατεβάσει ενημερώσεις σε λογισμικό ιών που βρίσκεται σε ένα παραβιασμένο σύστημα.

3.16.10. Ransomware

Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που αποκλείει την πρόσβαση στα δεδομένα του θύματος και απειλεί να τα δημοσιεύσει ή να τα διαγράψει, εκτός εάν πληρώσει λύτρα. Ενώ κάποιο απλό ransomware υπολογιστή μπορεί να κλειδώσει το σύστημα με τρόπο που δεν είναι δύσκολο να αντιστρέψει ένας έμπειρος χρήστης, το πιο προηγμένο κακόβουλο λογισμικό χρησιμοποιεί μια τεχνική που ονομάζεται κρυπτοϊικός εκβιασμός, ο οποίος κρυπτογραφεί τα αρχεία του θύματος με τρόπο που καθιστά σχεδόν αδύνατο να ανακτηθούν χωρίς κλειδί αποκρυπτογράφησης.

3.16.11. Adware

Το Adware είναι μια εφαρμογή λογισμικού που χρησιμοποιείται από εταιρείες για σκοπούς μάρκετινγκ, με διαφημιστικά μπάνερ να εμφανίζονται κατά τη διάρκεια που οποιουδήποτε πρόγραμμα εκτελείται. Το Adware μπορεί να ληφθεί αυτόματα σε ένα

σύστημα κατά την περιήγηση σε οποιονδήποτε ιστότοπο και μπορεί να προβληθεί μέσω αναδυόμενων παραθύρων ή μέσω μιας μπάρας που εμφανίζεται αυτόματα στην οθόνη του υπολογιστή.

3.16.12. Spyware

Το λογισμικό υποκλοπής spyware είναι ένας τύπος προγράμματος που εγκαθίσταται για τη συλλογή πληροφοριών σχετικά με τους χρήστες, τους υπολογιστές τους ή τις συνήθειες περιήγησής τους. Παρακολουθεί ό,τι κάνει ο χρήστης χωρίς να γίνεται αντιληπτό και στέλνει τα δεδομένα σε έναν απομακρυσμένο χρήστη. Μπορεί επίσης να κατεβάσει και να εγκαταστήσει άλλα κακόβουλα προγράμματα από το Διαδίκτυο. Το λογισμικό υποκλοπής spyware λειτουργεί όπως το adware, αλλά είναι συνήθως ένα ξεχωριστό πρόγραμμα που εγκαθίσταται εν αγνοία του χρήστη όταν εγκαθίσταται άλλη εφαρμογή δωρεάν λογισμικού.

(Melnick, 2020)

3.17. Αντιμετώπιση επιθέσεων

Η επίτευξη καλής άμυνας απαιτεί κατανόηση της επίθεσης. Τα μέτρα για τον μετριασμό αυτών των απειλών ποικίλλουν, αλλά τα βασικά στοιχεία ασφαλείας παραμένουν τα ίδια:

- Διαρκής ενημέρωση των συστημάτων και των βάσεων δεδομένων των anti-virus
- Τείχος προστασίας ώστε να επιτρέπει στη λίστα επιτρεπόμενων μόνο συγκεκριμένες θύρες και hosts
- Χρήση μοντέλου με λιγότερα προνόμια στο περιβάλλον IT
- Τακτικά αντίγραφα ασφαλείας
- Έλεγχος των συστημάτων IT για ύποπτη δραστηριότητα.
- Εκπαίδευση χρηστών
- Διατήρηση ισχυρών κωδικών

Κεφάλαιο 4: ΚΑΤΗΓΟΡΙΕΣ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΕΞΑΡΤΩΜΕΝΕΣ ΑΠΟ ΤΟΝ ΑΝΘΡΩΠΙΝΟ ΠΑΡΑΓΟΝΤΑ

Για ορισμένες κατηγορίες κυβερνοεπιθέσεων, οι οποίες αναλύονται παρακάτω, ο πιο σημαντικός παράγοντας προστασίας από αυτές είναι η συμπεριφορά των χρηστών.

4.1. Drive-by Επίθεση

Αναφερόμαστε σε Drive-by κίνδυνο όταν ένας αντίπαλος αποκτά πρόσβαση σε ένα σύστημα μέσω ενός χρήστη που επισκέπτεται έναν ιστότοπο κατά τη διάρκεια της κανονικής πορείας περιήγησης. Με αυτήν την τεχνική, το πρόγραμμα περιήγησης ιστού του χρήστη είναι συνήθως στοχευμένο για εκμετάλλευση, αλλά οι αντίπαλοι μπορούν επίσης να χρησιμοποιούν παραβιασμένους ιστότοπους για απόκτηση διακριτικών πρόσβασης σε εφαρμογές.

Υπάρχουν πολλοί τρόποι παράδοσης κώδικα εκμετάλλευσης σε ένα πρόγραμμα περιήγησης, όπως:

- Ένας νόμιμος ιστότοπος διακυβεύεται όπου οι αντίπαλοι έχουν εισάγει κάποια μορφή κακόβουλου κώδικα όπως το JavaScript, το iFrames και scripts μεταξύ ιστότοπων.
- Οι κακόβουλες διαφημίσεις προβάλλονται μέσω νόμιμων παρόχων διαφημίσεων.
- Οι ενσωματωμένες διεπαφές εφαρμογών ιστού αξιοποιούνται για την εισαγωγή οποιουδήποτε άλλου είδους αντικειμένου που μπορεί να χρησιμοποιηθεί για την προβολή περιεχομένου ιστού ή περιέχει ένα script που εκτελείται στον επισκέπτη (π.χ. δημοσιεύσεις φόρουμ, σχόλια και άλλο περιεχόμενο ιστού που ελέγχεται από τον χρήστη).

Συχνά ο ιστότοπος που χρησιμοποιείται από έναν αντίπαλο επισκέπτεται από μια συγκεκριμένη κοινότητα, όπως η κυβέρνηση, μια συγκεκριμένη βιομηχανία ή μια περιοχή, όπου ο στόχος είναι η επίθεση σε ένα συγκεκριμένο χρήστη ή σύνολο

χρηστών με βάση ένα κοινό ενδιαφέρον. Αυτό το είδος στοχευμένης επίθεσης αναφέρεται σε μια στρατηγική επίθεση ιστού ή επίθεση τρύπα watering hole.
Τυπική διαδικασία Drive-by επίθεσης:

- Ένας χρήστης επισκέπτεται έναν ιστότοπο που χρησιμοποιείται για τη φιλοξενία του ελεγχόμενου από τον αντίπαλο περιεχομένου.
- Τα σενάρια εκτελούνται αυτόματα, αναζητώντας συνήθως εκδόσεις του προγράμματος περιήγησης και προσθήκες για μια πιθανώς ευάλωτη έκδοση.
- Ο χρήστης μπορεί να χρειαστεί να βοηθήσει σε αυτήν τη διαδικασία ενεργοποιώντας scripting ή ενεργά στοιχεία του ιστότοπου και αγνοώντας τα πλαίσια διαλόγου προειδοποίησης.
- Με την εύρεση μιας ευάλωτης έκδοσης, ο κώδικας εκμετάλλευσης παραδίδεται στο πρόγραμμα περιήγησης.
- Εάν η εκμετάλλευση είναι επιτυχής, τότε θα δώσει την εκτέλεση κώδικα του αντιπάλου στο σύστημα του χρήστη, εκτός εάν υπάρχουν άλλες προστασίες.
- Σε ορισμένες περιπτώσεις απαιτείται δεύτερη επίσκεψη στον ιστότοπο μετά την αρχική σάρωση πριν από την παράδοση του κώδικα εκμετάλλευσης.

Σε αντίθεση με την εφαρμογή εκμετάλλευσης Public-Facing, το επίκεντρο αυτής της τεχνικής είναι η εκμετάλλευση λογισμικού σε τελικό σημείο πελάτη κατά την επίσκεψη σε έναν ιστότοπο. Αυτό συνήθως παρέχει σε έναν αντίπαλο πρόσβαση σε συστήματα στο εσωτερικό δίκτυο αντί για εξωτερικά συστήματα που ενδέχεται να βρίσκονται σε DMZ.

Οι αντίπαλοι μπορούν επίσης να χρησιμοποιούν παραβιασμένους ιστότοπους για να παραδώσουν σε έναν χρήστη μια κακόβουλη εφαρμογή που έχει σχεδιαστεί για την Κλοπή Διακριτικών Πρόσβασης Εφαρμογών, όπως τα διακριτικά OAuth, για να αποκτήσουν πρόσβαση σε προστατευμένες εφαρμογές και πληροφορίες. Αυτές οι κακόβουλες εφαρμογές έχουν παραδοθεί μέσω αναδυόμενων παραθύρων σε νόμιμους ιστότοπους. (ATT&CK, 2020)

4.2. Συνημμένο Spearphishing

Το συνημμένο spearphishing είναι μια ειδική παραλλαγή του spearphishing. Το συνημμένο spearphishing είναι διαφορετικό από άλλες μορφές spearphishing, δεδομένου ότι χρησιμοποιεί τη χρήση κακόβουλου λογισμικού που επισυνάπτεται σε ένα email. Όλες οι μορφές spearphishing παραδίδονται ηλεκτρονικά και στοχεύουν σε ένα συγκεκριμένο άτομο, εταιρεία ή κλάδο. Σε αυτό το σενάριο, οι αντίπαλοι επισυνάπτουν ένα αρχείο στο email spearphishing και συνήθως βασίζονται στην εκτέλεση χρήστη.

Υπάρχουν πολλές επιλογές για το συνημμένο, όπως έγγραφα του Microsoft Office, εκτελέσιμα αρχεία, PDF ή αρχειοθετημένα αρχεία. Με το άνοιγμα του συνημμένου, το ωφέλιμο φορτίο του αντιπάλου εκμεταλλεύεται μια ευπάθεια ή εκτελείται απευθείας στο σύστημα του χρήστη. Το κείμενο του email spearphishing συνήθως προσπαθεί να δώσει έναν εύλογο λόγο για τον οποίο ο χρήστης πρέπει να ανοίξει το αρχείο και μπορεί επιπλέον να εξηγήσει πώς να παρακάμψει τις προστασίες του συστήματος για να μπορέσει να ανοίξει το αρχείο. Το ηλεκτρονικό ταχυδρομείο μπορεί επίσης να περιέχει οδηγίες σχετικά με τον τρόπο αποκρυπτογράφησης ενός συνημμένου, όπως έναν κωδικό πρόσβασης αρχείου zip, προκειμένου να αποφύγει τα όρια προστασίας του email. Οι αντίπαλοι χειρίζονται συχνά επεκτάσεις αρχείων και εικονίδια για να κάνουν τα συνημμένα εκτελέσιμα αρχεία να φαίνονται αρχεία εγγράφων.

4.3. Σύνδεσμος Spearphishing

Το spearphishing με σύνδεσμο είναι μια συγκεκριμένη παραλλαγή του spearphishing. Είναι διαφορετικό από άλλες μορφές spearphishing στο ότι χρησιμοποιεί τη χρήση συνδέσμων για τη λήψη κακόβουλου λογισμικού που περιέχεται σε email, αντί να επισυνάπτει κακόβουλα αρχεία στο ίδιο το email, για να αποφευχθούν άμυνες που ενδέχεται να ελέγχουν συνημμένα email.

Όλες οι μορφές spearphishing παραδίδονται ηλεκτρονικά και στοχεύουν σε ένα συγκεκριμένο άτομο, εταιρεία ή κλάδο. Σε αυτήν την περίπτωση, τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου περιέχουν συνδέσμους. Γενικά, οι σύνδεσμοι

θα συνοδεύονται από κείμενο κοινωνικής μηχανικής και απαιτούν από τον χρήστη να κάνει ενεργό κλικ ή αντιγραφή και επικόλληση μιας διεύθυνσης URL σε ένα πρόγραμμα περιήγησης, αξιοποιώντας την εκτέλεση χρήστη. Ο ιστότοπος που επισκέπτεται ο χρήστης ενδέχεται να θέσει σε κίνδυνο το πρόγραμμα περιήγησης ιστού χρησιμοποιώντας ένα exploit, ή θα ζητηθεί από τον χρήστη να πραγματοποιήσει λήψη εφαρμογών, εγγράφων, αρχείων zip ή ακόμη και εκτελέσιμων, ανάλογα με το πρόσχημα του email. Μπορεί επίσης να περιλαμβάνουν συνδέσμους που προορίζονται να αλληλεπιδράσουν απευθείας με έναν αναγνώστη email, συμπεριλαμβανομένων ενσωματωμένων εικόνων που προορίζονται να εκμεταλλευτούν άμεσα το τελικό σύστημα ή να επαληθεύσουν τη λήψη ενός μηνύματος ηλεκτρονικού ταχυδρομείου (δηλ. Σφάλματα ιστού / web beacons).

Οι σύνδεσμοι ενδέχεται επίσης να κατευθύνουν τους χρήστες σε κακόβουλες εφαρμογές που έχουν σχεδιαστεί για την Κλοπή Διακριτικών Πρόσβασης Εφαρμογών, όπως τα διακριτικά OAuth, προκειμένου να αποκτήσουν πρόσβαση σε προστατευμένες εφαρμογές και πληροφορίες.

4.4. Spearphishing μέσω Υπηρεσίας

Το Spearphishing μέσω υπηρεσίας είναι μια συγκεκριμένη παραλλαγή του spearphishing. Διαφέρει από άλλες μορφές spearphishing στο ότι εκμεταλλεύεται τη χρήση υπηρεσιών τρίτων και όχι τα εταιρικά κανάλια email.

Όλες οι μορφές spearphishing παραδίδονται ηλεκτρονικά και στοχεύουν σε ένα συγκεκριμένο άτομο, εταιρεία ή κλάδο. Σε αυτό το σενάριο, οι αντίπαλοι στέλνουν μηνύματα μέσω διαφόρων υπηρεσιών κοινωνικών μέσων, προσωπικού email μέσω web και άλλων μη ελεγχόμενων από επιχειρήσεις υπηρεσιών. Αυτές οι υπηρεσίες είναι πιο πιθανό να έχουν μια λιγότερο αυστηρή πολιτική ασφάλειας από μια επιχείρηση. Όπως συμβαίνει με τα περισσότερα είδη spearphishing, ο στόχος είναι να δημιουργηθεί σχέση με τον στόχο ή να επιτευχθεί το ενδιαφέρον του στόχου με κάποιο τρόπο. Οι αντίπαλοι θα δημιουργήσουν ψεύτικους λογαριασμούς κοινωνικών μέσων και θα στέλνουν μηνύματα στους υπαλλήλους για πιθανές ευκαιρίες εργασίας. Ο αντίπαλος μπορεί στη συνέχεια να στείλει κακόβουλους συνδέσμους ή συνημμένα μέσω αυτών των υπηρεσιών.

Ένα κοινό παράδειγμα είναι η δημιουργία σχέσης με έναν στόχο μέσω των κοινωνικών μέσων και, στη συνέχεια, η αποστολή περιεχομένου σε μια προσωπική υπηρεσία webmail που χρησιμοποιεί ο στόχος στον υπολογιστή εργασίας τους. Αυτό επιτρέπει σε έναν αντίπαλο να παρακάμψει ορισμένους περιορισμούς email στον λογαριασμό εργασίας και ο στόχος είναι πιο πιθανό να ανοίξει το αρχείο, καθώς είναι κάτι που περίμενε. Εάν το ωφέλιμο φορτίο δεν λειτουργεί όπως αναμένεται, ο αντίπαλος μπορεί να συνεχίσει τις κανονικές επικοινωνίες και να αντιμετωπίσει προβλήματα με τον στόχο έτσι ώστε να λειτουργήσει. (ATT&CK, 2020)

4.5. Third-party Software

Third-party εφαρμογές και συστήματα ανάπτυξης λογισμικού ενδέχεται να χρησιμοποιούνται στο περιβάλλον δικτύου για σκοπούς διαχείρισης (π.χ. SCCM, VNC, HBSS, Altiris κ.λπ.). Εάν ένας αντίπαλος αποκτήσει πρόσβαση σε αυτά τα συστήματα, τότε μπορεί να είναι σε θέση να εκτελέσει κώδικα.

Οι εχθροί ενδέχεται να αποκτήσουν πρόσβαση και να χρησιμοποιούν συστήματα τρίτων που είναι εγκατεστημένα σε ένα εταιρικό δίκτυο, όπως συστήματα διαχείρισης, παρακολούθησης και ανάπτυξης, καθώς και πύλες τρίτων και διακομιστές άλματος που χρησιμοποιούνται για τη διαχείριση άλλων συστημάτων. Η πρόσβαση σε ένα third-party σύστημα λογισμικού ή σε εταιρικό επίπεδο ενδέχεται να επιτρέψει σε έναν αντίπαλο να εκτελέσει απομακρυσμένη εκτέλεση κώδικα σε όλα τα συστήματα που είναι συνδεδεμένα σε ένα τέτοιο σύστημα. Η πρόσβαση μπορεί να χρησιμοποιηθεί για να μετακινηθεί πλευρικά σε άλλα συστήματα, να συλλέξει πληροφορίες ή να προκαλέσει ένα συγκεκριμένο αποτέλεσμα.

Τα δικαιώματα που απαιτούνται για αυτήν την ενέργεια διαφέρουν ανάλογα με τη διαμόρφωση του συστήματος. Τοπικά διαπιστευτήρια μπορεί να είναι επαρκή με άμεση πρόσβαση στο σύστημα τρίτων, ή ενδέχεται να απαιτούνται συγκεκριμένα διαπιστευτήρια τομέα. Ωστόσο, το σύστημα ενδέχεται να απαιτεί λογαριασμό διαχειριστή για να συνδεθεί ή να εκτελέσει τον επιδιωκόμενο σκοπό.

4.6. Εκτέλεση Χρήστη

Ένας αντίπαλος μπορεί να βασίζεται σε συγκεκριμένες ενέργειες ενός χρήστη για να επιτύχει την εκτέλεση. Αυτό μπορεί να είναι άμεση εκτέλεση κώδικα, όπως όταν ένας χρήστης ανοίγει ένα κακόβουλο εκτελέσιμο που παραδίδεται μέσω του Συνημμένου Spearphishing με το εικονίδιο και την εμφανή επέκταση ενός αρχείου εγγράφου. Μπορεί επίσης να οδηγήσει σε άλλες τεχνικές εκτέλεσης, όπως όταν ένας χρήστης κάνει κλικ σε έναν σύνδεσμο που παραδίδεται μέσω του Συνδέσμου Spearphishing που οδηγεί σε εκμετάλλευση ενός προγράμματος περιήγησης ή μιας ευπάθειας εφαρμογών μέσω της εκμετάλλευσης για εκτέλεση πελάτη. Οι συνομιλητές ενδέχεται να χρησιμοποιούν διάφορους τύπους αρχείων που απαιτούν από τον χρήστη να τα εκτελέσει, συμπεριλαμβανομένων των .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif και .cpl.

Για παράδειγμα, ένας αντίπαλος μπορεί να οπλίζει τα αρχεία συντόμευσης των Windows (.lnk) για να κάνει το χρήστη να κάνει κλικ για να εκτελέσει το κακόβουλο ωφέλιμο φορτίο. Ένα κακόβουλο αρχείο .lnk ενδέχεται να περιέχει εντολές PowerShell. Τα ωφέλιμα φορτία μπορούν να συμπεριληφθούν στο ίδιο το αρχείο .lnk ή να ληφθούν από έναν απομακρυσμένο διακομιστή.

Ενώ η εκτέλεση χρήστη εμφανίζεται συχνά λίγο μετά την αρχική πρόσβαση, μπορεί να συμβεί σε άλλες φάσεις μιας εισβολής, όπως όταν ένας αντίπαλος τοποθετεί ένα αρχείο σε κοινόχρηστο κατάλογο ή στην επιφάνεια εργασίας ενός χρήστη, έτσι ώστε ο χρήστης να κάνει κλικ σε αυτό.

4.7. Επεκτάσεις Προγράμματος Περιήγησης

Οι επεκτάσεις προγράμματος περιήγησης ή τα πρόσθετα είναι μικρά προγράμματα που μπορούν να προσθέσουν λειτουργικότητα και να προσαρμόσουν πτυχές των προγραμμάτων περιήγησης στο Διαδίκτυο. Μπορούν να εγκατασταθούν απευθείας ή μέσω ενός καταστήματος εφαρμογών προγράμματος περιήγησης. Οι επεκτάσεις έχουν γενικά πρόσβαση και δικαιώματα σε οτιδήποτε έχει πρόσβαση στο πρόγραμμα περιήγησης.

Κακόβουλες επεκτάσεις μπορούν να εγκατασταθούν σε ένα πρόγραμμα περιήγησης μέσω κακόβουλων λήψεων στο κατάστημα εφαρμογών που μεταμφιέζονται ως νόμιμες επεκτάσεις, μέσω κοινωνικής μηχανικής ή από έναν αντίπαλο που έχει ήδη θέσει σε κίνδυνο ένα σύστημα. Η ασφάλεια μπορεί να περιοριστεί στα καταστήματα εφαρμογών του προγράμματος περιήγησης, οπότε ενδέχεται να μην είναι δύσκολο για κακόβουλες επεκτάσεις να νικήσουν τους αυτοματοποιημένους σαρωτές και να μεταφορτωθούν. Μόλις εγκατασταθεί η επέκταση, μπορεί να περιηγηθεί σε ιστότοπους στο παρασκήνιο, να κλέψει όλες τις πληροφορίες που ένας χρήστης εισάγει σε ένα πρόγραμμα περιήγησης, για να συμπεριλάβει διαπιστευτήρια, και να χρησιμοποιηθεί ως πρόγραμμα εγκατάστασης για RAT.

