1. Κακόβουλο λογισμικό (Malware)

Το κακόβουλο λογισμικό είναι ένας τύπος εφαρμογής που μπορεί να εκτελέσει μια ποικιλία κακόβουλων εργασιών. Ορισμένα είδη κακόβουλου λογισμικού έχουν σχεδιαστεί για να δημιουργούν μόνιμη πρόσβαση σε ένα δίκτυο, μερικά έχουν σχεδιαστεί για να κατασκοπεύουν τον χρήστη προκειμένου να αποκτήσουν διαπιστευτήρια ή άλλα πολύτιμα δεδομένα, ενώ ορισμένα έχουν σχεδιαστεί απλώς για να προκαλούν διακοπή. Ορισμένες μορφές κακόβουλου λογισμικού έχουν σχεδιαστεί για να εκβιάζουν το θύμα με κάποιο τρόπο. Ίσως η πιο αξιοσημείωτη μορφή κακόβουλου λογισμικού είναι το ransomware - ένα πρόγραμμα που έχει σχεδιαστεί για να κρυπτογραφεί τα αρχεία του θύματος και στη συνέχεια να του ζητά να πληρώσουν λύτρα για να λάβουν το κλειδί αποκρυπτογράφησης.

Πώς να αποτρέψετε επιθέσεις κακόβουλου λογισμικού

Η πρόληψη μολύνσεων από κακόβουλο λογισμικό δεν είναι εύκολη υπόθεση, καθώς απαιτεί μια πολύπλευρη προσέγγιση. Τουλάχιστον, θα χρειαστεί να:

• Βεβαιωθείτε ότι έχετε εγκατεστημένο το πιο πρόσφατο και καλύτερο λογισμικό προστασίας από κακόβουλο λογισμικό/ανεπιθύμητη αλληλογραφία.

• Βεβαιωθείτε ότι το προσωπικό σας είναι εκπαιδευμένο να εντοπίζει κακόβουλα email και ιστότοπους.

• Να έχετε μια ισχυρή πολιτική κωδικών πρόσβασης και να χρησιμοποιείτε έλεγχο ταυτότητας πολλαπλών παραγόντων όπου είναι δυνατόν.

• Διατηρείτε όλο το λογισμικό ενημερωμένο.

• Χρησιμοποιήστε λογαριασμούς διαχειριστή μόνο όταν είναι απολύτως απαραίτητο.

• Ελέγξτε την πρόσβαση σε συστήματα και δεδομένα και τηρήστε αυστηρά το μοντέλο με τα λιγότερα προνόμια.

• Παρακολουθήστε το δίκτυό σας για κακόβουλη δραστηριότητα, συμπεριλαμβανομένης της κρυπτογράφησης ύποπτων αρχείων, της εισερχόμενης/εξερχόμενης κίνησης δικτύου, ζητημάτων απόδοσης κ.λπ.

2. Ηλεκτρονικό Ψάρεμα (Phishing)

Μια επίθεση phishing είναι όπου ο εισβολέας προσπαθεί να ξεγελάσει ένα ανυποψίαστο θύμα για να του παραδώσει πολύτιμες πληροφορίες, όπως κωδικούς πρόσβασης, στοιχεία πιστωτικής κάρτας, πνευματική ιδιοκτησία κ.λπ. Οι επιθέσεις ηλεκτρονικού ψαρέματος συχνά φτάνουν με τη μορφή μηνύματος ηλεκτρονικού ταχυδρομείου που προσποιείται ότι προέρχεται από έναν νόμιμο οργανισμό, όπως η τράπεζά σας, η φορολογική υπηρεσία ή κάποια άλλη αξιόπιστη οντότητα. Το phishing είναι ίσως η πιο κοινή μορφή κυβερνοεπίθεσης, κυρίως επειδή είναι εύκολο να πραγματοποιηθεί και εκπληκτικά αποτελεσματικό.

Πώς να αποτρέψετε τις επιθέσεις phishing

Δεδομένου ότι οι επιθέσεις phishing χρησιμοποιούνται συχνά για να εξαπατήσουν ένα θύμα ώστε να εγκαταστήσει κακόβουλο λογισμικό στη συσκευή του, οι τεχνικές που χρησιμοποιούνται για την αποτροπή επιθέσεων ηλεκτρονικού ψαρέματος είναι σχεδόν οι ίδιες με την πρόληψη επιθέσεων κακόβουλου λογισμικού. Ωστόσο, θα μπορούσαμε να πούμε ότι οι επιθέσεις phishing είναι κυρίως αποτέλεσμα αμέλειας και, ως εκ τούτου, η εκπαίδευση ευαισθητοποίησης για την ασφάλεια θα ήταν ο καλύτερος τρόπος για την αποτροπή τους. Οι εργαζόμενοι θα πρέπει να είναι επαρκώς εκπαιδευμένοι για να αναγνωρίζουν ύποπτα email, συνδέσμους και ιστότοπους και να μην γνωρίζουν να εισάγουν πληροφορίες ή να κάνουν λήψη αρχείων από ιστότοπους που δεν εμπιστεύονται. Θα ήταν επίσης καλή ιδέα να κατεβάσετε τυχόν πρόσθετα που μπορούν να σας βοηθήσουν να εντοπίσετε κακόβουλους ιστότοπους**.**