4.8. Στοιχείο Σύνδεσης

Το MacOS παρέχει την επιλογή καταχώρισης συγκεκριμένων εφαρμογών για εκτέλεση όταν ένας χρήστης συνδέεται. Αυτές οι εφαρμογές εκτελούνται κάτω από το συνδεδεμένο περιβάλλον χρήστη και θα ξεκινούν κάθε φορά που ο χρήστης συνδέεται.

Τα στοιχεία σύνδεσης που εγκαθίστανται χρησιμοποιώντας το Service Management Framework δεν είναι ορατά στις Προτιμήσεις συστήματος και μπορούν να καταργηθούν μόνο από την εφαρμογή που τις δημιούργησε. Οι χρήστες έχουν άμεσο έλεγχο στα στοιχεία σύνδεσης που έχουν εγκατασταθεί χρησιμοποιώντας μια κοινόχρηστη λίστα αρχείων που είναι επίσης ορατά στις Προτιμήσεις συστήματος. Αυτά τα στοιχεία σύνδεσης αποθηκεύονται στον κατάλογο ~ / Library / Preferences / του χρήστη σε ένα αρχείο plist που ονομάζεται com.apple.loginitems.plist. Ορισμένες από αυτές τις εφαρμογές μπορούν να ανοίξουν ορατά παράθυρα διαλόγου στον χρήστη, αλλά δεν είναι όλα απαραίτητα, καθώς υπάρχει η επιλογή "Απόκρυψη" του παραθύρου.

Εάν ένας αντίπαλος μπορεί να εγγράψει το δικό του στοιχείο σύνδεσης ή να τροποποιήσει ένα υπάρχον, τότε μπορεί να το χρησιμοποιήσει για να εκτελέσει τον κωδικό του για έναν μηχανισμό επιμονής κάθε φορά που ο χρήστης συνδέεται. Η μέθοδος API SMLoginItemSetEnabled μπορεί να χρησιμοποιηθεί για τον ορισμό

στοιχείων σύνδεσης, αλλά και γλώσσες δέσμης ενεργειών όπως το AppleScript μπορούν να το κάνουν και αυτό.

4.9. Εκ νέου άνοιγμα Εφαρμογών

Οι χρήστες μπορούν να καθορίσουν ορισμένες εφαρμογές που θα ανοίξουν ξανά όταν ένας χρήστης επανεκκινήσει τον υπολογιστή τους. Παρόλο που αυτό γίνεται συνήθως μέσω γραφικού περιβάλλοντος εργασίας χρήστη (GUI) σε βάση app-by-app, υπάρχουν αρχεία λίστας ιδιοτήτων (plist) που περιέχουν αυτές τις πληροφορίες και βρίσκονται επίσης στο ~ / Library / Preferences / com.apple.loginwindow. plist και ~ / Library / Preferences / ByHost / com.apple.loginwindow. * .plist.

Ένας αντίπαλος μπορεί να τροποποιήσει ένα από αυτά τα αρχεία απευθείας για να συμπεριλάβει έναν σύνδεσμο προς το κακόβουλο εκτελέσιμο πρόγραμμα για να παρέχει έναν μηχανισμό επιμονής κάθε φορά που ο χρήστης κάνει επανεκκίνηση του υπολογιστή του. (ATT&CK, 2020)

4.10. Template Injection

Η προδιαγραφή Open Office XML (OOXML) της Microsoft ορίζει μια μορφή που βασίζεται σε XML για έγγραφα του Office (.docx, xlsx, .pptx) για την αντικατάσταση παλαιότερων δυαδικών μορφών (.doc, .xls, .ppt). Τα αρχεία OOXML είναι συσκευασμένα μαζί με αρχεία ZIP που διακυβεύονται από διάφορα αρχεία XML, που αναφέρονται ως μέρη, που περιέχουν ιδιότητες που καθορίζουν συλλογικά τον τρόπο απόδοσης ενός εγγράφου.

Οι ιδιότητες εντός τμημάτων ενδέχεται να αναφέρονται σε κοινόχρηστους δημόσιους πόρους που έχουν πρόσβαση μέσω διαδικτυακών διευθύνσεων URL. Για παράδειγμα, οι ιδιότητες προτύπου αναφέρονται σε ένα αρχείο, το οποίο χρησιμεύει ως

προσχηματισμένο σχεδιάγραμμα εγγράφου, το οποίο ανακτάται κατά τη φόρτωση του εγγράφου.

Οι αντίπαλοι ενδέχεται να κάνουν κατάχρηση αυτής της τεχνολογίας για να αποκρύψουν αρχικά τον κακόβουλο κώδικα που θα εκτελεστεί μέσω εγγράφων (δηλ. Σενάρια). Οι αναφορές προτύπων που εισάγονται σε ένα έγγραφο ενδέχεται να επιτρέψουν την ανάκτηση και την εκτέλεση κακόβουλων φορτίων κατά τη φόρτωση του εγγράφου. Αυτά τα έγγραφα μπορούν να παραδοθούν μέσω άλλων τεχνικών όπως το Συνημμένο Spearphishing ή και το Taint Shared Content και ενδέχεται να αποφύγουν τις στατικές ανιχνεύσεις, καθώς δεν υπάρχουν τυπικοί δείκτες (μακροεντολή VBA, σενάριο κ.λπ.) έως ότου ληφθεί το κακόβουλο φορτίο.

Αυτή η τεχνική μπορεί επίσης να ενεργοποιήσει τον εξαναγκασμένο έλεγχο ταυτότητας με την εισαγωγή ενός SMB / HTTPS (ή άλλης προτροπής διαπιστευτηρίων) URL και ενεργοποιώντας μια προσπάθεια ελέγχου ταυτότητας.

4.11. Απόρριψη Διαπιστευτηρίων

Η απόρριψη διαπιστευτηρίων είναι η διαδικασία απόκτησης πληροφοριών σύνδεσης και κωδικού πρόσβασης λογαριασμού, συνήθως με τη μορφή κατακερματισμένου ή σε μορφή καθαρού κειμένου κωδικού πρόσβασης, από το λειτουργικό σύστημα και το λογισμικό. Τα διαπιστευτήρια μπορούν στη συνέχεια να χρησιμοποιηθούν για την εκτέλεση της Lateral Movement και την πρόσβαση σε περιορισμένες πληροφορίες.

Πολλά από τα εργαλεία που αναφέρονται σε αυτήν την τεχνική μπορούν να χρησιμοποιηθούν τόσο από τους αντιπάλους όσο και από τους επαγγελματίες ελεγκτές ασφάλειας. Πιθανότατα υπάρχουν και πρόσθετα προσαρμοσμένα εργαλεία.

4.11.1. Windows

4.11.1.1. SAM

Το SAM (Διαχείριση λογαριασμών ασφαλείας- Security Accounts Manager) είναι ένα αρχείο βάσης δεδομένων που περιέχει τοπικούς λογαριασμούς για τον κεντρικό υπολογιστή, συνήθως αυτοί που βρίσκονται με την εντολή «καθαρός χρήστης». Για την απαρίθμηση της βάσης δεδομένων SAM, απαιτείται πρόσβαση σε επίπεδο συστήματος. Μπορούν να χρησιμοποιηθούν διάφορα εργαλεία για την ανάκτηση του αρχείου SAM μέσω τεχνικών στη μνήμη:

- pwdumpx.exe
- gsecdump
- Mimikatz
- secretdump.py

Εναλλακτικά, το SAM μπορεί να εξαχθεί από το Μητρώο με Reg:

- reg save HKLM \ sam sam
- reg save HKLM \ system system

Το Creddump7 μπορεί στη συνέχεια να χρησιμοποιηθεί για την τοπική επεξεργασία της βάσης δεδομένων SAM για την ανάκτηση κατακερματισμού.

Ο λογαριασμός Rid 500 είναι ο τοπικός, ενσωματωμένος διαχειριστής. Το Rid 501 είναι ο λογαριασμός επισκέπτη. Οι λογαριασμοί χρηστών ξεκινούν με RID 1.000+.

4.11.1.2. Προσωρινά Διαπιστευτήρια

Ο κατακερματισμός DCC2 (Domain Cached Credentials version 2), που χρησιμοποιείται από τα Windows Vista και νεότερα διαπιστευτήρια προσωρινής αποθήκευσης όταν ο ελεγκτής τομέα δεν είναι διαθέσιμος. Ο αριθμός των προεπιλεγμένων προσωρινά αποθηκευμένων διαπιστευτηρίων ποικίλλει και αυτός ο αριθμός μπορεί να αλλάξει ανά σύστημα. Αυτός ο κατακερματισμός δεν επιτρέπει

επιθέσεις τύπου pass-the-hash. Μπορούν να χρησιμοποιηθούν διάφορα εργαλεία για την ανάκτηση του αρχείου SAM μέσω τεχνικών στη μνήμη.

- pwdumpx.exe
- gsecdump
- Mimikatz

Εναλλακτικά, το reg.exe μπορεί να χρησιμοποιηθεί για εξαγωγή από το μητρώο και το Creddump7 που χρησιμοποιείται για τη συλλογή των διαπιστευτηρίων.

Τα προσωρινά αποθηκευμένα διαπιστευτήρια για τα Windows Vista προέρχονται χρησιμοποιώντας το PBKDF2.

4.11.1.3. Μυστικά της Τοπικής Αρχής Ασφαλείας(LSA)

Με την πρόσβαση SYSTEM σε έναν κεντρικό υπολογιστή, τα μυστικά LSA επιτρέπουν συχνά ασήμαντη πρόσβαση από έναν τοπικό λογαριασμό σε διαπιστευτήρια λογαριασμού βάσει τομέα. Το Μητρώο χρησιμοποιείται για την αποθήκευση των μυστικών LSA. Όταν οι υπηρεσίες εκτελούνται στο πλαίσιο τοπικών χρηστών ή τομέων, οι κωδικοί πρόσβασης αποθηκεύονται στο Μητρώο. Εάν είναι ενεργοποιημένη η αυτόματη σύνδεση, αυτές οι πληροφορίες θα αποθηκευτούν και στο μητρώο. Μπορούν να χρησιμοποιηθούν διάφορα εργαλεία για την ανάκτηση του αρχείου SAM μέσω τεχνικών στη μνήμη.

- pwdumpx.exe
- gsecdump
- Mimikatz
- secretdump.py

Εναλλακτικά, το reg.exe μπορεί να χρησιμοποιηθεί για εξαγωγή από το μητρώο και το Creddump7 που χρησιμοποιείται για τη συλλογή των διαπιστευτηρίων.

Οι κωδικοί πρόσβασης που εξάγονται από τον μηχανισμό του είναι κωδικοποιημένοι UTF-16, πράγμα που σημαίνει ότι επιστρέφονται σε απλό κείμενο. Τα Windows 10 προσθέτουν προστασίες για τα μυστικά LSA που περιγράφονται στο Mitigation.

4.11.1.4. NTDS από τον ελεγκτή τομέα

Η υπηρεσία καταλόγου Active Directory αποθηκεύει πληροφορίες σχετικά με τα μέλη του τομέα, συμπεριλαμβανομένων συσκευών και χρηστών, για την επαλήθευση διαπιστευτηρίων και τον ορισμό των δικαιωμάτων πρόσβασης. Η βάση δεδομένων τομέα της υπηρεσίας καταλόγου Active Directory αποθηκεύεται στο αρχείο NTDS.dit. Από προεπιλογή, το αρχείο NTDS θα βρίσκεται στο% SystemRoot% \ NTDS \ Ntds.dit ενός ελεγκτή τομέα.

Τα ακόλουθα εργαλεία και τεχνικές μπορούν να χρησιμοποιηθούν για την απαρίθμηση του αρχείου NTDS και ολόκληρων των περιεχομένων κατακερματισμού της υπηρεσίας καταλόγου Active Directory.

- Volume Shadow Copy
- secretdump.py
- Χρήση του ενσωματωμένου εργαλείου των Windows, ntdsutil.exe
- Invoke-NinjaCopy

4.11.1.5. Αρχεία Προτιμήσεων Πολιτικής Ομάδας (GPP – Group Policy Preferences Files)

Οι προτιμήσεις πολιτικής ομάδας (GPP) είναι εργαλεία που επιτρέπουν στους διαχειριστές να δημιουργούν πολιτικές τομέα με ενσωματωμένα διαπιστευτήρια. Αυτές οι πολιτικές, μεταξύ άλλων, επιτρέπουν στους διαχειριστές να ορίζουν τοπικούς λογαριασμούς.

Αυτές οι πολιτικές ομάδας αποθηκεύονται στο SYSVOL σε έναν ελεγκτή τομέα, αυτό σημαίνει ότι οποιοσδήποτε χρήστης τομέα μπορεί να δει το κοινόχρηστο SYSVOL και

να αποκρυπτογραφήσει τον κωδικό πρόσβασης εάν το ιδιωτικό κλειδί AES διαρρεύσει on-line.

Τα ακόλουθα εργαλεία και σενάρια μπορούν να χρησιμοποιηθούν για τη συλλογή και την αποκρυπτογράφηση του αρχείου κωδικού πρόσβασης από Preference Policy Group αρχεία XML:

- Ενότητα μετά την εκμετάλλευση του Metasploit: "post / windows / collect / διαπιστευτήρια / gpp"
- Get-GPPPassword
- gpprefdecrypt.py

Στο κοινόχρηστο στοιχείο SYSVOL, μπορούν να χρησιμοποιηθούν τα ακόλουθα για την απαρίθμηση πιθανών αρχείων XML.dir / s * .xml

- Κύρια ονόματα υπηρεσίας (SPN)
- Διαπιστευτήρια Plaintext

Αφού ένας χρήστης συνδεθεί σε ένα σύστημα, μια ποικιλία διαπιστευτηρίων δημιουργείται και αποθηκεύεται στη διαδικασία τοπικής αρχής υπηρεσίας υποσυστήματος (LSASS- Local Security Authority Subsystem Service) στη μνήμη. Αυτά τα διαπιστευτήρια μπορούν να συλλεχθούν από διαχειριστή χρήστη ή το σύστημα.

4.11.1.6. SSPI

Το SSPI (Security Support Provider Interface) λειτουργεί ως κοινή διεπαφή σε αρκετούς παρόχους υποστήριξης ασφαλείας (SSP): Ένας πάροχος υποστήριξης ασφαλείας είναι μια βιβλιοθήκη δυναμικής σύνδεσης (DLL) που καθιστά ένα ή περισσότερα πακέτα ασφαλείας διαθέσιμα σε εφαρμογές.

Τα ακόλουθα SSP μπορούν να χρησιμοποιηθούν για πρόσβαση σε διαπιστευτήρια:

- MSV: Τα διαδραστικά στοιχεία σύνδεσης, οι παρτίδες και οι υπηρεσίες σύνδεσης πραγματοποιούνται μέσω του πακέτου ελέγχου ταυτότητας MSV.
- Digigest: Το πρωτόκολλο ελέγχου ταυτότητας Digest έχει σχεδιαστεί για χρήση με ανταλλαγές Hypertext Transfer Protocol (HTTP) και Simple Authentication Security Layer (SASL).
- Kerberos: Προτιμάται για έλεγχο ταυτότητας τομέα αμοιβαίου πελάτη-διακομιστή στα Windows 2000 και μεταγενέστερα.
- CredSSP: Παρέχει έλεγχο ταυτότητας σε επίπεδο SSO και δικτύου για Remote Desktop Services.

Τα ακόλουθα εργαλεία μπορούν να χρησιμοποιηθούν για την απαρίθμηση διαπιστευτηρίων:

- Windows Credential Editor
- Mimikatz

Εκτός από τις τεχνικές στη μνήμη, η μνήμη διεργασίας LSASS μπορεί να απορριφθεί από τον κεντρικό υπολογιστή προορισμού και να αναλυθεί σε ένα τοπικό σύστημα.

Για παράδειγμα, στον κεντρικό υπολογιστή προορισμού χρησιμοποιείται το procdump:

- procdump -ma lsass.exe lsass_dump

Τοπικά, το mimikatz μπορεί να εκτελεστεί:

- sekurlsa :: Minidump lsassdump.dmp
- sekurlsa :: logonPasswords

4.11.1.7. DCSync

Το DCSync είναι μια παραλλαγή στο dumping διαπιστευτηρίων που μπορεί να χρησιμοποιηθεί για την απόκτηση ευαίσθητων πληροφοριών από έναν ελεγκτή τομέα. Αντί να εκτελεί αναγνωρίσιμο κακόβουλο κώδικα, η ενέργεια λειτουργεί καταχρώντας τη διεπαφή προγραμματισμού εφαρμογών του ελεγκτή τομέα (API-Application Programming Interface) για να προσομοιώσει τη διαδικασία αναπαραγωγής από έναν απομακρυσμένο ελεγκτή τομέα.

Οποιαδήποτε μέλη των διαχειριστών, των διαχειριστών τομέα, των εταιρικών ομάδων διαχειριστών ή των λογαριασμών υπολογιστών στον ελεγκτή τομέα μπορούν να εκτελέσουν το DCSync για να τραβήξουν δεδομένα κωδικού πρόσβασης από την υπηρεσία καταλόγου Active Directory, τα οποία ενδέχεται να περιλαμβάνουν τρέχοντες και ιστορικούς κατακερματισμούς δυνητικά χρήσιμων λογαριασμών, όπως KRBTGT και Διαχειριστών. Οι κατακερματισμοί μπορούν με τη σειρά τους να χρησιμοποιηθούν για να δημιουργήσουν ένα Golden Ticket για χρήση στο Pass the Ticket ή να αλλάξουν τον κωδικό πρόσβασης ενός λογαριασμού όπως σημειώνεται στη Διαχείριση λογαριασμού.

Η λειτουργία DCSync συμπεριλήφθηκε στη μονάδα "lsadump" στο Mimikatz. Το Lsadump περιλαμβάνει επίσης το NetSync, το οποίο εκτελεί DCSync μέσω ενός παλαιού πρωτοκόλλου αναπαραγωγής.

4.11.2. Linux

4.11.2.1. Σύστημα Αρχείων Proc

Το σύστημα αρχείων proc στο Linux περιέχει πολλές πληροφορίες σχετικά με την κατάσταση του τρέχοντος λειτουργικού συστήματος. Οι διαδικασίες που εκτελούνται με δικαιώματα root μπορούν να χρησιμοποιήσουν αυτήν τη δυνατότητα για να αποκόψουν τη ζωντανή μνήμη άλλων προγραμμάτων που εκτελούνται. Εάν οποιοδήποτε από αυτά τα προγράμματα αποθηκεύει κωδικούς πρόσβασης σε καθαρό κείμενο ή κατακερματισμό κωδικού πρόσβασης στη μνήμη, αυτές οι τιμές μπορούν στη συνέχεια να συλλεχθούν είτε για χρήση είτε για βίαιες επιθέσεις, αντίστοιχα. Αυτή η λειτουργικότητα έχει εφαρμοστεί στο MimiPenguin, ένα εργαλείο ανοιχτού κώδικα

εμπνευσμένο από το Mimikatz. Το εργαλείο αυτό σβήνει τη μνήμη διεργασίας και, στη συνέχεια, συλλέγει κωδικούς πρόσβασης και κατακερματισμούς αναζητώντας συμβολοσειρές κειμένου και μοτίβα regex για το πώς δεδομένες εφαρμογές όπως το Gnome Keyring, το sshd και το Apache χρησιμοποιούν μνήμη για να αποθηκεύουν τέτοια αντικείμενα ελέγχου ταυτότητας. (ATT&CK, 2020)

4.12. Διαπιστευτήρια σε Αρχεία

Οι αντίπαλοι μπορούν να αναζητούν τοπικά συστήματα αρχείων και απομακρυσμένες κοινοποιήσεις αρχείων για αρχεία που περιέχουν κωδικούς πρόσβασης. Αυτά μπορεί να είναι αρχεία που δημιουργούνται από χρήστες για να αποθηκεύουν τα δικά τους διαπιστευτήρια, κοινόχρηστα διαπιστευτήρια για μια ομάδα ατόμων, αρχεία διαμόρφωσης που περιέχουν κωδικούς πρόσβασης για ένα σύστημα, υπηρεσία, πηγαίο κώδικα ή δυαδικά αρχεία που περιέχουν ενσωματωμένους κωδικούς πρόσβασης.

Είναι δυνατή η εξαγωγή κωδικών πρόσβασης από αντίγραφα ασφαλείας ή αποθηκευμένων εικονικών μηχανών μέσω του Dumping Διαπιστευτηρίων. Οι κωδικοί πρόσβασης μπορούν επίσης να ληφθούν από το Group Policy Preferences που είναι αποθηκευμένες στον Windows Domain Controller.

Σε περιβάλλοντα cloud, τα διαπιστευτήρια χρήστη που έχουν επικυρωθεί αποθηκεύονται συχνά σε τοπικά αρχεία διαμόρφωσης και διαπιστευτηρίων. Σε ορισμένες περιπτώσεις, αυτά τα αρχεία μπορούν να αντιγραφούν και να επαναχρησιμοποιηθούν σε άλλο μηχάνημα ή τα περιεχόμενα μπορούν να διαβαστούν και στη συνέχεια να χρησιμοποιηθούν για έλεγχο ταυτότητας χωρίς να χρειάζεται να αντιγραφούν αρχεία.

4.13. Εξαναγκαστική Πιστοποίηση

Το SMB (Server Message Block) χρησιμοποιείται συνήθως σε δίκτυα Windows για έλεγχο ταυτότητας και επικοινωνία μεταξύ συστημάτων για πρόσβαση σε πόρους και κοινή χρήση αρχείων. Όταν ένα σύστημα Windows προσπαθεί να συνδεθεί σε έναν πόρο SMB, θα επιχειρήσει αυτόματα να πραγματοποιήσει έλεγχο ταυτότητας και να στείλει πληροφορίες διαπιστευτηρίου για τον τρέχοντα χρήστη στο απομακρυσμένο σύστημα. Αυτή η συμπεριφορά είναι χαρακτηριστική σε εταιρικά περιβάλλοντα, έτσι ώστε οι χρήστες να μην χρειάζεται να εισάγουν διαπιστευτήρια για πρόσβαση σε πόρους δικτύου. Το Web Distributed Authoring and Versioning (WebDAV) χρησιμοποιείται συνήθως από τα συστήματα Windows ως εφεδρικό πρωτόκολλο όταν το SMB είναι αποκλεισμένο ή αποτύχει. Το WebDAV είναι μια επέκταση του HTTP και συνήθως λειτουργεί σε θύρες TCP 80 και 443.

Οι αντίπαλοι ενδέχεται να επωφεληθούν από αυτήν τη συμπεριφορά για να αποκτήσουν πρόσβαση σε κατακερματισμούς λογαριασμού χρήστη μέσω εξαναγκαστικής πιστοποίησης SMB. Ένας αντίπαλος μπορεί να στείλει ένα συνημμένο σε έναν χρήστη μέσω spearphishing που περιέχει έναν σύνδεσμο πόρων σε έναν εξωτερικό διακομιστή που ελέγχεται από τον αντίπαλο (π.χ. Template Injection), ή να τοποθετήσει ένα ειδικά κατασκευασμένο αρχείο στη διαδρομή πλοήγησης για προνομιακούς λογαριασμούς (π.χ. αρχείο .SFF τοποθετημένο στην επιφάνεια εργασίας) ή ανοιχτό στο κοινό αρχείο για πρόσβαση από θύματα. Όταν το σύστημα του χρήστη αποκτήσει πρόσβαση στον μη αξιόπιστο πόρο, θα επιχειρήσει έλεγχο ταυτότητας και θα στείλει πληροφορίες, συμπεριλαμβανομένων των διαπιστευτηρίων κατακερματισμού του χρήστη μέσω SMB στον διακομιστή που ελέγχεται από τον αντίπαλο. Με την πρόσβαση στον κατακερματισμό διαπιστευτηρίων, ένας αντίπαλος μπορεί να εκτελέσει Brute Force cracking εκτός σύνδεσης για να αποκτήσει πρόσβαση σε διαπιστευτήρια απλού κειμένου.

Υπάρχουν διάφοροι τρόποι με τους οποίους μπορεί να συμβεί αυτό. Ορισμένες ιδιαιτερότητες από την άγρια χρήση περιλαμβάνουν:

- Ένα συνημμένο spearphishing που περιέχει ένα έγγραφο με έναν πόρο που φορτώνεται αυτόματα όταν ανοίγει το έγγραφο. Το έγγραφο μπορεί να περιλαμβάνει, για παράδειγμα, ένα αίτημα παρόμοιο με το file[:]//[remote address]/Normal.dotm για ενεργοποίηση του αιτήματος SMB.

- Ένα τροποποιημένο αρχείο .LNK ή .SCF με το όνομα αρχείου εικονιδίου που δείχνει μια εξωτερική αναφορά όπως \[remote address]\pic.png που θα αναγκάσει το σύστημα να φορτώσει τον πόρο όταν το εικονίδιο αποδίδεται για την επανηλλημένη συλλογή διαπιστευτηρίων. (ATT&CK, 2020)

4.14. Προτροπή Εισαγωγής – Input

Όταν εκτελούνται προγράμματα που χρειάζονται πρόσθετα δικαιώματα από αυτά που υπάρχουν στο τρέχον περιβάλλον χρήστη, είναι σύνηθες για το λειτουργικό σύστημα να ζητά από τον χρήστη κατάλληλα διαπιστευτήρια για να εξουσιοδοτήσει τα αυξημένα δικαιώματα για την εργασία, όπως παράκαμψη ελέγχου λογαριασμού χρήστη.

Οι αντίπαλοι ενδέχεται να μιμούνται αυτήν τη λειτουργία για να ζητούν από τους χρήστες διαπιστευτήρια με μια φαινομενικά νόμιμη προτροπή και μιμούνται την κανονική χρήση, όπως ένα ψεύτικο πρόγραμμα εγκατάστασης που απαιτεί πρόσθετη πρόσβαση ή μια πλαστή ακολουθία ενεργειών κατάργησης κακόβουλου λογισμικού. Αυτός ο τύπος προτροπής μπορεί να χρησιμοποιηθεί για τη συλλογή διαπιστευτηρίων μέσω διαφόρων γλωσσών όπως το AppleScript και το PowerShell.

4.15. Kerberoasting

Τα SPNs (Service principal names) χρησιμοποιούνται για τον μοναδικό προσδιορισμό κάθε παρουσίας μιας υπηρεσίας των Windows. Για να ενεργοποιηθεί ο έλεγχος ταυτότητας, η Kerberos απαιτεί τα SPN να συσχετίζονται με τουλάχιστον έναν λογαριασμό σύνδεσης στην υπηρεσία.

Οι αντίπαλοι που διαθέτουν ένα έγκυρο εισιτήριο εκχώρησης εισιτηρίων Kerberos (TGT- ticket-granting ticket) μπορούν να ζητήσουν ένα ή περισσότερα εισιτήρια υπηρεσίας παροχής υπηρεσιών Kerberos (TGS) για οποιοδήποτε SPN από έναν

ελεγκτή τομέα (DC- domain controller). Τμήματα αυτών των εισιτηρίων μπορεί να είναι κρυπτογραφημένα με τον αλγόριθμο RC4, που σημαίνει ότι το Kerberos 5 TGS-REP etype 23 hash του λογαριασμού υπηρεσίας που σχετίζεται με το SPN χρησιμοποιείται ως ιδιωτικό κλειδί και επομένως είναι ευάλωτο σε offline Brute Force επιθέσεις που ενδέχεται να εκθέσουν διαπιστευτήρια απλού κειμένου.

Αυτή η ίδια επίθεση θα μπορούσε να εκτελεστεί χρησιμοποιώντας εισιτήρια υπηρεσίας που έχουν ληφθεί από την κίνηση του δικτύου.

Οι “σπασμένοι” κατακερματισμοί ενδέχεται να επιτρέψουν Persistence, Privilege Escalation, και Lateral Movement μέσω πρόσβασης σε έγκυρους λογαριασμούς.

4.16. Keychain

Τα Keychains είναι ο ενσωματωμένος τρόπος για το macOS να παρακολουθεί τους κωδικούς πρόσβασης και τα διαπιστευτήρια των χρηστών για πολλές υπηρεσίες και λειτουργίες όπως κωδικούς πρόσβασης WiFi, ιστότοπους, ασφαλείς σημειώσεις, πιστοποιητικά και Kerberos. Τα αρχεία Keychain βρίσκονται στο ~ / Library / Keychains /, / Library / Keychains / και / Network / Library / Keychains /.

Το βοηθητικό πρόγραμμα γραμμής εντολών ασφαλείας, το οποίο είναι ενσωματωμένο σε macOS από προεπιλογή, παρέχει έναν χρήσιμο τρόπο διαχείρισης αυτών των διαπιστευτηρίων.

Για να διαχειριστούν τα διαπιστευτήριά τους, οι χρήστες πρέπει να χρησιμοποιούν πρόσθετα διαπιστευτήρια για να αποκτήσουν πρόσβαση στο Keychain τους. Εάν ένας αντίπαλος γνωρίζει τα διαπιστευτήρια για το Keychain σύνδεσης, τότε μπορεί να έχει πρόσβαση σε όλα τα άλλα διαπιστευτήρια που είναι αποθηκευμένα σε αυτό το “θησαυροφυλάκιο”. Από προεπιλογή, η φράση πρόσβασης για το keychain είναι τα διαπιστευτήρια σύνδεσης του χρήστη. (ATT&CK, 2020)

4.17. Ιδιωτικά κλειδιά

Τα ιδιωτικά κλειδιά κρυπτογράφησης και τα πιστοποιητικά χρησιμοποιούνται για έλεγχο ταυτότητας, κρυπτογράφηση / αποκρυπτογράφηση και ψηφιακές υπογραφές.

Οι αντίπαλοι ενδέχεται να συλλέγουν ιδιωτικά κλειδιά από παραβιασμένα συστήματα για χρήση στον έλεγχο ταυτότητας σε απομακρυσμένες υπηρεσίες όπως SSH ή για χρήση στην αποκρυπτογράφηση άλλων συλλεγόμενων αρχείων, όπως email. Οι κοινές επεκτάσεις αρχείου κλειδιού και πιστοποιητικών περιλαμβάνουν: .key, .pgp, .gpg, .ppk., .P12, .pem, .pfx, .cer, .p7b, .asc. Οι αντίπαλοι ενδέχεται επίσης να ψάχνουν σε κοινούς βασικούς καταλόγους, όπως ~ / .ssh για κλειδιά SSH σε συστήματα που βασίζονται σε nix ή C: \ Users (username) .ssh \ σε Windows.

Τα ιδιωτικά κλειδιά θα πρέπει να απαιτούν κωδικό πρόσβασης για τη λειτουργία, οπότε ένας αντίπαλος μπορεί επίσης να χρησιμοποιήσει την καταχώριση εισόδου για την πληκτρολόγηση ή την απόπειρα Brute Force της φράσης πρόσβασης σε κατάσταση εκτός σύνδεσης.

4.18. Κλοπή Web Session Cookie

Ένας αντίπαλος μπορεί να κλέψει cookies διαδικτυακής εφαρμογής ή υπηρεσίας και να τα χρησιμοποιήσει για να αποκτήσει πρόσβαση σε εφαρμογές ιστού ή υπηρεσίες Διαδικτύου ως επικυρωμένος χρήστης χωρίς να χρειάζεται διαπιστευτήρια. Οι εφαρμογές και οι υπηρεσίες Ιστού χρησιμοποιούν συχνά cookies συνεδρίας ως διακριτικό ελέγχου ταυτότητας μετά από έλεγχο ταυτότητας ενός χρήστη σε έναν ιστότοπο.

Τα cookies ισχύουν συχνά για μεγάλο χρονικό διάστημα, ακόμα και αν η διαδικτυακή εφαρμογή δεν χρησιμοποιείται ενεργά. Τα cookies μπορούν να βρεθούν σε δίσκο, στη μνήμη διεργασίας του προγράμματος περιήγησης και στην κυκλοφορία δικτύου σε απομακρυσμένα συστήματα. Επιπλέον, άλλες εφαρμογές στο μηχάνημα στόχων ενδέχεται να αποθηκεύουν ευαίσθητα cookies ελέγχου ταυτότητας στη μνήμη (π.χ.

εφαρμογές που κάνουν έλεγχο ταυτότητας σε υπηρεσίες cloud). Τα cookies συνεδρίας μπορούν να χρησιμοποιηθούν για παράκαμψη ορισμένων πρωτοκόλλων ελέγχου ταυτότητας πολλών παραγόντων.

Υπάρχουν πολλά παραδείγματα κακόβουλου λογισμικού που στοχεύουν σε cookies από προγράμματα περιήγησης ιστού στο τοπικό σύστημα. Υπάρχουν επίσης πλαίσια ανοιχτού κώδικα, όπως το Evilginx 2 και το Mauraena που μπορούν να συλλέξουν cookies συνεδρίας μέσω ενός διακομιστή μεσολάβησης man-in-the-middle που μπορεί να ρυθμιστεί από έναν αντίπαλο και να χρησιμοποιηθεί σε εκστρατείες ηλεκτρονικού ψαρέματος.

Αφού ένας αντίπαλος αποκτήσει ένα έγκυρο cookie, τότε μπορεί να πραγματοποιήσει μια τεχνική Web Session Cookie για να συνδεθεί στην αντίστοιχη εφαρμογή ιστού.

4.19. Παρακολούθηση Ελέγχου Ταυτότητας Δύο Παραγόντων

Συνιστάται η χρήση ελέγχου ταυτότητας δύο ή πολλών παραγόντων καθώς παρέχει υψηλότερο επίπεδο ασφάλειας από τα ονόματα χρηστών και τους κωδικούς πρόσβασης μόνο, αλλά οι οργανισμοί πρέπει να γνωρίζουν τεχνικές που θα μπορούσαν να χρησιμοποιηθούν για την παρακολούθηση και παράκαμψη αυτών των μηχανισμών ασφαλείας. Οι αντίπαλοι ενδέχεται να στοχεύουν μηχανισμούς ελέγχου ταυτότητας, όπως smart cards, για να αποκτήσουν πρόσβαση σε συστήματα, υπηρεσίες και πόρους δικτύου.

Εάν μια smart card χρησιμοποιείται για έλεγχο ταυτότητας δύο παραγόντων (2FA), τότε θα πρέπει να χρησιμοποιηθεί ένας keylogger για τη λήψη του κωδικού πρόσβασης που σχετίζεται με μια smart card κατά τη διάρκεια της κανονικής χρήσης. Με μια κάρτα που έχει εισαχθεί και πρόσβαση στον κωδικό πρόσβασης της έξυπνης κάρτας, ένας αντίπαλος μπορεί να συνδεθεί σε έναν πόρο δικτύου χρησιμοποιώντας το μολυσμένο σύστημα για να κάνει τον έλεγχο ταυτότητας με μεσολάβηση με το διακριτικό υλικού που έχει εισαχθεί.

Οι αντίπαλοι μπορούν επίσης να χρησιμοποιούν ένα keylogger για να στοχεύουν παρόμοια άλλα tokens υλικού, όπως το RSA SecurID. Η καταγραφή εισόδου διακριτικού, συμπεριλαμβανομένου του προσωπικού κωδικού αναγνώρισης ενός χρήστη, μπορεί να παρέχει προσωρινή πρόσβαση όπως επανάληψη του εφάπαξ κωδικού πρόσβασης μέχρι την επόμενη ανατροπή τιμής, καθώς και πιθανώς επιτρέποντας στους αντιπάλους να προβλέψουν αξιόπιστα μελλοντικές τιμές ελέγχου ταυτότητας, δεδομένης πρόσβασης στον αλγόριθμο, για τη δημιουργία συνημμένων προσωρινών κωδικών.

Άλλες μέθοδοι του 2FA μπορούν να υποκλαπούν και να χρησιμοποιηθούν από έναν αντίπαλο για έλεγχο ταυτότητας. Είναι σύνηθες να αποστέλλονται κωδικοί μιας χρήσης μέσω επικοινωνιών εκτός ζώνης (email, SMS). Εάν η συσκευή ή η υπηρεσία δεν είναι ασφαλής, τότε ενδέχεται να είναι ευάλωτη στην παρακολούθηση. Παρόλο που επικεντρώνονται κυρίως σε εγκληματίες στον κυβερνοχώρο, αυτοί οι μηχανισμοί ελέγχου ταυτότητας έχουν αποτελέσει στόχο προηγμένων φορέων. (ATT&CK, 2020)

4.20. Pass the hash

Το Pass the hash (PtH) είναι μια μέθοδος επικύρωσης ταυτότητας ως χρήστη χωρίς να υπάρχει πρόσβαση στον κωδικό πρόσβασης του χρήστη. Αυτή η μέθοδος παρακάμπτει τα τυπικά βήματα ελέγχου ταυτότητας που απαιτούν κωδικό πρόσβασης σε cleartext, μεταβαίνοντας απευθείας στο τμήμα ελέγχου ταυτότητας που χρησιμοποιεί τον κατακερματισμό κωδικού πρόσβασης.

Σε αυτήν την τεχνική, καταγράφονται έγκυροι κωδικοί κατακερματισμού για τον λογαριασμό που χρησιμοποιείται χρησιμοποιώντας μια τεχνική πρόσβασης διαπιστευτηρίου. Τα καταγεγραμμένα hash χρησιμοποιούνται με PtH για έλεγχο ταυτότητας ως ο χρήστης. Μόλις γίνει έλεγχος ταυτότητας, το PtH μπορεί να χρησιμοποιηθεί για την εκτέλεση ενεργειών σε τοπικά ή απομακρυσμένα συστήματα.

Τα Windows 7 και νεότερες εκδόσεις με KB2871997 απαιτούν έγκυρα διαπιστευτήρια domain user ή κατακερματισμούς διαχειριστή RID 500.

4.21. Pass the ticket

Το Pass the Ticket (PtT) είναι μια μέθοδος ελέγχου ταυτότητας σε ένα σύστημα χρησιμοποιώντας εισιτήρια Kerberos χωρίς να έχετε πρόσβαση στον κωδικό πρόσβασης ενός λογαριασμού. Ο έλεγχος ταυτότητας Kerberos μπορεί να χρησιμοποιηθεί ως το πρώτο βήμα για την πλευρική μετακίνηση σε ένα απομακρυσμένο σύστημα.

Σε αυτήν την τεχνική, τα έγκυρα εισιτήρια Kerberos για έγκυρους λογαριασμούς καταγράφονται από το Credential Dumping. Μπορούν να ληφθούν εισιτήρια υπηρεσίας ενός χρήστη ή εισιτήριο εκχώρησης εισιτηρίων (TGT-Ticket Granting Ticket), ανάλογα με το επίπεδο πρόσβασης. Ένα εισιτήριο υπηρεσίας επιτρέπει την πρόσβαση σε έναν συγκεκριμένο πόρο, ενώ ένα TGT μπορεί να χρησιμοποιηθεί για να ζητήσει εισιτήρια υπηρεσίας από την Υπηρεσία Εκχώρησης Εισιτηρίων (TGS-Ticket Granting Service) για πρόσβαση σε οποιονδήποτε πόρο στον οποίο ο χρήστης έχει δικαιώματα πρόσβασης.

Τα Silver Tickets μπορούν να ληφθούν για υπηρεσίες που χρησιμοποιούν το Kerberos ως μηχανισμό ελέγχου ταυτότητας και χρησιμοποιούνται για τη δημιουργία εισιτηρίων για πρόσβαση στον συγκεκριμένο πόρο και στο σύστημα που φιλοξενεί τον πόρο (π.χ. SharePoint).

Τα Golden Tickets μπορούν να αποκτηθούν για τον domain χρησιμοποιώντας τον λογαριασμό υπηρεσίας διανομής κλειδιών KRBTGT λογαριασμού NTLM hash, το οποίο επιτρέπει τη δημιουργία TGT για οποιονδήποτε λογαριασμό στην υπηρεσία καταλόγου Active Directory. (ATT&CK, 2020)

4.22. Παραβίαση SSH

Το Secure Shell (SSH) είναι ένα τυπικό μέσο απομακρυσμένης πρόσβασης σε συστήματα Linux και macOS. Επιτρέπει σε έναν χρήστη να συνδεθεί σε άλλο σύστημα μέσω ενός κρυπτογραφημένου tunnel, που συνήθως επικυρώνει μέσω κωδικού πρόσβασης, πιστοποιητικού ή της χρήσης ενός ασύμμετρου ζεύγους κλειδιών κρυπτογράφησης.

Προκειμένου να επιτύχουν Lateral Movement από έναν παραβιασμένο κεντρικό υπολογιστή, οι αντίπαλοι μπορούν να επωφεληθούν από σχέσεις εμπιστοσύνης που έχουν δημιουργηθεί με άλλα συστήματα μέσω ελέγχου ταυτότητας δημόσιου κλειδιού σε ενεργές συνεδρίες SSH, παραβιάζοντας μια υπάρχουσα σύνδεση με άλλο σύστημα. Αυτό μπορεί να συμβεί μέσω της επίθεσης στον ίδιο τον SSH agent μέσω πρόσβασης στην υποδοχή του agent. Εάν ένας αντίπαλος μπορεί να αποκτήσει πρόσβαση root, τότε η παραβίαση των συνεδριών SSH είναι πιθανότατα ασήμαντη. Η παραβίαση του SSH agent παρέχει επίσης πρόσβαση σε διαπιστευτήρια SSH.

Το SSH Hijacking διαφέρει από τη χρήση Απομακρυσμένων Υπηρεσιών επειδή εισέρχεται σε μια υπάρχουσα περίοδο λειτουργίας SSH αντί να δημιουργεί μια νέα περίοδο σύνδεσης με τη χρήση έγκυρων λογαριασμών.

4.23. Windows Admin Shares

Τα συστήματα των Windows έχουν κρυφά κοινόχρηστα δίκτυα που είναι προσβάσιμα μόνο στους διαχειριστές και παρέχουν τη δυνατότητα απομακρυσμένης αντιγραφής αρχείων και άλλων λειτουργιών διαχείρισης. Παραδείγματα κοινών στοιχείων δικτύου περιλαμβάνουν C$, ADMIN$ και IPC$.

Οι αντίπαλοι μπορούν να χρησιμοποιήσουν αυτήν την τεχνική σε συνδυασμό με έγκυρους λογαριασμούς σε επίπεδο διαχειριστή για να αποκτήσουν απομακρυσμένη πρόσβαση σε ένα δίκτυο μέσω μπλοκ μηνυμάτων διακομιστή (SMB - server message block) για να αλληλεπιδράσουν με συστήματα που χρησιμοποιούν κλήσεις απομακρυσμένης διαδικασίας (RPC), μεταφορά αρχείων και εκτέλεση μεταφοράς

δυαδικά αρχεία μέσω απομακρυσμένης εκτέλεσης. Παράδειγμα τεχνικών εκτέλεσης που βασίζονται σε επικυρωμένες περιόδους σύνδεσης μέσω SMB / RPC είναι τα Scheduled Task, Service Execution και Windows Management Instrumentation. Το Adversaries μπορεί επίσης να χρησιμοποιήσει κατακερματισμούς NTLM για πρόσβαση σε κοινόχρηστα στοιχεία διαχειριστή σε συστήματα με Pass the Hash και ορισμένα επίπεδα διαμόρφωσης και ενημέρωσης κώδικα.

Το βοηθητικό πρόγραμμα Net μπορεί να χρησιμοποιηθεί για σύνδεση σε κοινές χρήσεις Windows σε απομακρυσμένα συστήματα χρησιμοποιώντας εντολές net use με έγκυρα διαπιστευτήρια.

4.24. Δεδομένα από Αποθετήρια Πληροφοριών

Οι αντίπαλοι μπορούν να αξιοποιήσουν τα αποθετήρια πληροφοριών για να συλλέξουν πολύτιμες πληροφορίες. Τα αποθετήρια πληροφοριών είναι εργαλεία που επιτρέπουν την αποθήκευση πληροφοριών, συνήθως για τη διευκόλυνση της συνεργασίας ή της ανταλλαγής πληροφοριών μεταξύ των χρηστών και μπορούν να αποθηκεύσουν μια ευρεία ποικιλία δεδομένων που μπορούν να βοηθήσουν τους αντιπάλους σε περαιτέρω στόχους ή άμεση πρόσβαση στις πληροφορίες-στόχους.

Οι αντίπαλοι μπορούν επίσης να συλλέγουν πληροφορίες από κοινόχρηστα αποθετήρια αποθήκευσης που φιλοξενούνται σε υποδομές cloud ή σε εφαρμογές λογισμικού ως υπηρεσία (SaaS), καθώς ο χώρος αποθήκευσης είναι μία από τις πιο θεμελιώδεις απαιτήσεις για υπηρεσίες και συστήματα cloud.

Το παρακάτω είναι μια σύντομη λίστα παραδειγμάτων πληροφοριών που ενδέχεται να διατηρούν πιθανή αξία σε έναν αντίπαλο και μπορούν επίσης να βρεθούν σε ένα αποθετήριο πληροφοριών:

- Πολιτικές, διαδικασίες και πρότυπα
- Διαγράμματα φυσικού / λογικού δικτύου
- Διαγράμματα αρχιτεκτονικής συστήματος
- Τεκμηρίωση τεχνικού συστήματος
- Διαπιστευτήρια δοκιμής / ανάπτυξης
- Προγράμματα εργασίας / έργου
- Αποσπάσματα πηγαίου κώδικα
- Σύνδεσμοι με κοινόχρηστα δίκτυα και άλλους εσωτερικούς πόρους

Συγκεκριμένα κοινά αποθετήρια πληροφοριών περιλαμβάνουν:

4.24.1. Microsoft SharePoint

Βρέθηκε σε πολλά εταιρικά δίκτυα και συχνά χρησιμοποιείται για την αποθήκευση και την κοινοποίηση σημαντικών εγγράφων τεκμηρίωσης.

4.24.2. Atlassian Confluence

Το Confluence, το οποίο συχνά βρίσκεται σε αναπτυξιακά περιβάλλοντα παράλληλα με το Atlassian JIRA, χρησιμοποιείται γενικά για την αποθήκευση εγγράφων τεκμηρίωσης που σχετίζονται με το development.

4.24.3. Man in the Browser

Οι αντίπαλοι μπορεί να εκμεταλλευτούν τις ευπάθειες ασφαλείας και την εγγενή λειτουργικότητα στο λογισμικό του προγράμματος περιήγησης για να αλλάξουν το περιεχόμενο, να τροποποιήσουν τη συμπεριφορά και να παρακολουθήσει πληροφορίες ως μέρος διαφόρων ατόμων στις τεχνικές του προγράμματος περιήγησης.

Ένα συγκεκριμένο παράδειγμα είναι όταν ένας αντίπαλος εισάγει λογισμικό σε ένα πρόγραμμα περιήγησης που τους επιτρέπει να κληρονομήσουν cookie, περιόδους σύνδεσης HTTP και πιστοποιητικά πελάτη SSL ενός χρήστη και να χρησιμοποιήσουν το πρόγραμμα περιήγησης ως τρόπο περιστροφής σε ένα πιστοποιημένο intranet.

Το pivoting του προγράμματος περιήγησης απαιτεί την εκτέλεση του SeDebugPrivilege και μια διαδικασία υψηλής ακεραιότητας. Η επισκεψιμότητα του προγράμματος περιήγησης κάνει pivoting στο πρόγραμμα περιήγησης του αντιπάλου μέσω του προγράμματος περιήγησης του χρήστη ρυθμίζοντας έναν διακομιστή μεσολάβησης HTTP που θα ανακατευθύνει οποιαδήποτε κίνηση HTTP και HTTPS. Αυτό δεν αλλάζει με κανέναν τρόπο την κίνηση του χρήστη. Η σύνδεση διακομιστή μεσολάβησης διακόπτεται μόλις κλείσει το πρόγραμμα περιήγησης. Όποια επεξεργασία του προγράμματος περιήγησης εισάγεται ο διακομιστής μεσολάβησης, ο αντίπαλος αναλαμβάνει το πλαίσιο ασφαλείας αυτής της διαδικασίας. Τα προγράμματα περιήγησης δημιουργούν συνήθως μια νέα διαδικασία για κάθε καρτέλα που ανοίγει και τα δικαιώματα και τα πιστοποιητικά διαχωρίζονται ανάλογα.

Με αυτά τα δικαιώματα, ένας αντίπαλος θα μπορούσε να περιηγηθεί σε οποιονδήποτε πόρο σε ένα intranet που είναι προσβάσιμο μέσω του προγράμματος περιήγησης και στον οποίο το πρόγραμμα περιήγησης έχει επαρκή δικαιώματα, όπως Sharepoint ή webmail. Η περιστροφή του προγράμματος περιήγησης εξαλείφει επίσης την ασφάλεια που παρέχεται από τον έλεγχο ταυτότητας δύο παραγόντων.

(ATT&CK, 2020)

Κεφάλαιο 5: ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

5.1. Δεδομένα Ασφάλειας στον Κυβερνοχώρο για το 2020

- Το 85% των ατόμων που δημοσιεύουν φωτογραφίες κουταβιών είναι υπεύθυνοι για διαδικτυακή απάτη.
- Το 43% των παραβιάσεων δεδομένων είναι εφαρμογές ιστού που βασίζονται σε cloud
- Το 67% των παραβιάσεων δεδομένων προέκυψε από κλοπή διαπιστευτηρίων, ανθρώπινο σφάλμα ή επιθέσεις κοινωνικής μηχανικής.
- Λιγότερες από 1 στις 20 παραβιάσεις εκμεταλλεύονται αδυναμίες
- Το 70% των παραβιάσεων προκαλούνται από εξωτερικούς παράγοντες
- Οι συμμορίες οργανωμένου εγκλήματος αντιπροσωπεύουν το 55% των επιθέσεων
- Το 37% των παραβιάσεων κλοπής διαπιστευτηρίων χρησιμοποίησε κλεμμένα ή αδύναμα διαπιστευτήρια
- Το 25% αφορούσε phishing
- Ανθρώπινο σφάλμα αντιπροσωπεύει το 22% των περιπτώσεων διαρροής δεδομένων
- Το Ransomware εντοπίζεται στο 27% των περιστατικών κακόβουλου λογισμικού παρουσιάζοντας αύξηση από το 24% του 2019
- Το 18% των οργανισμών ανέφεραν επίθεση ransomware
- Το 41% των πελατών θα σταματούσαν να αγοράζουν από μια επιχείρηση που είναι θύμα μιας επίθεσης ransomware
- Μία επίθεση στον κυβερνοχώρο συμβαίνει κάθε 39 δευτερόλεπτα
- Το 75% των διαδικτυακών επιθέσεων ξεκινούν με email
- Το 21% των διαδικτυακών χρηστών είναι θύματα των χάκερς
- Το 11% των διαδικτυακών χρηστών έχουν πέσει θύματα κλοπής δεδομένων
- Το 72% των παραβιάσεων στοχεύουν μεγάλες επιχειρήσεις
- Το 10% των οργανισμών λαμβάνουν κακόβουλο λογισμικό εξόρυξης κρυπτονομισμάτων
- Το 80% των παραβιάσεων των χάκερς περιλαμβάνουν brute force ή κλεμμένα διαπιστευτήρια

(Fintechnews, 2020)

5.2. Στατιστικά Στοιχεία Κυβερνοεπιθέσεων στην περίοδο εμφάνισης του Κορωνοϊού

- Ο Κορωνοϊός κατηγορείται για την αύξηση κατά 238% σε επιθέσεις σε τράπεζες
- 80% των εταιρειών έχουν δει αύξηση των κυβερνοεπιθέσεων
- Το 27% των επιθέσεων στοχεύουν σε τράπεζες ή στην υγειονομική περίθαλψη
- Οι επιθέσεις βάσει cloud αυξήθηκαν 630% μεταξύ Ιανουαρίου και Απριλίου 2020
- Οι προσπάθειες phishing αυξήθηκαν κατά 600% από τα τέλη Φεβρουαρίου
- Η Apple αντιπροσώπευε το 10% των επώνυμων προσπαθειών phishing στο πρώτο τρίμηνο του 2020
- Οι επιθέσεις Ransomware αυξήθηκαν 148% τον Μάρτιο
- 394.000 μοναδικές διευθύνσεις IP επιτέθηκαν σε βρετανικές εταιρείες το πρώτο τρίμηνο
- Οι επιθέσεις που στοχεύουν στους εργαζόμενους από το σπίτι αυξήθηκαν πέντε φορές τις έξι εβδομάδες της καραντίνας
- Οι επιθέσεις αυξήθηκαν κατά 30% το πρώτο τρίμηνο του 2020 στις επιχειρήσεις του Ηνωμένου Βασιλείου
- Οι επισκέψεις σε ιστότοπους και φόρουμ των χάκερς αυξήθηκαν κατά 66% τον Μάρτιο
- Η μέση πληρωμή ransomware αυξήθηκε κατά 33% φτάνοντας στα 111.605$, σε σύγκριση με το 4ο τρίμηνο του 2019
- Ο νέος Trojan EventBot που ταυτοποιήθηκε τον Μάρτιο, έχει στοχεύσει 200 εφαρμογές τραπεζικής και μεταφοράς χρημάτων

(Fintechnews, 2020)

5.3. Ηλεκτρονικές Επιθέσεις μέσω Phishing

Περίπου το 91% όλων των διαδικτυακών επιθέσεων περιλαμβάνουν κάποια μορφή phishing. Το Spear phishing ή η στόχευση ατόμων με προσωπικά, μη τυχαία μηνύματα ηλεκτρονικού ταχυδρομείου που αναφέρουν το όνομα, τη θέση τους ή άλλες

συγκεκριμένες πληροφορίες, περιέχουν κακόβουλα αρχεία στο 94% των περιπτώσεων, ενώ το 6% βασίζεται σε άλλες μεθόδους, όπως η χρήση κακόβουλων συνδέσμων. Το ποσοστό των χάκερ που χρησιμοποιούν το ηλεκτρονικό ψάρεμα ως μέθοδο επίθεσης αυξάνεται, καθώς ήταν 89% το 2016. (99firms, 2020)

5.4. Το πιο κοινό έγκλημα στον Κυβερνοχώρο

Η κλοπή ταυτότητας παραμένει το κορυφαίο έγκλημα στον κυβερνοχώρο, καθώς προσφέρει τα περισσότερα οφέλη σε όσους ασχολούνται με την κλοπή δεδομένων.

Μπορούν να χρησιμοποιήσουν τα δεδομένα για να διαπράξουν απάτη, να ενεργοποιήσουν υπηρεσίες στο όνομά σας, να ψαρέψουν τις επαφές σας και άλλα. Ακολουθούν κοινωνικές μηχανικές, botnets, επιθέσεις πλημμυρών και cyberstalking.

Το χρηματικό κέρδος παραμένει η κορυφαία προτεραιότητα για εγκληματίες στον κυβερνοχώρο σε όλο τον κόσμο, με το 71% αυτών των αδικημάτων να οφείλεται σε οικονομικά κίνητρα. (99firms, 2020)

5.5. Οικονομικά Στοιχεία σχετικά με την Κυβερνοασφάλεια και τις Κυβερνοεπιθέσεις

i) Το 2018, η Παγκόσμια αγορά ασφάλειας στον κυβερνοχώρο αποτιμήθηκε κάτω από τα 119 δισεκατομμύρια δολάρια. Μέχρι το 2023, η αξία του αναμένεται να υπερδιπλασιαστεί, φτάνοντας τα 248 δισεκατομμύρια δολάρια.
ii) Η Ευρώπη διαθέτει την υψηλότερη ετήσια ανάπτυξη όσον αφορά την ασφάλεια στον κυβερνοχώρο.
iii) Οι παγκόσμιες δαπάνες για την ασφάλεια στον κυβερνοχώρο αναμένεται να φθάσουν τα 133,7 δισεκατομμύρια δολάρια έως το 2022.

Οι απειλές στον κυβερνοχώρο αποτελούν αυξανόμενη ανησυχία στον ψηφιακό κόσμο. Σε παγκόσμιο επίπεδο, παρουσιάζεται αύξηση 141% των εξόδων για την ασφάλεια στον κυβερνοχώρο συγκριτικά με το 2010. Τα επόμενα χρόνια το

ποσό που θα ξοδεύουν οι εταιρείες για να διατηρήσουν τα δεδομένα των χρηστών τους ασφαλή θα ανέλθει στα 133,7 δισεκατομμύρια δολάρια, σύμφωνα με τις υποδείξεις των τάσεων της ασφάλειας στον κυβερνοχώρο.

iv) Η ασφάλεια στον κυβερνοχώρο είναι μια από τις πιο επικερδείς βιομηχανίες της σύγχρονης εποχής. Με την αύξηση των παγκόσμιων δαπανών, ο αριθμός των εταιρειών που δραστηριοποιούνται σε αυτόν τον τομέα πρόκειται να αυξηθεί.

v) Η ευρωπαϊκή αγορά ασφάλειας στον κυβερνοχώρο ανήλθε σε 36,02 δισεκατομμύρια δολάρια το 2019.

Οι αναδυόμενες τάσεις στον τομέα της ασφάλειας στον κυβερνοχώρο δείχνουν ότι η Ευρώπη αναμένεται να είναι η περιοχή με το υψηλότερο σύνθετο ετήσιο ποσοστό ανάπτυξης τα επόμενα 5 χρόνια όσον αφορά τη συγκεκριμένη βιομηχανία. Μέχρι το 2025, η Ευρωπαϊκή αγορά ασφάλειας στον κυβερνοχώρο αναμένεται να ξεπεράσει την αξία των 65 δισεκατομμυρίων δολαρίων.

vi) Η παγκόσμια οικονομία εγκλήματος στον κυβερνοχώρο αποφέρει 1,5 τρισεκατομμύρια δολάρια ετησίως.

Αυτές οι επιθέσεις είναι τόσο δημοφιλείς επειδή μπορούν να αποδώσουν μαζικά. Κατά τη διάρκεια του 2018, πραγματοποιήθηκε μια μελέτη σύμφωνα με την οποία η βιομηχανία εγκλήματος στον κυβερνοχώρο αποφέρει 1,5 δισεκατομμύρια δολάρια σε ετήσια κέρδη, τα οποία προέρχονται από:

a. 860 δισεκατομμύρια δολάρια προέρχονται από παράνομες διαδικτυακές αγορές.
b. 500 δισεκατομμύρια δολάρια προέρχονται από την κλοπή εμπορικών μυστικών.
c. 160 δισεκατομμύρια δολάρια προέρχονται από την εμπορία δεδομένων.
d. 1,6 δισεκατομμύρια δολάρια προέρχονται από crimeware-as-a-service.
e. 1 δισεκατομμύριο δολάρια προέρχεται από ransomware.

vii) Τα πρόστιμα του GDPR ανήλθαν σε 63 εκατομμύρια δολάρια τον πρώτο χρόνο εφαρμογής του. (Varonis, 2020)

viii) Οι επιχειρήσεις ξόδεψαν κατά μέσο όρο 1,3 εκατομμύρια δολάρια για να πληρούν τις απαιτήσεις συμμόρφωσης και αναμένεται να διαθέσουν επιπλέον 1,8 εκατομμύρια δολάρια.

ix) Οι νομικές συμβουλές και οι ομάδες κοστίζουν στις UK FTSE 350 εταιρείες περίπου το 40% του προϋπολογισμού τους στο GDPR ή 2,4 εκατομμύρια δολάρια.

(99firms, 2020)

Κεφάλαιο 6: Ο ΡΟΛΟΣ ΤΩΝ ΑΝΘΡΩΠΩΝ ΣΤΗΝ ΕΠΙΔΡΑΣΗ ΤΩΝ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΣΤΟΥΣ ΟΡΓΑΝΙΣΜΟΥΣ

Ο κεντρικός ρόλος της πληροφορίας και της τεχνολογίας πληροφοριών έχει καταστήσει την ασφάλεια των πληροφοριών βασικό μέλημα για τους οργανισμούς.

Το ανθρώπινο σφάλμα είναι η κύρια αιτία του 95% των παραβιάσεων της ασφάλειας στον κυβερνοχώρο. Οπότε, εάν το ανθρώπινο λάθος είχε εξαλειφθεί εντελώς, 19 από τις 20 παραβιάσεις στον κυβερνοχώρο ενδέχεται να μην είχαν συμβεί. (Ohlhorst, 2014) (IBM, 2014)

Σε ένα πλαίσιο ασφάλειας, το ανθρώπινο σφάλμα σημαίνει ακούσιες ενέργειες ή έλλειψη δράσης από υπαλλήλους και χρήστες που προκαλούν, διαδίδουν ή επιτρέπουν παραβίαση ασφαλείας.

Το ανθρώπινο σφάλμα περιλαμβάνει ένα ευρύ φάσμα ενεργειών - από τη λήψη συνημμένου που έχει μολυνθεί από κακόβουλο λογισμικό έως την αποτυχία χρήσης ενός ισχυρού κωδικού πρόσβασης - που αποτελεί μέρος του λόγου για τον οποίο είναι τόσο δύσκολο να περιοριστεί.

Με τα ολοένα πιο προηγμένα και περίπλοκα περιβάλλοντα εργασίας, διατίθεται ένας αυξανόμενος αριθμός εργαλείων και υπηρεσιών που χρησιμοποιούνται και απαιτούν ονόματα χρήστη και κωδικούς πρόσβασης που ο εργαζόμενος πρέπει να θυμάται για καθένα από αυτά τα εργαλεία. Σαν αποτέλεσμα, όσα αναφέρθηκαν αποτελούν επιπλέον φόρτο για τους εργαζόμενους, οι οποίοι αρχίζουν να λαμβάνουν συντομεύσεις για να διευκολυνθούν ειδικά όταν δεν τους παρέχονται εναλλακτικές, ασφαλείς λύσεις.

Η κοινωνική μηχανική διαδραματίζει αυξανόμενο ρόλο σε όλους τους τύπους παραβιάσεων της ασφάλειας και χρησιμοποιείται για την εκμετάλλευση της ικανότητας των υπαλλήλων να παραδίδουν δεδομένα ή διαπιστευτήρια απευθείας στα χέρια κακών παραγόντων χωρίς να χρειάζεται να χρησιμοποιήσουν προγράμματα κακόβουλου λογισμικού ή εκμετάλλευσης λογισμικού.

6.1. Τύποι ανθρώπινου σφάλματος

Τα πιο συνηθισμένα σφάλματα που παρατηρούνται είναι τα εξής:

i. Κοινή χρήση κωδικών πρόσβασης με φίλους και συναδέλφους

ii. Καταγραφή κωδικών πρόσβασης σε σημειώσεις post-it στην οθόνη του υπολογιστή

iii. Χρήση ή δημιουργία κωδικών πρόσβασης που δεν είναι πολύ περίπλοκα, όπως ονόματα μελών της οικογένειάς τους και ημερομηνία γέννησης.

Τα γεγονότα από την έκθεση του Εθνικού Κέντρου για την Ασφάλεια στον Κυβερνοχώρο για το 2019 παρουσιάζουν το γεγονός ότι το “123456” παραμένει ο πιο δημοφιλής κωδικός πρόσβασης στον κόσμο.

iv. Χρήση κοινού κωδικού πρόσβασης για πολλούς ιστότοπους.

Το 45% των ατόμων επαναχρησιμοποιούν τον κωδικό πρόσβασης του κύριου λογαριασμού email τους σε άλλες υπηρεσίες (Hadlington, 2017)

v. Χρήση διαδικτυακών συστημάτων αποθήκευσης για ανταλλαγή και διατήρηση προσωπικών ή ευαίσθητων πληροφοριών.

vi. Εισαγωγή πληροφοριών πληρωμής σε ιστότοπους, οι οποίοι δε διαθέτουν σαφείς πληροφορίες ασφαλείας ή πιστοποίηση.

vii. Χρήση δημόσιου Wi-Fi ελεύθερης πρόσβασης.

viii. Αναζήτηση ενημέρωσης σχετικά με πτυχές της διαδικτυακής ασφάλειας από αξιόπιστο φίλο ή συνάδελφο.

ix. Λήψη δωρεάν λογισμικού προστασίας από ιούς από άγνωστη πηγή.

x. Απενεργοποίηση του προγράμματος προστασίας από ιούς στον υπολογιστή εργασίας για να είναι δυνατή η λήψη πληροφοριών από ιστότοπους.

xi. Χρήση προσωπικού USB για μεταφορά δεδομένων σε αυτό.

xii. Παράλειψη ελέγχου και άμεσης ενημέρωσης του λογισμικού.

Οι εγκληματίες του κυβερνοχώρου ψάχνουν συνεχώς νέους τρόπους εκμετάλλευσης του λογισμικού. Όταν ανακαλυφθούν τρωτά σημεία, οι προγραμματιστές λογισμικού αγωνίζονται να διορθώσουν την ευπάθεια και να

στείλουν την ενημέρωση κώδικα σε όλους τους χρήστες προτού οι εγκληματίες του κυβερνοχώρου μπορούν να θέσουν σε κίνδυνο περισσότερους χρήστες. Γι' αυτό είναι σημαντικό οι χρήστες να εγκαθιστούν ενημερώσεις ασφαλείας στους υπολογιστές τους μόλις αυτές είναι διαθέσιμες. Παρόλ' αυτά όμως, συχνά οι τελικοί χρήστες καθυστερούν την εγκατάσταση ενημερώσεων με αποτέλεσμα την απειλή της ασφάλειας του συστήματός τους.

xiii. Λήψη ψηφιακών μέσων (μουσική, ταινίες, παιχνίδια) από πηγές χωρίς άδεια.

xiv. Κοινοποίηση της τρέχουσας τοποθεσίας ατόμου στα κοινωνικά μέσα.

xv. Άνοιγμα συνδέσμων που περιέχονται σε ανεπιθύμητα email από άγνωστη πηγή.

xvi. Αποστολή προσωπικών πληροφοριών σε τρίτους μέσω του Διαδικτύου.

xvii. Άνοιγμα συνδέσμων που περιέχονται σε μηνύματα ηλεκτρονικού ταχυδρομείου από αξιόπιστο αποστολέα.

xviii. Παράλειψη ελέγχου για ενημερώσεις σε εγκατεστημένο λογισμικό προστασίας από ιούς.

xix. Λήψη δεδομένων και υλικού από ιστότοπους στον υπολογιστή εργασίας χωρίς έλεγχο της αυθεντικότητάς τους.

xx. Αποθήκευση πληροφοριών εταιρείας σε προσωπική ηλεκτρονική συσκευή.

xxi. Εκτεθειμένα ευαίσθητα έγγραφα χωρίς παρακολούθηση σε γραφεία, αίθουσες συσκέψεων ή δίσκους εξόδου εκτυπωτή, δίνοντας τη δυνατότητα παραβίασης σε όποιον αποκτά πρόσβαση στις εγκαταστάσεις της επιχείρησης

xxii. Η εσφαλμένη παράδοση, δηλαδή η αποστολή σε λάθος παραλήπτη, αποτελεί κοινή απειλή για την ασφάλεια των εταιρικών δεδομένων.

Σύμφωνα με την αναφορά παραβιάσεων της Verizon για το 2018, η εσφαλμένη παράδοση ήταν η πέμπτη πιο κοινή αιτία όλων των παραβιάσεων της ασφάλειας στον κυβερνοχώρο. Με πολλά άτομα να βασίζονται σε λειτουργίες όπως η αυτόματη πρόταση πελατών για αποστολή email, είναι εύκολο για οποιονδήποτε χρήστη να στείλει κατά λάθος εμπιστευτικές πληροφορίες σε λάθος άτομο εάν δεν είναι προσεκτικός. (Hadlington, 2017)

Παρά τη μεγάλη ποικιλία κατηγοριών ανθρώπινου σφάλματος, τα σφάλματα αυτά μπορούν γενικά να κατηγοριοποιηθούν σε τρεις διαφορετικούς τύπους: σφάλματα βάσει δεξιοτήτων, βάσει αποφάσεων και σφάλματα βάσει πεποιθήσεων. Η διαφορά μεταξύ αυτών των σφαλμάτων βάσει δεξιοτήτων και βάσει αποφάσεων εξαρτάται ουσιαστικά από το αν το άτομο είχε ή όχι τις απαιτούμενες γνώσεις για να εκτελέσει τη σωστή ενέργεια. (Ahola, 2019). Ενώ τα σφάλματα βάσει πεποιθήσεων, αφορά τη συμπεριφορά των εργαζομένων και τη στάση τους σχετικά με τα θέματα ασφάλειας και το μερίδιο ευθύνης που τους αναλογεί.

Σφάλματα βάσει αποφάσεων

Το ανθρώπινο σφάλμα βάσει αποφάσεων προκύπτει κατά την εκτέλεση οικείων εργασιών και δραστηριοτήτων. Σε αυτά τα σενάρια, ο τελικός χρήστης γνωρίζει ποια είναι η σωστή πορεία δράσης, αλλά δεν την ακολουθεί λόγω προσωρινού ολισθήματος, λάθους ή αμέλειας. Αυτά μπορεί να συμβούν επειδή ο εργαζόμενος είναι κουρασμένος, δεν προσέχει ή αποσπάται η προσοχή του.

Σφάλματα βάσει δεξιοτήτων

Τα σφάλματα βάσει δεξιοτήτων προκύπτουν όταν ένας χρήστης δεν έχει το απαραίτητο επίπεδο γνώσης, δεν έχει αρκετές πληροφορίες σχετικά με τη συγκεκριμένη περίσταση και ενεργεί εσφαλμένα ή δεν συνειδητοποιεί ότι λαμβάνει μια απόφαση μέσω της αδράνειας του.

Σφάλματα βάσει πεποιθήσεων

Τα σφάλματα αυτά προκύπτουν από λανθασμένες πεποιθήσεις των εργαζομένων σχετικά με την πολιτική που ακολουθεί ο οργανισμός στον οποίο εργάζονται για την ασφάλεια των πληροφοριών και το μερίδιο ευθύνης που κατέχουν οι ίδιοι οι εργαζόμενοι.

Παραδείγματα αντίστοιχης συμπεριφοράς είναι τα εξής:

i. Πεποίθηση ότι η διοίκηση έχει την ευθύνη να διασφαλίσει ότι μια εταιρεία προστατεύεται από το έγκλημα στον κυβερνοχώρο

ii. Άγνοια του ρόλου τους στην προστασία της εταιρείας από πιθανούς εγκληματίες στον κυβερνοχώρο.

iii. Πεποίθηση ότι τα συστήματα υπολογιστών παρέχουν όλη την προστασία που χρειάζεται μια εταιρεία.

iv. Πεποίθηση ότι η αναφορά του εγκλήματος στον κυβερνοχώρο δεν επιφέρει αποτελέσματα.

v. Πεποίθηση ότι η αστυνομία δεν έχει την ικανότητα να αντιμετωπίζει αποτελεσματικά το έγκλημα στον κυβερνοχώρο.

vi. Πεποίθηση ότι οι εγκληματίες στον κυβερνοχώρο είναι πιο προχωρημένοι από τους την ομάδα IT της εταιρείας.

vii. Ανησυχία για τη φήμη της εταιρείας σε περίπτωση αναφοράς της επίθεσης στον κυβερνοχώρο στην Αστυνομία.

viii. Ελλειπής γνώση της πολιτικής χρήσης της εταιρείας.

ix. Δε γνωρίζουν πώς να αναφέρουν επίθεση στον κυβερνοχώρο εάν συμβεί κάτι τέτοιο.

x. Πεποίθηση ότι η αναφορά διαδικτυακής επίθεσης στην εταιρεία δεν αποτελεί ατομική ευθύνη.

xi. Παράβλεψη του υλικού της εταιρείας σχετικά με τις απειλές από το έγκλημα στον κυβερνοχώρο.

xii. Αδυναμία εντοπισμού στοιχείων που υποδεικνύουν μια επίθεση στον κυβερνοχώρο.

xiii. Πεποίθηση ότι η μεγαλύτερη απειλή για συστήματα πληροφορικής προέρχεται από άτομα εντός της εταιρείας.

xiv. Πεποίθηση ότι οι εγκληματίες στον κυβερνοχώρο στοχεύουν μια εταιρεία μόνο όταν υπάρχει σημαντικό οικονομικό κέρδος.

xv. Πεποίθηση ότι μόνο μεγάλες εταιρείες στοχεύονται από χάκερ και εγκληματίες στον κυβερνοχώρο. (Hadlington, 2017)

Κεφάλαιο 7: ΣΤΑΔΙΑ ΑΝΑΠΤΥΞΗΣ ΤΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ

Ένα από τα ζητήματα που εντοπίστηκαν στη λεγόμενη βιβλιογραφία συμπεριφορικής ασφάλειας πληροφοριών αφορά το γιατί οι εργαζόμενοι συμμορφώνονται ή παραβιάζουν τις διαδικασίες ασφάλειας πληροφοριών (ISP) του οργανισμού τους. Αυτό περιλαμβάνει τις περιπτώσεις όπου οι εργαζόμενοι μπορούν να παρακάμψουν ορισμένες διαδικασίες ασφάλειας πληροφοριών, όπως να αφήσουν τους υπολογιστές τους ξεκλείδωτους, να στέλνουν εμπιστευτικά e-mail χωρίς κρυπτογράφηση ή να ανοίγουν συνδέσμους σε μολυσμένους ιστότοπους.

Από πρακτική άποψη, η κατανόηση τέτοιων συμπεριφορών είναι σημαντική. Εάν οι χρήστες δεν συμμορφώνονται με τις (ISPs-Information Security Procedures) διαδικασίες ασφάλειας πληροφοριών, παρόλο που είναι τεχνικά εξελιγμένες, χάνουν την αποτελεσματικότητά τους . Πράγματι, η υιοθέτηση επισφαλών συμπεριφορών των εργαζομένων εξακολουθεί να αποτελεί βασική εξήγηση για παραβιάσεις στην ασφάλεια πληροφοριών που δημιουργούν σημαντικές οικονομικές απώλειες για τους οργανισμούς. Για το λόγο αυτό, οι επιχειρήσεις ακολουθούν τα εξής στάδια ανάπτυξης της συμπεριφοράς ασφάλειας πληροφοριών (ISB – Information Security Behavior) των εργαζομένων, ώστε να καθοδήγήσουν την συμπεριφορά τους και να εξαληφθούν τα περιστατικά ανθρώπινου σφάλματος που οδηγούν σε επιτυχημένες κυβερνοεπιθέσεις και διαρροές απόρρητων στοιχείων των επιχειρήσεων.
(Mari Karjalainen, 2020)

7.1. Στάδια ανάπτυξης της ISB των εργαζομένων

Στοιχεία της Θεωρίας Σταδίων	**Χαρακτηριστικά στο Στάδιο 1: Διαισθητική σκέψη**	**Χαρακτηριστικά στο Στάδιο 2: Δηλωτική σκέψη**	**Χαρακτηριστικά στο Στάδιο 3: Σκέψη σχετικά με τον οργανισμό**	**Χαρακτηριστικά στο Στάδιο 4: Σκέψη ρουτίνας**
Ειδικές γνώσεις ασφαλείας σταδίου που εξηγούν τις ISB, δηλαδή συμμόρφωση (C) ή μη συμμόρφωση (N) με ISP	Διαισθητικές γνώσεις (N) Σχετικοί εμπειρικοί παράγοντες: -Διαχωρισμός -Υπερεκτίμηση ικανοτήτων/ υποεκτίμηση απαίτησης ασφάλειας πληροφοριών -Ικανοποίηση ασφάλειας πληροφοριών	Δηλωτικές γνώσεις (C / N) Σχετικοί εμπειρικοί παράγοντες: -Σχετικές με την ασφάλεια πληροφοριών(N): σύγκρουση αξίας, ενόχληση -Ετερόνομες(C/ N): εξάρτηση από την αρχή, εξάρτηση από το πρότυπο, κοινωνική συμμόρφωση	Γνώσεις οργανισμών (C) Σχετικοί εμπειρικοί παράγοντες: -Αξιολόγηση των κινδύνων -Αξία συνάφειας -Εμπιστοσύνη στους ISP	Ρουτίνες που σχετίζονται με τις γνώσεις(C) Σχετικοί εμπειρικοί παράγοντες: -Γνώσεις πρακτορείων που εξηγούν τις ISB με χαμηλή γνωστική προσπάθεια
Ενισχυτές αλλαγής σταδίου που προάγουν την αλλαγή συμπεριφοράς	Μεταξύ 1-2: Ενισχυτές κινήτρων - Σχετικοί εμπειρικοί παράγοντες: -Εσωτερικός: προσωπικό ενδιαφέρον και δραστηριότητα -Εξωτερικός: άμεσα και έμμεσα ατυχήματα ασφάλειας πληροφοριών, ορατότητα των μέσων Οργανωτικός	Μεταξύ 2–3: Ενισχυτές αντίστασης - Σχετικοί εμπειρικοί παράγοντες: -Βιωματικό περιεχόμενο μάθησης -Συνεργατικές μέθοδοι μάθησης	Μεταξύ 3–4: Βελτιωτές συχνότητας - Σχετικοί εμπειρικοί παράγοντες: -Αύξηση της ευαισθησίας των κινδύνων για την ασφάλεια των πληροφοριών -Βελτίωση συνδεσιμότητας αξίας -Συμφιλίωση συμπεριφορικής αποτελεσματικότητας	

Εικόνα 4: Πίνακας Σταδίων ανάπτυξης του ISB των εργαζομένων

7.1.1. Στάδιο 1: Διαισθητικό Στάδιο Σκέψης

Τα αποτελέσματα δείχνουν ότι οι εργαζόμενοι έχουν ορισμένες διαισθητικές πεποιθήσεις που σχετίζονται με την ασφάλεια των πληροφοριών, οι οποίες ως μια πιο θεμελιώδης κατηγορία γνώσης, λαμβάνονται μέσω ανατροφής, εκπαίδευσης ή προηγούμενων εμπειριών. Τέτοιες πεποιθήσεις είναι μερικές φορές σε αντίθεση με τις ISP των οργανισμών. Επομένως, η συμβατή ISB - όπως η αποφυγή μηνυμάτων ηλεκτρονικού ταχυδρομείου για την αποστολή κρίσιμων πληροφοριών ή η χρήση ισχυρών κωδικών πρόσβασης - συχνά δεν έχει διαισθητικό νόημα στους υπαλλήλους. Κατά συνέπεια, οι εργαζόμενοι δεν αναγνωρίζουν την αδυναμία τους σχετικά με την ασφάλεια των πληροφοριών και την καθοριστική αξία της νέας ISB, όπως τα οφέλη της επιλογής ενός ισχυρού κωδικού πρόσβασης. Έτσι, οι εργαζόμενοι σε αυτό το στάδιο είναι ασυνείδητα ανίκανοι, δηλαδή, η ISB τους είναι ασυνείδητα ασυμβίβαστη με τις ISP του οργανισμού τους. Στη συνέχεια, παρουσιάζονται κάποιες τυπικές διαισθητικές γνώσεις που σχετίζονται με αυτό το προπαρασκευαστικό στάδιο.

Ο διαχωρισμός σημαίνει ότι ένας ερωτώμενος συνδέει διαισθητικά την ευθύνη για τη διασφάλιση της ασφάλειας των πληροφοριών με άλλα μέρη, όπως υπαλλήλους ή τεχνολογίες πληροφορικής (IT) ή έχει εσφαλμένη εμπιστοσύνη στην πληροφορική. Για παράδειγμα, οι εργαζόμενοι μπορεί να αναμένουν ότι το προσωπικό πληροφορικής φροντίζει για την ασφάλεια των πληροφοριών και, ως εκ τούτου, μπορεί να μην γνωρίζουν τις ευθύνες τους σχετικά με την ασφάλεια των πληροφοριών. Ένα παράδειγμα ψευδούς εμπιστοσύνης στην πληροφορική είναι ότι οι εργαζόμενοι μπορεί να μην καταλαβαίνουν ότι οι κωδικοί πρόσβασής τους είναι υπερβολικά απλοί και είναι επομένως εύκολο να σπάσουν. Επιπλέον, επειδή οι εργαζόμενοι στο στάδιο της διαισθητικής σκέψης δεν είναι εξοικειωμένοι με τις επίσημες ISP του οργανισμού και των συναφών αναγκών του, μπορεί να υπερεκτιμούν τις δικές τους γνώσεις και ικανότητες ασφάλειας πληροφοριών, να υποτιμούν τη σημασία των ISP ή να μην βλέπουν την ανάγκη βελτίωσης. Αυτές οι αδυναμίες - υπερεκτίμηση ικανοτήτων, υποεκτίμηση ασφάλειας πληροφοριών και ικανοποίηση ασφάλειας πληροφοριών - λειτουργούν ως τυπικές γνώσεις στο στάδιο της διαισθητικής σκέψης και εμποδίζουν τους υπαλλήλους να δουν την ανάγκη να αλλάξουν τη συμπεριφορά τους.

Παρουσιάζονται για το λόγο αυτό βελτιωτικά κίνητρα, τα οποία είναι αποτελεσματικά για τη δημιουργία προθέσεων που σχετίζονται με την ασφάλεια των πληροφοριών.

Η απαρχή των γνώσεων για την ασφάλεια των πληροφοριών και της αλλαγής συμπεριφοράς σπάνια συμβαίνει αυθόρμητα λόγω των εσωτερικών ενισχυτών κινήτρων, δηλαδή του προσωπικού ενδιαφέροντος και της δραστηριότητας που αποσκοπούν στην εκμάθηση νέων ISP. Αντίθετα, μερικές φορές, οι πάροχοι υπηρεσιών Διαδικτύου και οι δύο έρχονται σε αντίθεση με τη διαισθητική σκέψη των εργαζομένων (Στάδιο 1) και δεν είναι εγγενώς κίνητρα. Κατά συνέπεια, η έναρξη της μάθησης συνήθως απαιτεί εξωτερικές εκδηλώσεις ή πράξεις οργανωτικού ελέγχου. Οι ενισχυτές κινήτρων μπορούν να αλλάξουν τις γνώσεις ασφάλειας πληροφοριών των υπαλλήλων από διαισθητικές σε δηλωτικές. Αυτό σημαίνει ότι επιτρέπουν στους υπαλλήλους να συνειδητοποιήσουν μια ασυμφωνία μεταξύ της τρέχουσας ISB και των ISP και, σε ορισμένες περιπτώσεις, να τους παρακινήσουν να συμμορφωθούν.

Διαπιστώσαμε ότι τόσο οι εξωτερικοί ενισχυτές όσο και οι ενισχυτές που σχετίζονται με τον έλεγχο μπορούν να παρακινήσουν τους υπαλλήλους να αλλάξουν τις γνώσεις τους και την πραγματική αλλαγή συμπεριφοράς.

Ωστόσο, ακόμη και αν είναι διαθέσιμα ενισχυτικά κίνητρα, οι εργαζόμενοι μπορεί να αποτύχουν να αλλάξουν τις διαισθητικές τους γνώσεις και το ISB. Αυτό συμβαίνει εάν τα μέτρα ενίσχυσης αλλαγής συμπεριφοράς δεν είναι επαρκή για την πρόκληση αιτιώδους συλλογισμού μεταξύ της ISB των εργαζομένων και των συνεπειών της. Χωρίς αποτελεσματικούς ενισχυτές κινήτρων, οι εργαζόμενοι συνεχίζουν να σκέφτονται και να συμπεριφέρονται σύμφωνα με τις υπάρχουσες διαισθητικές τους γνώσεις αντί να αναπτύσσουν νέες. Έτσι, απαιτείται ένας επαναλαμβανόμενος ενισχυτής κινήτρων για την προώθηση αλλαγής συμπεριφοράς. Οι επιτυχημένοι ενισχυτές κινήτρων μετακινούν τους υπαλλήλους στο στάδιο της δηλωτικής σκέψης.

7.1.2. Στάδιο 2: Δηλωτικό Στάδιο Σκέψης

Οι δηλωτικές γνώσεις εμφανίζονται ως συνέπεια της επιτυχούς απόκτησης γνώσεων και των επικοινωνιών που περιλαμβάνουν ενισχυτές κινήτρων. Αυτό σημαίνει ότι οι εργαζόμενοι έχουν τη δυνατότητα να αξιολογήσουν την ορθότητα της ISB τους με βάση

την κατανόηση των ISP βάσει των γεγονότων και των συναφών συνεπειών τους. Ωστόσο, οι υπάλληλοι σε αυτό το στάδιο συνήθως παραβιάζουν εν γνώσει τους τις ISP, επειδή αποκλειστικά οι πληροφορίες που βασίζονται σε πραγματικό χρόνο δεν αποτελούν επαρκή βάση για συμβατή ISB, καθώς δεν προσφέρει κατανόηση της σημασίας των ISP στο συγκεκριμένο οργανωτικό πλαίσιο και την προσωπική κατάσταση.

Αλλαγή ενισχυτών μετάβασης από το Στάδιο 2 στο Στάδιο 3 - Βελτιωτικά:

Μία από τις βασικές προκλήσεις στο στάδιο της δηλωτικής σκέψης είναι να κάνει τους υπαλλήλους να ανταποκρίνονται στις γνώσεις τους βάσει γεγονότων, προκειμένου να έχουν μια ενεργή ISB με σημαντικό προσωπικό νόημα.

Η αντίδραση αναφέρεται στην ενεργή και σκόπιμη γνωστική επεξεργασία της γνώσης που απαιτείται για την επίτευξη λύσεων σε πρακτικά προβλήματα (Hatton and Smith, 1995), όπως η μη συμμόρφωση με τους ISP. Από αυτή την άποψη, οι συνεντεύξεις μας αποκάλυψαν αρκετούς βελτιωτές της απόκρισης, δηλαδή το βιωματικό εκπαιδευτικό περιεχόμενο και τις συνεργατικές μεθόδους μάθησης.

7.1.3. Στάδιο 3: Στάδιο Σκέψης σχετιζόμενο με τον Οργανισμό

Οι βελτιωτικοί παράγοντες της επιτρέπουν το σχηματισμό γνωστικών σχετικών με τον Οργανισμό, υποδεικνύοντας ότι οι εργαζόμενοι είναι συνειδητά ικανοί να συμμορφώνονται με τις ISP. Υποστηρίζουμε ότι, σε αυτό το στάδιο, οι γνώσεις για την ασφάλεια των πληροφοριών και η συμπεριφορά μετατρέπονται από εξωτερικά κατευθυνόμενες σε αυτοκατευθυνόμενες με βάση τη γνώση σχετικά με την αποτελεσματικότητα και την εσωτερίκευση των τιμών. Αυτό σημαίνει ότι η συμβατή ISB βασίζεται σε συνειδητοποιημένους λόγους ασφάλειας πληροφοριών που σχετίζονται με τις υποκειμενικές εκτιμήσεις των εργαζομένων μεταξύ προσωπικής προσπάθειας και ωφέλειας ασφάλειας πληροφοριών, καθώς και προσωπικών αξιών και στόχων. Κατά συνέπεια, διαπιστώσαμε ότι η συμμόρφωση των εργαζομένων εξηγείται μέσω των γνώσεων των οργανισμών που αφορούν συγκεκριμένα την κατάσταση, δηλαδή την εξέταση των πλεονεκτημάτων της διαδικαστικής συμμόρφωσης που συνδέεται με το εξωτερικό περιβάλλον (αξιολόγηση των

κινδύνων), τις επαγγελματικές αξίες και την αποτελεσματικότητα των ISP (εμπιστοσύνη στις ISP). Οι εργαζόμενοι συμμορφώνονται με τις ISP επειδή έχουν εμπειρία λόγω δράσης για την οποία είναι υπεύθυνοι και όχι ως σύγκρουση μεταξύ των ISP και των γνώσεων σχετικά με την αξιολόγηση των κινδύνων, την αξία , και την εμπιστοσύνη στις ISP.

Ακόμη και αν οι εργαζόμενοι σε αυτό το στάδιο συμμορφώνονται με τις ISP, όπως και στα προηγούμενα στάδια, οι υπερισχύουσες γνώσεις μπορούν να ενθαρρύνουν τους υπαλλήλους που συμμορφώνονται προς την παραβίαση των παρόχων υπηρεσιών Διαδικτύου. Έτσι, απαιτείται μεγαλύτερη επιμονή σχετικά με συμβατή ISB μέσω ενισχυτών συχνότητας.

Αλλαγή ενισχυτών μετάβασης από το Στάδιο 3 στο Στάδιο 4 – ενισχυτές συχνότητας:

Στο στάδιο της σκέψης που σχετίζεται με τον Οργανισμό, ο στόχος είναι να γίνει η συμβατή ISB μέρος των εργασιών των εργαζομένων, χωρίς πρόσθετη γνωστική προσπάθεια. Για το σκοπό αυτό, οι εργαζόμενοι χρειάζονται ενισχυτές συχνότητας που ενισχύουν τις σχετικές με τον οργανισμό γνώσεις μέσω feedback που υποστηρίζει την αυτονομία που σχετίζεται με τη διατήρηση της αλλαγής συμπεριφοράς και την αύξηση της αυτοματοποίησης της συμπεριφοράς.

Χωρίς ενισχυτές συχνότητας, η συμμόρφωση με τις ISP είναι εφικτή μέσω της συνειδητής και συγκεκριμένης κατάστασης λήψης αποφάσεων, αλλά είναι επίσης ευάλωτη σε υπερισχύουσες γνώσεις. Η επικοινωνία ασφάλειας πληροφοριών που χρησιμοποιεί συνεχώς αυτούς τους ενισχυτές συχνότητας μετακινεί τους υπαλλήλους στο τελικό στάδιο σκέψης που σχετίζεται με τη ρουτίνα.

7.1.4. Στάδιο 4: Σκέψη που σχετίζεται με την ρουτίνα

Στο τελικό στάδιο της διαδικασίας ανάπτυξης, οι εργαζόμενοι συμμορφώνονται με τις ISP. Οι γνώσεις σχετικά με την ασφάλεια πληροφοριών που σχετίζονται με τη ρουτίνα, χαρακτηρίζουν αυτό το στάδιο και υποδηλώνουν ότι ως αποτέλεσμα των ενισχυτών συχνότητας, οι εργαζόμενοι συμμορφώνονται με τις ISP με χαμηλή γνωστική

προσπάθεια, δηλαδή, καθίστανται ασυνείδητα ικανοί να συμμορφωθούν με τις ISP. Οι γνώσεις που σχετίζονται με τη ρουτίνα, ως αποτέλεσμα μιας αναπτυξιακής διαδικασίας, δείχνουν ότι οι ISP έχουν θεωρηθεί δεδομένες σε ορισμένα κοινωνικά πλαίσια που είναι ανεξάρτητα από τα feedback. Επιπλέον, η συμπεριφορά των εργαζομένων σε αυτό το στάδιο δεν εξαρτάται σε μεγάλο βαθμό από τις επιτακτικές γνώσεις όπως στα προηγούμενα στάδια. Το πρώτο και το τελικό στάδιο της θεωρίας του σταδίου μπορεί να φαίνεται σχεδόν πανομοιότυπο, ωστόσο απαιτείται πάντα μια διαδικασία μάθησης για τη διαμόρφωση συμμορφούμενης ISB. Κατά τη διαδικασία υιοθέτησης νέων ISP, οι εργαζόμενοι σχηματίζουν νέα σκέψη και ISB που ισχύουν σε συγκεκριμένες καταστάσεις ή περιστάσεις εργασίας.

Σύμφωνα με τους ερωτηθέντες, οι ISP συνήθως συμμορφώνονται, εκτός από καταστάσεις όπου ένα άτομο αισθάνεται κοινωνική πίεση, η οποία μπορεί να είναι εσωτερική (π.χ. αποφυγή αρνητικών συναισθημάτων) ή εξωτερική (π.χ. αίσθηση φόβου). Ένα παράδειγμα εσωτερικής κοινωνικής πίεσης είναι ότι οι εργαζόμενοι ενδέχεται να αποκαλύψουν ευαίσθητες πληροφορίες επειδή θέλουν να βοηθήσουν τους άλλους ή να διατηρήσουν καλές εργασιακές σχέσεις. Με αυτή την αιτία μπορεί να μην ζητήσουν να δουν τα σήματα των υπαλλήλων ή να μην κλειδώσουν τους υπολογιστές τους επειδή αισθάνονται ντροπιασμένοι να ενεργήσουν με αυτόν τον τρόπο. Ένα παράδειγμα εξωτερικής κοινωνικής πίεσης είναι όταν ένας υπάλληλος αποκαλύπτει ευαίσθητες πληροφορίες, είτε προσωπικά είτε μέσω email, επειδή αισθάνεται ότι απειλείται.

Τέλος, σε περιπτώσεις καιροσκοπίας δεν έχουμε συμμόρφωση στις ISP εάν ένα άτομο έχει κίνητρο για σκόπιμη κακοποίηση, όταν δηλαδή το άτομο έχει προσωπικό όφελος όπως το νομισματικό όφελος ή προκαλεί σκόπιμα ζημιά στην εταιρεία.

Κεφάλαιο 8: ISO/IEC 27002 ΓΙΑ ΤΟΝ ΠΕΡΙΟΡΙΣΜΟ ΤΟΥ ΑΝΘΡΩΠΙΝΟΥ ΣΦΑΛΜΑΤΟΣ

Το πρότυπο ISO 27002 είναι μια συλλογή οδηγιών ασφαλείας πληροφοριών που έχουν σκοπό να βοηθήσουν έναν οργανισμό να εφαρμόσει, να διατηρήσει και να βελτιώσει τη διαχείριση της ασφάλειας πληροφοριών του.

Το πρότυπο αυτό περιλαμβάνει και οδηγίες σχετικά με τις υποχρεώσεις των εργαζόμενων των οργανισμών για την προστασία των στοιχείων ελέγχου ταυτότητας.

8.1. Μυστικές πληροφορίες ελέγχου ταυτότητας

Οι εργαζόμενοι προτείνεται να καθοδηγούνται από τους οργανισμούς σχετικά με τις εξής ενέργειες με στόχο τη σωστή χρήση μυστικών πληροφοριών ελέγχου ταυτότητας:

1. Διατήρηση εμπιστευτικότητας μυστικών πληροφοριών ελέγχου ταυτότητας, διασφαλίζοντας ότι δεν κοινοποιούνται σε άλλα μέρη, συμπεριλαμβανομένων των αρχών
2. Αποφυγή διατήρησης αρχείου αποθήκευσης των μυστικών πληροφοριών ελέγχου ταυτότητας σε ηλεκτρονική ή γραπτή μορφή, εκτός εάν αυτό μπορεί να αποθηκευτεί με ασφάλεια και η μέθοδος αποθήκευσης έχει εγκριθεί
3. Αλλαγή μυστικών πληροφοριών ελέγχου ταυτότητας όποτε υπάρχει ένδειξη για πιθανή παραβίαση
4. Οι κωδικοί πρόσβασης που χρησιμοποιούνται να είναι εύκολο να απομνημονευθούν, να μην έχουν σχέση με ατομικές πληροφορίες που να μπορεί κάποιος να μαντέψει, να μην περιλαμβάνουν ολόκληρες λέξεις και

φράσεις ώστε να μην είναι ευάλωτοι σε επιθέσεις λεξικού, χωρίς διαδοχικούς πανομοιότυπους, αλφαριθμητικούς ή αλφαβητικούς χαρακτήρες

5. Χρήση διαφορετικών κωδικών για επαγγελματικούς και μη επαγγελματικούς λογαριασμούς
6. Μη κοινοποίηση των ατομικών μυστικών πληροφοριών ελέγχου ταυτότητας του κάθε χρήστη
7. Διασφάλιση κατάλληλης προστασίας των κωδικών πρόσβασης όταν οι κωδικοί πρόσβασης χρησιμοποιούνται ως μυστικές πληροφορίες ελέγχου ταυτότητας σε αυτοματοποιημένες διαδικασίες σύνδεσης

8.2. Φυσική ασφάλεια

Οι οργανισμοί, χρειάζεται επίσης να μεριμνούν για τις περιμέτρους φυσικής ασφάλειας, με περιμέτρους ασφαλείας για την προστασία περιοχών που περιέχουν ευαίσθητες ή κρίσιμες πληροφορίες και εγκαταστάσεις επεξεργασίας πληροφοριών.

Οι ακόλουθες οδηγίες αφορούν τις περιμέτρους φυσικής ασφάλειας που μπορούν να εφαρμόζονται από τους οργανισμούς:

1. Καθορισμός περιμέτρων ασφαλείας και χωροθέτησή τους ανάλογα με τις απαιτήσεις ασφαλείας των περιουσιακών στοιχείων εντός της περιμέτρου και τα αποτελέσματα που θα προκύψουν από μια εκτίμηση κινδύνου

2. Προδιαγραφές ασφαλείας για την περίμετρο του κτιρίου ή του χώρου των εγκαταστάσεων:

    a. Η εξωτερική οροφή, οι τοίχοι και το δάπεδο του χώρου να είναι συμπαγούς κατασκευής και όλες οι εξωτερικές πόρτες να προστατεύονται κατάλληλα από μη εξουσιοδοτημένη πρόσβαση με μηχανισμούς ελέγχου (π.χ. ράβδοι, συναγερμοί, κλειδαριές)

b. Οι πόρτες και τα παράθυρα να κλειδώνονται όταν δεν παρακολουθούνται και να λαμβάνεται υπόψη η εξωτερική προστασία για τα παράθυρα, ιδίως στο επίπεδο του εδάφους

3. ΄Υπαρξη επανδρωμένου χώρου υποδοχής ή άλλων μέσων για τον έλεγχο της φυσικής πρόσβασης στο χώρο ή το κτίριο

4. Περιορισμός της πρόσβασης σε τοποθεσίες και κτίρια μόνο σε εξουσιοδοτημένο προσωπικό.

5. Κατασκευή φυσικών εμποδίων για την αποτροπή μη εξουσιοδοτημένης φυσικής πρόσβασης

6. Οι πυροσβεστικές πόρτες να διαθέτουν συναγερμό, συστήματα παρακολούθησης και να δοκιμάζονται σε συνδυασμό με τους τοίχους για να καθοριστεί το απαιτούμενο επίπεδο αντίστασης σύμφωνα με τα κατάλληλα περιφερειακά, εθνικά και διεθνή πρότυπα

7. Εγκατάσταση κατάλληλων συστημάτων ανίχνευσης εισβολέων σύμφωνα με τα εθνικά, περιφερειακά ή διεθνή πρότυπα και τακτικός έλεγχος ώστε να καλύπτουν όλες τις εξωτερικές πόρτες και τα προσβάσιμα παράθυρα

8. Διαχωρισμός εγκαταστάσεων επεξεργασίας πληροφοριών που διαχειρίζεται ο οργανισμός από εγκαταστάσεις διαχείρισης εξωτερικών φορέων

Η εφαρμογή φυσικών ελέγχων, ειδικά για ασφαλείς περιοχές, προτείνεται να προσαρμόζεται στις τεχνικές και οικονομικές συνθήκες του οργανισμού, όπως ορίζεται στην εκτίμηση κινδύνου.

Οι ασφαλείς περιοχές είναι σκόπιμο να προστατεύονται με κατάλληλους ελέγχους εισόδου για να διασφαλιστεί ότι επιτρέπεται μόνο πρόσβαση σε εξουσιοδοτημένο προσωπικό:

a. Καταγραφή της ημερομηνίας και της ώρας εισόδου και αναχώρησης των επισκεπτών και επίβλεψη όλων των επισκεπτών

b. Πρόσβαση μόνο για συγκεκριμένους, εξουσιοδοτημένους σκοπούς και έκδοση οδηγιών σχετικά με τις απαιτήσεις ασφαλείας της περιοχής και τις διαδικασίες έκτακτης ανάγκης

c. Ταυτοποίηση επισκεπτών με χρήση έγκυρων και πιστοποιημένων μέσων

d. Περιορισμός της πρόσβασης σε περιοχές όπου γίνεται επεξεργασία ή αποθήκευση εμπιστευτικών πληροφοριών σε εξουσιοδοτημένα άτομα μόνο με την εφαρμογή κατάλληλων ελέγχων πρόσβασης, π.χ. εφαρμόζοντας ένα μηχανισμό ελέγχου ταυτότητας δύο παραγόντων, όπως κάρτα πρόσβασης και μυστικό PIN

e. Διατήρηση και παρακολούθηση ασφαλείας φυσικού βιβλίου καταγραφής ή ηλεκτρονικού ίχνους ελέγχου κάθε πρόσβασης.

f. Υποχρέωση όλων των εργαζομένων, των εργολάβων και των εξωτερικών συνεργατών είναι να φορούν κάποια μορφή ορατής ταυτοποίησης και να ειδοποιείται αμέσως το προσωπικό ασφαλείας εάν παρατηρηθεί κάποιος επισκέπτης χωρίς συνοδεία και οποιοσδήποτε δεν φέρει ορατή ταυτότητα

g. Περιορισμένη πρόσβαση του προσωπικού υπηρεσιών εξωτερικής υποστήριξης σε ασφαλείς περιοχές ή εμπιστευτικές εγκαταστάσεις επεξεργασίας πληροφοριών και δυνατότητα πρόσβασης μόνο όταν απαιτείται και με την προϋπόθεση να έχει εγκριθεί και να παρακολουθείται

h. Επανεξέταση, τακτική ενημέρωση και ανάκληση όταν κριθεί απαραίτητο των δικαιωμάτων πρόσβασης σε ασφαλείς περιοχές

8.3. Πολιτική χρήσης Κρυπτογραφικών ελέγχων

Είναι πρωταρχικής σημασίας να αναπτυχθεί και να εφαρμοστεί μια πολιτική για τη χρήση κρυπτογραφικών ελέγχων για την προστασία των πληροφοριών, σύμφωνα με την οποία θα λαμβάνονται υπόψη τα εξής:

1. εμπιστευτικότητα: χρήση κρυπτογράφησης πληροφοριών για την προστασία ευαίσθητων ή κρίσιμων πληροφοριών, αποθηκευμένων ή μεταδιδόμενων
2. ακεραιότητα / αυθεντικότητα: χρήση ψηφιακών υπογραφών ή κωδικών ελέγχου ταυτότητας μηνυμάτων για την επαλήθευση της αυθεντικότητας ή της ακεραιότητας των αποθηκευμένων ή μεταδιδόμενων ευαίσθητων ή κρίσιμων πληροφοριών
3. έλεγχος ταυτότητας: χρήση κρυπτογραφικών τεχνικών για τον έλεγχο ταυτότητας χρηστών και άλλων οντοτήτων συστήματος που ζητούν πρόσβαση ή συναλλαγή με χρήστες συστήματος, οντότητες και πόρους.
4. μη απόρριψη εγκυρότητας: χρήση κρυπτογραφικών τεχνικών για την παροχή αποδεικτικών στοιχείων για την εμφάνιση ή τη μη εμφάνιση συμβάντος ή ενέργειας

Η λήψη απόφασης σχετικά με το εάν μια κρυπτογραφική λύση είναι κατάλληλη, αποτελεί μέρος της ευρύτερης διαδικασίας αξιολόγησης κινδύνου και επιλογής μεθόδων ελέγχου. Αυτή η αξιολόγηση μπορεί στη συνέχεια να χρησιμοποιηθεί για να προσδιοριστεί εάν είναι κατάλληλο ένα κρυπτογραφικό στοιχείο ελέγχου, τι είδους έλεγχος πρέπει να εφαρμοστεί και για ποιο σκοπό και επιχειρηματικές διαδικασίες.

Είναι αναγκαία μια πολιτική για τη χρήση κρυπτογραφικών ελέγχων για τη μεγιστοποίηση των οφελών και την ελαχιστοποίηση των κινδύνων από τη χρήση κρυπτογραφικών τεχνικών και για την αποφυγή ακατάλληλης ή λανθασμένης χρήσης.

Οι οργανισμοί θα μπορούσαν να διαθέτουν συστήματα διαχείρισης κωδικών πρόσβασης, τα οποία να είναι διαδραστικά, να διασφαλίζουν ποιοτικούς κωδικούς πρόσβασης και να έχουν τα εξής χαρακτηριστικά:

a. Επιβολή χρήσης μεμονωμένων αναγνωριστικών χρήστη και κωδικών πρόσβασης για τη διατήρηση της λογοδοσίας

b. Δυνατότητα των χρηστών να επιλέγουν και να αλλάζουν τους δικούς τους κωδικούς πρόσβασης και να περιλαμβάνουν μια διαδικασία επιβεβαίωσης για να επιτρέπονται τα σφάλματα εισαγωγής

c. Επιβολή επιλογής ποιοτικών κωδικών πρόσβασης

d. Επιβολή αλλαγής των κωδικών πρόσβασης στους χρήστες κατά την πρώτη σύνδεση

e. Επιβολή τακτικών αλλαγών στους κωδικούς πρόσβασης

f. Διατήρηση αρχείου κωδικών πρόσβασης που χρησιμοποιήθηκαν προηγουμένως και αποτροπή επαναχρησιμοποίησης τους

g. Απόκρυψη των κωδικών πρόσβασης στην οθόνη κατά την εισαγωγή τους από το χρήστη

h. Αποθήκευση αρχείων κωδικού πρόσβασης ξεχωριστά από τα δεδομένα συστήματος εφαρμογής

i. Αποθήκευση και μετάδοση κωδικών πρόσβασης σε προστατευμένη μορφή

Ορισμένες εφαρμογές απαιτούν την εκχώρηση κωδικών πρόσβασης χρήστη από ανεξάρτητη αρχή. Σε τέτοιες περιπτώσεις, τα σημεία b), d) και e) της παραπάνω καθοδήγησης δεν ισχύουν. Στις περισσότερες περιπτώσεις, οι κωδικοί πρόσβασης επιλέγονται και διατηρούνται από τους χρήστες.

8.4. Διαχείριση δικαιωμάτων πρόσβασης

Για τον καλύτερο έλεγχο των ενεργειών των χρηστών είναι αναγκαία η κατανομή και η χρήση προνομιακών δικαιωμάτων πρόσβασης, τα οποία πρέπει να περιορίζονται και να ελέγχονται.

Η κατανομή των προνομιακών δικαιωμάτων πρόσβασης είναι ωφέλημο να ελέγχεται μέσω επίσημης διαδικασίας εξουσιοδότησης σύμφωνα με τη σχετική πολιτική ελέγχου πρόσβασης:

1. Προσδιορισμός προνομιακών δικαιωμάτων πρόσβασης που σχετίζονται με κάθε σύστημα ή διαδικασία, όπως λειτουργικό σύστημα, σύστημα διαχείρισης βάσεων δεδομένων και οι χρήστες στους οποίους πρέπει να εκχωρηθούν

2. Κατανομή των προνομιακών δικαιωμάτων πρόσβασης στους χρήστες βάσει ανάγκης και σύμφωνα με την πολιτική ελέγχου πρόσβασης, δηλαδή με βάση την ελάχιστη απαίτηση για τους λειτουργικούς ρόλους τους

3. Διατήρηση μιας διαδικασίας εξουσιοδότησης και ένα αρχείο με όλα τα δικαιώματα που έχουν εκχωρηθεί. Προνομιακά δικαιώματα πρόσβασης δεν πρέπει να παραχωρούνται έως ότου ολοκληρωθεί η διαδικασία εξουσιοδότησης.

4. Καθορισμός των απαιτήσεων για τη λήξη των προνομιακών δικαιωμάτων πρόσβασης

5. Τα προνομιακά δικαιώματα πρόσβασης πρέπει να εκχωρούνται σε ένα αναγνωριστικό χρήστη διαφορετικό από εκείνο που χρησιμοποιείται για τακτικές επιχειρηματικές δραστηριότητες. Οι τακτικές επιχειρηματικές δραστηριότητες δεν πρέπει να εκτελούνται από προνομιακό αναγνωριστικό

6. Τακτική επανεξέταση των ικανοτήτων των χρηστών με προνομιακά δικαιώματα πρόσβασης προκειμένου να εξακριβώνεται εάν είναι σύμφωνες με τα καθήκοντά τους

7. Καθιέρωση και διατήρηση συγκεκριμένων διαδικασιών προκειμένου να αποφευχθεί η μη εξουσιοδοτημένη χρήση γενικών αναγνωριστικών χρήστη διαχείρισης, σύμφωνα με τις δυνατότητες διαμόρφωσης των συστημάτων

8. Για τα γενικά αναγνωριστικά χρήστη διαχείρισης, το απόρρητο των πληροφοριών μυστικού ελέγχου ταυτότητας θα πρέπει να διατηρείται όταν κοινοποιείται, όπως αλλαγή κωδικών πρόσβασης συχνά και το συντομότερο δυνατό όταν ένας προνομιούχος χρήστης φεύγει ή αλλάζει εργασία,

επικοινωνώντας τους μεταξύ προνομιούχων χρηστών με κατάλληλους μηχανισμούς

Η ακατάλληλη χρήση προνομίων διαχείρισης συστήματος, δηλαδή κάθε δυνατότητα ή λειτουργία ενός συστήματος πληροφοριών που επιτρέπει στο χρήστη να παρακάμψει τα στοιχεία ελέγχου συστήματος ή εφαρμογών, αποτελεί σημαντικό παράγοντα για την αποτυχία ή παραβίαση των συστημάτων.

8.5. Διαχείριση μυστικών πληροφοριών ελέγχου ταυτότητας των χρηστών

Η κατανομή των μυστικών πληροφοριών ελέγχου ταυτότητας μπορεί να ελέγχεται μέσω μιας επίσημης διαδικασίας διαχείρισης.

Η διαδικασία περιλαμβάνει τις ακόλουθες απαιτήσεις:

a. Υπογραφή δήλωσης από τους χρήστες για να διατηρούν εμπιστευτικές τις προσωπικές πληροφορίες μυστικού ελέγχου ταυτότητας και να διατηρούν κοινόχρηστες μυστικές πληροφορίες ελέγχου ταυτότητας αποκλειστικά εντός των μελών της ομάδας. Αυτή η υπογεγραμμένη δήλωση μπορεί να περιλαμβάνεται στους όρους και τις προϋποθέσεις εργασίας
b. Παροχή αρχικά ασφαλών προσωρινών πληροφοριών μυστικού ελέγχου ταυτότητας στους χρήστες, τις οποίες αναγκάζονται να αλλάξουν κατά την πρώτη χρήση, όταν απαιτείται από τους χρήστες να διατηρούν τις δικές τους πληροφορίες μυστικού ελέγχου ταυτότητας
c. Καθιέρωση διαδικασιών για την επαλήθευση της ταυτότητας ενός χρήστη πριν από την παροχή νέων, αντικαταστατικών ή προσωρινών μυστικών στοιχείων ελέγχου ταυτότητας
d. Ασφαλής παροχή των προσωρινών πληροφοριών μυστικού ελέγχου ταυτότητας στους χρήστες με ασφαλή τρόπο και αποφυγή της χρήσης

εξωτερικών μερών ή μη προστατευόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου.

e. Μοναδικότητα και μη προβλεψιμότητα των προσωρινών πληροφοριών μυστικού ελέγχου για ένα άτομο

f. Επιβεβαίωση λήψης μυστικών πληροφοριών ελέγχου ταυτότητας από τους χρήστες

g. Τροποποίηση των προεπιλεγμένων πληροφοριών μυστικού ελέγχου ταυτότητας προμηθευτή μετά την εγκατάσταση συστημάτων ή λογισμικού.

Οι κωδικοί πρόσβασης είναι ένας κοινώς χρησιμοποιούμενος τύπος πληροφοριών μυστικού ελέγχου ταυτότητας και αποτελούν ένα κοινό μέσο επαλήθευσης της ταυτότητας ενός χρήστη. Άλλοι τύποι πληροφοριών μυστικού ελέγχου ταυτότητας είναι τα κρυπτογραφικά κλειδιά και άλλα δεδομένα που αποθηκεύονται σε tokens, όπως έξυπνες κάρτες που παράγουν κωδικούς ελέγχου ταυτότητας.

8.6. Κατάργηση ή προσαρμογή των δικαιωμάτων πρόσβασης

Τα δικαιώματα πρόσβασης όλων των υπαλλήλων και των εξωτερικών χρηστών σε εγκαταστάσεις πληροφοριών και επεξεργασίας πληροφοριών είναι απαραίτητο να αφαιρεθούν κατά τη λήξη της εργασίας τους, της σύμβασης ή της συμφωνίας τους, ή να προσαρμοστούν σύμφωνα με την αλλαγή του ρόλου τους.

Μετά τον τερματισμό, τα δικαιώματα πρόσβασης ενός ατόμου σε πληροφορίες και περιουσιακά στοιχεία που σχετίζονται με τις εγκαταστάσεις και τις υπηρεσίες επεξεργασίας πληροφοριών είναι αναγκαίο να αφαιρεθούν ή να ανασταλούν. Αυτό θα καθορίσει εάν είναι απαραίτητο να καταργηθούν τα δικαιώματα πρόσβασης. Οι αλλαγές στην απασχόληση είναι σκόπιμο να αντικατοπτρίζονται στην κατάργηση όλων των δικαιωμάτων πρόσβασης που δεν εγκρίθηκαν για τη νέα απασχόληση. Τα δικαιώματα πρόσβασης που προτείνεται να καταργηθούν ή να προσαρμοστούν περιλαμβάνουν εκείνα της φυσικής και λογικής πρόσβασης. Η αφαίρεση ή η προσαρμογή μπορεί να γίνει με αφαίρεση, ανάκληση ή αντικατάσταση κλειδιών, δελτίων ταυτότητας, εγκαταστάσεων επεξεργασίας πληροφοριών ή συνδρομών. Κάθε

τεκμηρίωση που προσδιορίζει τα δικαιώματα πρόσβασης των εργαζομένων και των εργολάβων πρέπει να αντικατοπτρίζει την κατάργηση ή την προσαρμογή των δικαιωμάτων πρόσβασης. Εάν ένας υπάλληλος που έχει αποχωρήσει ή ένας χρήστης εξωτερικού μέρους γνωρίζει τους κωδικούς πρόσβασης για τα αναγνωριστικά χρήστη που παραμένουν ενεργά, αυτοί είναι καλό να αλλάξουν κατά τη λήξη ή την αλλαγή εργασίας, σύμβασης ή συμφωνίας.

Τα δικαιώματα πρόσβασης για πληροφορίες και περιουσιακά στοιχεία που σχετίζονται με εγκαταστάσεις επεξεργασίας πληροφοριών είναι σημαντικό να μειωθούν ή να αφαιρεθούν πριν από τη λήξη ή την αλλαγή της εργασίας, ανάλογα με την αξιολόγηση παραγόντων κινδύνου όπως:

1. Εάν ο τερματισμός ή η αλλαγή ξεκινά από τον υπάλληλο, τον εξωτερικό χρήστη ή από τη διοίκηση και τον λόγο τερματισμού
2. Τις τρέχουσες ευθύνες του υπαλλήλου, του εξωτερικού χρήστη ή οποιουδήποτε άλλου χρήστη
3. Την αξία των περιουσιακών στοιχείων που είναι προσβάσιμα αυτήν τη στιγμή

Σε ορισμένες περιπτώσεις, τα δικαιώματα πρόσβασης μπορεί να εκχωρηθούν με βάση το ότι είναι διαθέσιμα σε περισσότερα άτομα από τον αποχωρούντα υπάλληλο ή τον εξωτερικό χρήστη, π.χ. αναγνωριστικά ομάδας. Σε τέτοιες περιπτώσεις, τα άτομα που αναχωρούν θα πρέπει να αφαιρεθούν από οποιεσδήποτε λίστες πρόσβασης και θα πρέπει να γίνουν ρυθμίσεις για να συμβουλεύουν όλους τους άλλους υπαλλήλους και τους εξωτερικούς χρήστες που εμπλέκονται να μην μοιράζονται πλέον αυτές τις πληροφορίες με το άτομο που αναχωρεί.

Σε περιπτώσεις τερματισμού που ξεκινά από τη διαχείριση, οι δυσαρεστημένοι υπάλληλοι ή οι χρήστες εξωτερικών τομέων μπορούν να καταστρέψουν σκόπιμα πληροφορίες ή να σαμποτάρουν εγκαταστάσεις επεξεργασίας πληροφοριών. Σε περιπτώσεις ατόμων που παραιτούνται ή απολύονται, ενδέχεται να συλλέξουν πληροφορίες για μελλοντική χρήση.

8.7. Έλεγχος πρόσβασης στον πηγαίο κώδικα

Η πρόσβαση στον πηγαίο κώδικα του προγράμματος και σε συναφή στοιχεία όπως σχέδια, προδιαγραφές, σχέδια επαλήθευσης και σχέδια επικύρωσης έχει βαρύνουσα σημασία να ελέγχεται αυστηρά προκειμένου να αποφευχθεί η εισαγωγή μη εξουσιοδοτημένης λειτουργικότητας και να αποφευχθούν ακούσιες αλλαγές καθώς και να διατηρηθεί η εμπιστευτικότητα πολύτιμων δεδομένων. Για τον πηγαίο κώδικα προγράμματος, αυτό μπορεί να επιτευχθεί με ελεγχόμενη κεντρική αποθήκευση τέτοιου κώδικα, κατά προτίμηση σε βιβλιοθήκες πηγών προγράμματος. Οι ακόλουθες οδηγίες αφορούν στον έλεγχο της πρόσβασης σε τέτοιες βιβλιοθήκες προέλευσης προγραμμάτων, προκειμένου να μειωθεί η πιθανότητα διαφθοράς των προγραμμάτων υπολογιστών:

- Αποφυγή διατήρησης βιβλιοθηκών πηγών προγράμματος σε λειτουργικά συστήματα
- Διαχείριση του πηγαίου κώδικα προγράμματος και των βιβλιοθηκών πηγών προγράμματος σύμφωνα με καθιερωμένες διαδικασίες
- Περιοσμένη πρόσβαση του προσωπικού υποστήριξης σε βιβλιοθήκες πηγών προγράμματος
- Πραγματοποίηση της ενημέρωσης βιβλιοθηκών πηγών προγράμματος και συναφών στοιχείων και έκδοση πηγών προγράμματος σε προγραμματιστές αποκλειστικά έπειτα από τη λήψη της κατάλληλης εξουσιοδότησης
- Διατήρηση των καταχωρίσεων προγραμμάτων σε ασφαλές περιβάλλον
- Διατήρηση αρχείου καταγραφής ελέγχου για όλες τις προσβάσεις σε βιβλιοθήκες πηγών προγράμματος
- Αυστηρές διαδικασίες ελέγχου αλλαγών για την συντήρηση και την αντιγραφή βιβλιοθηκών πηγών προγράμματος

Εάν ο πηγαίος κώδικας του προγράμματος προορίζεται να δημοσιευτεί, θα χρειαστεί να εφαρμοστούν πρόσθετοι έλεγχοι για να διασφαλιστεί η ακεραιότητά του, όπως η ψηφιακή υπογραφή. (IEC, 2013)

Κεφάλαιο 9: ΣΥΝΔΕΣΗ ΑΝΘΡΩΠΙΝΟΥ ΠΑΡΑΓΟΝΤΑ - ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ

Βάσει των σταδίων που αναλύθηκαν στο Κεφάλαιο 7 και τη συμπεριφορά των εργαζομένων σε καθένα από αυτά, είναι εμφανές το γεγονός ότι ο κάθε οργανισμός θα πρέπει να μεριμνά για τη σωστή εκπαίδευση και επίβλεψη των εργαζομένων του σε κάθε στάδιο ανάπτυξης της συμπεριφοράς ασφάλειας πληροφοριών.

Πλέον, έχοντας αναλύσει τα προβλήματα στη συμπεριφορά των εργαζομένων και τα χαρακτηριστικά της ψυχολογίας τους που τους οδηγούν σε ριψοκίνδυνες ενέργειες για την ασφάλεια των συστημάτων τους από τις Κυβερνοεπιθέσεις, μπορεί να γίνει η διασύνδεση μεταξύ των χαρακτηριστικών αυτών και των κατηγοριών Κυβερνοεπιθέσεων.

9.1. Drive-by Επίθεση

Στην περίπτωση της Drive-by επίθεσης, ο αντίπαλος αποκτά πρόσβαση στο σύστημα του χρήστη, όταν αυτός επισκέπτεται κάποια ιστοσελίδα, η οποία έχει παραβιαστεί.

Σύμφωνα με μελέτη του De Montfort University (Hadlington, 2017), ο εθισμός των εργαζομένων στο διαδίκτυο και η κατάχρησή του εν ώρα εργασίας, είναι ο λόγος που οι εργαζόμενοι επισκέπτονται παραβιασμένους ιστοτόπους ή λαμβάνουν ακούσια κακόβουλο λογισμικό θέτοντας τις πληροφορίες των οργανισμών που εργάζονται σε κίνδυνο. Οι εργαζόμενοι που παρουσιάζουν εθισμό στο διαδίκτυο, παρακάμπτουν τις προειδοποιήσεις για την ασφάλεια των ιστοτόπων που επισκέπτονται και δε συμμορφώνονται εύκολα με τα πρωτόκολλα.

Για να εξαλειφθούν αυτού του είδους οι επιθέσεις, οι εργαζόμενοι πρέπει να αντιληφθούν ότι δεν είναι αποδεκτό να χρησιμοποιούν το διαδίκτυο για σκοπούς που δε σχετίζονται με την εργασία τους. Καθώς οι περισσότεροι εργαζόμενοι θεωρούν πως είναι φυσιολογική αυτή η συμπεριφορά, οι οργανισμοί θα πρέπει να ενημερώνουν και να εκπαιδεύουν τους εργαζόμενους σχετικά με τη συμπεριφορά ασφάλειας πληροφοριών που πρέπει να υιοθετήσουν, ακολουθώντας τα στάδια που αναλύθηκαν

παραπάνω, εφόσον, ακόμα και οι επίσημοι ιστότοποι στους οποίους εισέρχονται στα πλαίσια της εργασίας τους ενδέχεται να παραβιαστούν.

Επίσης, οι χρήστες τείνουν να γεμίζουν τους υπολογιστές τους με περιττές εφαρμογές και προσθήκες προγράμματος περιήγησης που δεν είναι ούτε χρήσιμες ούτε συντηρούνται από τους προγραμματιστές. Η κατάργησή των περιττών εφαρμογών και προσθηκών μειώνει σημαντικά τις πιθανότητες παραβίασης δεδομένων.

Τέλος, όταν ο κατασκευαστής λογισμικού κυκλοφορεί νέα ενημέρωση, οι εγκληματίες του Κυβερνοχώρου προσπαθούν να εκμεταλλευτούν το γεγονός ότι μόνο το 38% των χρηστών αναβαθμίζουν το λογισμικό τους αυτόματα ή αμέσως μόλις είναι διαθέσιμη μία αναβάθμιση, και να επιτεθούν. Για το λόγο αυτό, οι χρήστες θα πρέπει διαμορφώσουν το λειτουργικό τους σύστημα, τα προγράμματα περιήγησης και όλες τις εφαρμογές που είναι εφικτό, ώστε να ενημερώνονται αυτόματα, ενώ για τις υπόλοιπες, θα πρέπει να τις ενημερώνουν το συντομότερο δυνατό. (Laing, 2017)

9.2. Συνημμένο Spearphishing, Σύνδεσμος Spearphishing, Spearphishing μέσω Υπηρεσίας

Σε κάθε περίπτωση Spearphishing ο στόχος των αντιπάλων είναι συγκεκριμένος, είτε αυτός είναι ένας άνθρωπος, μία εταιρία ή ένας κλάδος. Έτσι οι αντίπαλοι βασιζόμενοι στην κοινωνική μηχανική εκμεταλλεύονται τις μηχανικές ενέργειες των εργαζομένων, οι οποίοι δεν ελέγχουν συνήθως την εγκυρότητα του αποστολέα ενός μηνύματος που λαμβάνουν στο ηλεκτρονικό ταχυδρομείο.

Πολλοί υπάλληλοι αγνοούν την απειλή που δημιουργεί μια επίθεση Spearphishing στην επιχείρηση. Κάθε μέρα, εταιρείες σε όλο τον κόσμο εμπιστεύονται την ασφάλεια της επιχείρησής τους και τους πελάτες τους σε υπαλλήλους που δεν ξέρουν πώς να αναγνωρίσουν μια στοχευμένη επίθεση ηλεκτρονικού ψαρέματος. (Vidwans, n.d.)

Για να μειωθεί το ποσοστό επιτυχίας του Spearphishing, οι εργαζόμενοι θα πρέπει να ελέγχουν αν υπάρχουν κακόβουλοι σύνδεσμοι ή συνημμένα, καθώς και την εγκυρότητα του αποστολέα. Επιπλέον, δε θα πρέπει να εισάγουν τους κωδικούς τους ή να παρακάμπτουν τις προειδοποιήσεις ασφαλείας σύμφωνα με τις οδηγίες που τους

δίνονται στα μηνύματα που λαμβάνουν. Η εκπαίδευση των εργαζομένων σε κάθε περίπτωση είναι απαραίτητη.

Παρόλ' αυτά, η αποτελεσματικότητα αυτού του είδους των επιθέσεων δεν είναι εύκολο να εξαληφθεί καθώς ενδέχεται να μην υπάρχουν παραδοσιακοί δείκτες που προειδοποιούν ότι ένα μήνυμα ηλεκτρονικού ταχυδρομείου αποτελεί απειλή. (ATT&CK, 2020)

9.3. Third-party Software

Αυτή η κατηγορία επιθέσεων προκαλείται όταν ένας αντίπαλος αποκτήσει πρόσβαση σε εφαρμογές και συστήματα ανάπτυξης λογισμικού ενός οργανισμού και ευνοείται από την κακή διαχείριση των προσωπικών κωδικών των εργαζομένων στους οργανισμούς.

Για να αποφευχθούν αυτού του είδους οι επιθέσεις, οι εργαζόμενοι θα πρέπει να χρησιμοποιούν ισχυρούς και μοναδικούς κωδικούς που δε θα μοιράζονται με τους συναδέλφους τους και δε θα τους έχουν σημειωμένους σε γραπτή μορφή σε σημεία που έχουν πρόσβαση τρίτοι.

Οι περισσότεροι οργανισμοί υποτιμούν την πιθανότητα να γίνουν θύματα Κυβερνοεπιθέσεων και δε λαμβάνουν τα απαραίτητα μέτρα προστασίας. Θα πρέπει να εφαρμόζεται αυστηρή πολιτική έγκρισης για τη χρήση των συστημάτων ανάπτυξης.

Επιπλέον, θα πρέπει να εκτελείται η ανάπτυξη εφαρμογών σε τακτά χρονικά διαστήματα, ώστε να ξεχωρίζει η ακανόνιστη δραστηριότητα ανάπτυξης και να παρακολουθείται η δραστηριότητα της διαδικασίας που δεν σχετίζεται με γνωστό έγκυρο λογισμικό. Τέλος, πρέπει να παρακολουθείται η δραστηριότητα σύνδεσης λογαριασμού στο σύστημα ανάπτυξης. (ATT&CK, 2020)

9.4. Εκτέλεση Χρήστη

Αντίστοιχα με την περίπτωση του Spearphishing, οι αντίπαλοι βασίζονται στις μηχανικές ενέργειες και την απροσεξία των χρηστών με σκοπό την εκτέλεση κακόβουλου λογισμικού, το οποίο τοποθετείται σε κοινόχρηστο κατάλογο ή στην επιφάνεια εργασίας του χρήστη. Οι χρήστες θα πρέπει να προσέχουν τι αρχεία ανοίγουν, ακόμα και αν αυτά είναι ήδη εγκατεστημένα στο υπολογιστή τους, ιδιαίτερα εάν δεν θυμούνται την προέλευσή τους.

9.5. Επεκτάσεις Προγράμματος Περιήγησης

Εάν οι επεκτάσεις αντί να εκτελούνται με τα πλήρη δικαιώματα του χρήστη, εκτελούνται με ένα περιορισμένο σύνολο προνομίων, το πρόγραμμα περιήγησης παρέχει πρόσβαση στις επεκτάσεις, μόνο σε εκείνα τα δικαιώματα που ζητούνται ρητά στο μανιφέστο της επέκτασης. Εφόσον απαιτείται οι επεκτάσεις να δηλώσουν τα δικαιώματά τους κατά το χρόνο εγκατάστασης, ένας εισβολέας που θέτει σε κίνδυνο μια επέκταση θα περιορίζεται σε αυτά τα δικαιώματα κατά το χρόνο εκτέλεσης. (Adam Barth, n.d.)

Οι εργαζόμενοι θα πρέπει επιπροσθέτως να κλείνουν όλες τις περιόδους σύνδεσης του προγράμματος περιήγησης όταν τελειώνουν τη χρήση τους για να αποτρέψουν τη συνέχιση της εκτέλεσης τυχόν δυνητικά κακόβουλων επεκτάσεων.

Για την ανίχνευση αυτού του είδους επιθέσεων είναι απαραίτητη η παρακολούθηση για τυχόν νέα στοιχεία που έχουν γραφτεί στο μητρώο ή σε αρχεία PE που είναι εγγεγραμμένα στο δίσκο, καθώς μπορεί να σχετίζεται με την εγκατάσταση επέκτασης προγράμματος περιήγησης.

9.6. Στοιχείο Σύνδεσης

Η αποφυγή αυτού του είδους επίθεσης μπορεί να αποφευχθεί εάν αποτρέπεται η τροποποίηση αρχείων plist από τους χρήστες κάνοντάς τα μόνο για ανάγνωση.

Επιπλέον, κρατώντας πατημένο το πλήκτρο shift κατά τη σύνδεση, εμποδίζεται το άνοιγμα των εφαρμογών αυτόματα.

Είναι επίσης απαραίτητη η παρακολούθηση της εκτέλεσης της διαδικασίας για μη φυσιολογική εκτέλεσή της που προκύπτει από τροποποιημένα αρχεία plist καθώς και παρακολούθηση βοηθητικών προγραμμάτων που χρησιμοποιούνται για την τροποποίηση αρχείων plist ή που λαμβάνουν ένα αρχείο plist ως είσοδο, το οποίο μπορεί να υποδηλώνει ύποπτη δραστηριότητα.

Οι ενέργειες αυτές συνήθως δε γίνονται από τους εργαζόμενους και χρειάζεται οι οργανισμοί να εκπαιδεύουν τους εργαζόμενους ακολουθώντας τα στάδια ανάπτυξης του ISB. (ATT&CK, 2020)

9.7. Εκ νέου άνοιγμα Εφαρμογών

Αυτή η επίθεση προκύπτει όταν ο αντίπαλος έχει τροποποιήσει αρχεία που χρησιμοποιούν οι εργαζόμενοι για να συμπεριλάβει έναν σύνδεσμο προς το κακόβουλο εκτελέσιμο πρόγραμμα για να παρέχει έναν μηχανισμό επιμονής κάθε φορά που ο χρήστης κάνει επανεκκίνηση του υπολογιστή του. Για να αποφύγουν αυτή την επίθεση οι εργαζόμενοι θα πρέπει να κρατούν πατημένο το πλήκτρο Shift κατά τη σύνδεση, το οποίο αποτρέπει το άνοιγμα των εφαρμογών αυτόματα.

Για την απενεργοποίηση ή πλήρη κατάργηση αυτών των λειτουργιών ή προγραμμάτων εκτελείται η ακόλουθη εντολή τερματικού: defaults write -g ApplePersistence -bool no. (ATT&CK, 2020)

9.8. Template Injection

Σε αυτή την περίπτωση επιθέσεων, ο αριθμός των επιτυχημένων επιθέσεων μπορεί να μειωθεί εφόσον οι εργαζόμενοι είναι εκπαιδευμένοι σχετικά με τις τεχνικές κοινωνικής μηχανικής που χρησιμοποιούν οι αντίπαλοι και τα μηνύματα ηλεκτρονικού

ψαρέματος (Spearphishing) που τους αποστέλλουν, στα οποία αποκρύπτουν κακόβουλο κώδικα ο οποίος εκτελείται μέσω εγγράφων.

Αντίστοιχα με τις περιπτώσεις Spearphishing, η επιτυχία της επίθεσης τύπου Template Injection βασίζεται στην ημιμάθεια των εργαζόμενων σχετικά με τις ενέργειες για την πρόληψη των Κυβερνοεπιθέσεων.

9.9. Απόρριψη Διαπιστευτηρίων

Βασική απαίτηση για την προστασία από αυτή την επίθεση είναι ο περιορισμός της αλληλεπικάλυψης διαπιστευτηρίων σε λογαριασμούς και συστήματα, εκπαιδεύοντας τους χρήστες και τους διαχειριστές να μην χρησιμοποιούν τον ίδιο κωδικό πρόσβασης για πολλούς λογαριασμούς.

Αντίστοιχα και με τις περισσότερες κατηγορίες επιθέσεων όπου βασικός υπαίτιος είναι το ανθρώπινο λάθος, οι λογαριασμοί των τοπικών διαχειριστών θα πρέπει να ορίζουν πολύπλοκους και μοναδικούς κωδικούς πρόσβασης για όλα τα συστήματα του δικτύου.

9.10. Διαπιστευτήρια σε Αρχεία

Είναι απαραίτητη η εκπαίδευση των χρηστών για να επιβεβαιωθεί ότι οι προγραμματιστές και οι διαχειριστές συστήματος γνωρίζουν τον κίνδυνο που σχετίζεται με την κατοχή κωδικών πρόσβασης απλού κειμένου σε αρχεία διαμόρφωσης λογισμικού που ενδέχεται να παραμείνουν σε συστήματα ή διακομιστές τελικού σημείου (endpoint).

Επιπλέον, ο περιορισμός των κοινόχρηστων αρχείων σε συγκεκριμένους καταλόγους, στους οποίους έχουν πρόσβαση μόνο οι απαραίτητοι χρήστες είναι αναγκαίος, αλλά και η καθιέρωση οργανωτικής πολιτικής που απαγορεύει την αποθήκευση κωδικών πρόσβασης σε αρχεία. (ATT&CK, 2020)

9.11. Προτροπή εισαγωγής – input

Σε αυτή την περίπτωση, οι εργαζόμενοι θα πρέπει να είναι εκπαιδευμένοι και να είναι στο τέταρτο στάδιο ανάπτυξης της ISB ώστε να μπορούν να εφαρμόσουν τα μέτρα για την πρόληψη των Κυβερνοεπιθέσεων και να μην εισαγάγουν διαπιστευτήρια σε προγράμματα αντιπάλων που στοχεύουν στην κλοπή τους. (ATT&CK, 2020)

9.12. Keychain

Για να αντιμετωπιστεί αυτή η κατηγορία επιθέσεων, χρειάζεται να αυξηθεί η πολυπλοκότητα για την είσοδο του αντιπάλου. Για λόγους διευκόλυνσης, οι χρήστες συνήθως χρησιμοποιούν τον ίδιο κωδικό σε πολλαπλούς λογαριασμούς. Μία απλή αλλαγή στον κωδικό πρόσβασης για το keychain ώστε να διαφέρει από τον κωδικό πρόσβασης σύνδεσης του χρήστη είναι αρκετή, διότι αυξάνει την πολυπλοκότητα για έναν αντίπαλο επειδή πρέπει να γνωρίζει έναν επιπλέον κωδικό πρόσβασης για να εισέλθει.

9.13. Κλοπή Web Session Cookies

Οι εργαζόμενοι, για να αποφύγουν την κλοπή των Web Session Cookies θα πρέπει να είναι σωστά εκπαιδευμένοι, ώστε να αντιλαμβάνονται τις προσπάθειες ηλεκτρονικού ψαρέματος, όπου τους ζητείται να εισαγάγουν διαπιστευτήρια σε έναν ιστότοπο που έχει εσφαλμένη διεύθυνση δικτύου για την εφαρμογή στην οποία συνδέονται.

Επιπλέον, οι χρήστες συχνά αποθηκεύουν τους κωδικούς πρόσβασης σε προγράμματα περιήγησης ιστού, όπως το Google Chrome για λόγους διευκόλυνσης. Αυτή η συμπεριφορά όμως, θα πρέπει να αποφεύγεται διότι αυξάνει σημαντικά τον κίνδυνο κλοπής ευαίσθητων δεδομένων, ενώ επίσης είναι αναγκαίος ο καθαρισμός των cookies ανά τακτά χρονικά διαστήματα. (Bartley, 2020)

9.14. Παρακολούθηση ελέγχου ταυτότητας δύο παραγόντων

Στις περιπτώσεις που οι οργανισμοί χρησιμοποιούν έλεγχο ταυτότητας δύο παραγόντων μέσω smart cards θα πρέπει να εκπαιδεύουν τους εργαζόμενους, έτσι ώστε αυτοί να αφαιρούν τις smart cards όταν αυτές δε χρησιμοποιούνται. Με αυτό τον τρόπο επιτυγχάνεται η αποφυγή παρακολούθησης του ελέγχου ταυτότητας.

Επίσης, καθώς και αυτή η επίθεση βασίζεται στην κοινωνική μηχανική, οι Οργανισμοί μπορούν να επενδύσουν σε εκπαιδευτικά προγράμματα ευαισθητοποίησης στον τομέα της κοινωνικής μηχανικής για να εξοπλίσουν τους υπαλλήλους τους έτσι ώστε να αντέχουν σε επιθέσεις κοινωνικής μηχανικής. Οι παραβιάσεις προσομοίωσης και τα πλαστά σενάρια είναι ένας πολύ καλός τρόπος για να κατανοήσουν οι εργαζόμενοι πώς λειτουργεί η κοινωνική μηχανική. (Mitchell, 2019)

9.15. Pass the Ticket, Pass the Hash, Ιδιωτικά Κλειδιά, Εξαναγκαστική Πιστοποίηση

Στην περίπτωση της επίθεσης Pass the ticket, για να περιοριστεί η επίδραση ενός Golden Ticket που ίσως να δημιουργήθηκε προηγουμένως, οι χρήστες θα πρέπει να επαναφέρουν δύο φορές τον ενσωματωμένο κωδικό πρόσβασης λογαριασμού KRBTGT, ο οποίος θα ακυρώσει τυχόν υπάρχοντα Golden Tickets που έχουν δημιουργηθεί με το hash KRBTGT και άλλα εισιτήρια Kerberos που προέρχονται από αυτό.

Επιπλέον, οι εργαζόμενοι που έχουν λογαριασμούς τοπικών διαχειριστών θα πρέπει να χρησιμοποιούν σύνθετους και μοναδικούς κωδικούς πρόσβασης, τους οποίους δε θα μοιράζονται με τρίτους και θα αλλάζουν σε τακτά χρονικά διαστήματα.

Ενώ οι οργανισμοί, θα πρέπει να περιορίζουν τα δικαιώματα των λογαριασμών διαχειριστών τομέα και να μην επιτρέπουν σε έναν χρήστη να είναι τοπικός διαχειριστής για πολλά συστήματα.

Η αντίστοιχη πολιτική διαχείρισης των κωδικών πρόσβασης ισχύει και για την αποτροπή της επίθεσης Pass the hash, μέσω Ιδιωτικών κλειδιών και εξαναγκαστικής πιστοποίησης. (ATT&CK, 2020)

9.16. Kerberoasting

Στην περίπτωση του Kerberoasting είναι πιθανό να εκτεθούν οι κωδικοί πρόσβασης λογαριασμών υπηρεσίας. Ωστόσο, υπάρχουν τρόποι για τον μετριασμό ή και την εξάλειψη αυτού του κινδύνου.

Οι χρήστες θα πρέπει να υιοθετήσουν ισχυρές πρακτικές διαχείρισης των κωδικών πρόσβασης για λογαριασμούς υπηρεσιών. Οι κωδικοί πρόσβασής τους θα πρέπει να δημιουργούνται τυχαία, να αποτελούνται από τουλάχιστον 30 χαρακτήρες και να αντικαθίστανται συχνά.

Όπου είναι δυνατόν, θα πρέπει να υιοθετηθεί η χρήση των λογαριασμών Managed Service Group (gMSA). Οι κωδικοί πρόσβασης (256 τυχαία byte) για τα gMSA δημιουργούνται και αλλάζουν συχνά από την υπηρεσία καταλόγου Active Directory, αφαιρώντας αυτό το φορτίο από τους διαχειριστές. (Stealthbits, 2020)

9.17. Παραβίαση SSH

Σε αυτή την περίπτωση χρειάζεται τα ζεύγη κλειδιών SSH να διαθέτουν ισχυρούς κωδικούς πρόσβασης και να αποφεύγεται η χρήση τεχνολογιών αποθήκευσης κλειδιών όπως το ssh-agent, εκτός εάν προστατεύονται σωστά.

Μέσω της διαχείρισης των προνομιούχων λογαριασμών δεν πρέπει να επιτρέπεται η απομακρυσμένη πρόσβαση μέσω SSH ως root ή άλλων προνομιούχων λογαριασμών.

9.18. Windows Admin Shares

Για την αποτελεσματική αντιμετώπιση αυτής της επίθεσης είναι απαραίτητη η άρνηση απομακρυσμένης χρήσης τοπικών διαπιστευτηρίων διαχειριστή για σύνδεση σε συστήματα και να μην επιτρέπεται στους λογαριασμούς χρηστών τομέα να βρίσκονται στην ομάδα των Local Administrators σε πολλά συστήματα.

Επιπλέον οι χρήστες δεν πρέπει να επαναχρησιμοποιούν κωδικούς πρόσβασης λογαριασμού τοπικού διαχειριστή σε όλα τα συστήματα, ενώ πρέπει να εξασφαλιστεί η πολυπλοκότητα και η μοναδικότητα στους κωδικούς πρόσβασης έτσι ώστε να μην μπορούν να τους σπάσουν ή να τους μαντέψουν.

9.19. Δεδομένα από αποθετήρια πληροφοριών

Για τον περιορισμό των περιπτώσεων κλοπής δεδομένων από τα αποθετήρια πληροφοριών, θα πρέπει να ακολουθείται η “αρχή του ελαχίστου προνομίου” (Principle of Least Privilege - POLP), σύμφωνα με το οποίο οι χρήστες πρέπει να έχουν πρόσβαση μόνο στους πόρους που χρειάζονται, ώστε να μπορούν να εκτελούν επαρκώς τα καθήκοντα που τους αναλογούν. Επιπροσθέτως, θα πρέπει να εφαρμόζονται μηχανισμοί ελέγχου πρόσβασης που περιλαμβάνουν έλεγχο ταυτότητας και εξουσιοδότησης των χρηστών.

Και σε αυτή την περίπτωση είναι αναγκαία η εκπαίδευση των εργαζόμενων, καθώς και η ανάπτυξη και δημοσίευση πολιτικών που ορίζουν ποια είναι η αποδεκτή μορφή των πληροφοριών που πρόκειται να αποθηκευτούν στα αποθετήρια πληροφοριών. (ATT&CK, 2020)

Κεφάλαιο 10: ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι επιθέσεις στον Κυβερνοχώρο αποτελούν ένα πρόβλημα που θα συνεχίσει να υπάρχει και να αυξάνεται στο μέλλον. Οι συνέπειες τους είναι σημαντικές τόσο στον οικονομικό τομέα, αλλά και στην ακεραιότητα των προσωπικών δεδομένων και της πνευματικής ιδιοκτησίας. Εφόσον το ανθρώπινο λάθος είναι καταλυτικός παράγοντας για την επιτυχία μεγάλου μέρους των Κυβερνοεπιθέσεων, η πρόληψή του αποτελεί τον τρόπο εξάλειψής των Κυβερνοεπιθέσεων.

Στη σύγχρονη κοινωνία, οι Οργανισμοί υποτιμούν την πιθανότητα να γίνουν θύματα Κυβερνοεπίθεσης και για το λόγο αυτό δε θέτουν τα μέτρα για την Κυβερνοασφάλεια ως προτεραιότητα για τη λειτουργία τους. Αποτέλεσμα αυτής της κατάστασης είναι οι εργαζόμενοι να συμπεριφέρονται σύμφωνα με τις δικές τους πεποιθήσεις, οι οποίες δεν συνάδουν με τις διαδικασίες ασφάλειας των πληροφοριών.

Για να επιτευχθεί η μείωση του ανθρώπινου σφάλματος, είναι απαραίτητη η εκπαίδευση των εργαζομένων, ώστε να γνωρίζουν τη σημασία του ρόλου τους στην ασφάλεια των πληροφοριών του Οργανισμού στον οποίο εργάζονται, αλλά και ποιες ενέργειές τους θέτουν τον Οργανισμό σε κίνδυνο.

Τα πρώτα βήματα για την προστασία των δεδομένων έγιναν το 2018 με την εφαρμογή του κανονισμού GDPR. Για την περαιτέρω προστασία των πληροφοριών και τη μείωση των επιτυχημένων Κυβερνοεπιθέσεων και των συνεπειών τους, θα μπορούσαν να υπάρχουν κανονισμοί που θα θέτουν ως βασική προυπόθεση για τους Οργανισμούς, ανεξάρτητα από το μέγεθός τους, την εκπαίδευση των εργαζομένων σχετικά με τη Συμπεριφορά Ασφάλειας Πληροφοριών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

99firms, 2020. *99firms.* [Ηλεκτρονικό]
Available at: https://99firms.com/blog/cyber-security-statistics/#:~:text=Cyber%2Dattacks%20occur%202%2C244%20times,of%20breaches%20are%20financially%20motivated.
Accenture, 2019. *Accenture.* [Ηλεκτρονικό]
Available at: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study
Adam Barth, A. P. F. P. S., χ.χ. *Protecting Browsers from Extension Vulnerabilities,* Berkeley: https://static.googleusercontent.com/media/research.google.com/el//pubs/archive/38394.pdf.
Ahola, M., 2019. *usecure.* [Ηλεκτρονικό]
Available at: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches#:~:text=In%20a%20security%20context%2C%20human,security%20breach%20to%20take%20place.&text=This%20all%20adds%20up%2C%20and,make%20life%20easier%20for%20themselves.
ATT&CK, M., 2020. *MITRE ATT&CK.* [Ηλεκτρονικό]
Available at: https://attack.mitre.org/matrices/enterprise/
Bartley, M., 2020. *Security Boulevard.* [Ηλεκτρονικό]
Available at: https://securityboulevard.com/2020/01/how-to-prevent-cookie-stealing-and-hijacking-sessions-easiest-guide/
Cisco, 2020. *Cisco.* [Ηλεκτρονικό]
Available at: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
Fintechnews, 2020. *Fintechnews.* [Ηλεκτρονικό]
Available at: https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/
Hadlington, L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon.*
IBM, 2014. *IBM.* [Ηλεκτρονικό]
Available at: https://research.ibm.com/?lnk=fdi
IEC, I. /., 2013. *ISO / IEC 27002,* s.l.: s.n.
Kaspersky, χ.χ. *Kaspersky.* [Ηλεκτρονικό]
Available at: https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering
Laing, B., 2017. *Lastline.* [Ηλεκτρονικό]
Available at: https://www.lastline.com/blog/drive-by-download/
Mari Karjalainen, M. S. S. S., 2020. Toward a stage theory of the development of employees' information security behavior. *Computers & Security.*
Melnick, J., 2020. *Netwrix Blog.* [Ηλεκτρονικό]
Available at: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
Mitchell, A., 2019. *RCR Wireless.* [Ηλεκτρονικό]
Available at: https://www.rcrwireless.com/20190402/sponsored/how-2fa-can-be-hacked-using-social-engineering

Ohlhorst, F., 2014. *Techrepublic.* [Ηλεκτρονικό]
Available at: https://www.techrepublic.com/article/ibm-says-most-security-breaches-are-eue-to-human-error/
Stealthbits, 2020. *Stealthbits.* [Ηλεκτρονικό]
Available at: https://attack.stealthbits.com/cracking-kerberos-tgs-tickets-using-kerberoasting#:~:text=The%20best%20mitigation%20for%20a,leverage%20long%20and%20complex%20passwords.&text=Using%20group%20managed%20service%20accounts,and%20managed%20centrally%20within%20
Upguard, 2020. *Upguard.* [Ηλεκτρονικό]
Available at: https://www.upguard.com/blog/cybersecurity-important
Varonis, 2020. *Varonis.* [Ηλεκτρονικό]
Available at: https://www.varonis.com/blog/cybersecurity-statistics/
Vidwans, R., χ.χ. *Clearedin.* [Ηλεκτρονικό]
Available at: https://www.clearedin.com/blog/spear-phishing-attack-success