10 Συμβουλές για την Αποτροπή Επιθέσεων Phishing – Συμβουλές για την αποτροπή επιθέσεων

Για τις 10 απλές συμβουλές για τον εντοπισμό και την πρόληψη των απατών phishing, πατήστε τον πιο κάτω σύνδεσμο.

https://bit.ly/3KujJ7e

1. Μάθετε πώς μοιάζει μια απάτη phishing

Νέες μέθοδοι επίθεσης phishing αναπτύσσονται συνεχώς, αλλά μοιράζονται κοινά στοιχεία που μπορούν να εντοπιστούν, αν ξέρετε τι να αναζητήσετε. Υπάρχουν πολλοί ιστότοποι στο διαδίκτυο που θα σας κρατούν ενήμερους για τις πιο πρόσφατες επιθέσεις phishing και τα βασικά τους αναγνωριστικά. Όσο νωρίτερα μάθετε για τις πιο πρόσφατες μεθόδους επίθεσης και τις μοιραστείτε με τους χρήστες σας μέσω τακτικής εκπαίδευσης ευαισθητοποίησης σχετικά με την ασφάλεια, τόσο πιο πιθανό είναι να αποφύγετε μια πιθανή επίθεση.

2. Μην κάνετε κλικ σε συνδέσμους

Γενικά δεν συνιστάται να κάνετε κλικ σε έναν σύνδεσμο σε ένα email ή ένα άμεσο μήνυμα, ακόμα κι αν γνωρίζετε τον αποστολέα. Το ελάχιστο που πρέπει να κάνετε είναι να τοποθετείτε τον δείκτη του ποντικιού πάνω από τον σύνδεσμο για να δείτε εάν ο προορισμός είναι ο σωστός. Ορισμένες επιθέσεις phishing είναι αρκετά περίπλοκες και η διεύθυνση URL προορισμού μπορεί να μοιάζει με αντίγραφο του γνήσιου ιστότοπου, που έχει ρυθμιστεί για να καταγράφει πατήματα πλήκτρων ή να κλέβει πληροφορίες σύνδεσης/πιστωτικής κάρτας. Εάν είναι δυνατόν να μεταβείτε απευθείας στον ιστότοπο μέσω της μηχανής αναζήτησής σας, αντί να κάνετε κλικ στον σύνδεσμο, τότε θα πρέπει να το κάνετε.

3. Αποκτήστε δωρεάν πρόσθετα (add-ons) κατά του phishing

Τα περισσότερα προγράμματα περιήγησης στις μέρες μας σάς επιτρέπουν να κάνετε λήψη πρόσθετων που εντοπίζουν τα σημάδια ενός κακόβουλου ιστότοπου ή σας ειδοποιούν για γνωστούς ιστότοπους ηλεκτρονικού ψαρέματος. Συνήθως είναι εντελώς δωρεάν, επομένως δεν υπάρχει λόγος να μην το έχετε εγκαταστήσει σε κάθε συσκευή στον οργανισμό σας.

4. Μην δίνετε τις πληροφορίες σας σε μη ασφαλή ιστότοπο

Εάν η διεύθυνση URL του ιστότοπου δεν ξεκινά με “https” ή δεν μπορείτε να δείτε ένα εικονίδιο κλειστού λουκέτου δίπλα στη διεύθυνση URL, μην εισαγάγετε ευαίσθητες πληροφορίες ή μην πραγματοποιήσετε λήψη αρχείων από αυτόν τον ιστότοπο. Οι ιστότοποι χωρίς πιστοποιητικά ασφαλείας μπορεί να μην

προορίζονται για απάτες ηλεκτρονικού “ψαρέματος” (phishing), αλλά είναι καλύτερο να είστε ασφαλείς παρά να λυπάστε.

5. Εναλλάσσετε τακτικά τους κωδικούς πρόσβασης

Εάν διαθέτετε διαδικτυακούς λογαριασμούς, θα πρέπει να συνηθίσετε να εναλλάσσετε τακτικά τους κωδικούς πρόσβασής σας, ώστε να αποτρέψετε έναν εισβολέα από το να αποκτήσει απεριόριστη πρόσβαση. Οι λογαριασμοί σας μπορεί να έχουν παραβιαστεί χωρίς να το γνωρίζετε, επομένως η προσθήκη αυτού του επιπλέον επιπέδου προστασίας μέσω της εναλλαγής κωδικού πρόσβασης μπορεί να αποτρέψει συνεχείς επιθέσεις και να αποκλείσει πιθανούς εισβολείς.

6. Μην αγνοείτε τις ενημερώσεις

Η λήψη πολλών μηνυμάτων ενημέρωσης μπορεί να είναι απογοητευτική και μπορεί να είναι δελεαστικό να τα αναβάλλετε ή να τα αγνοήσετε εντελώς. Μην το κάνετε αυτό. Οι ενημερώσεις κώδικα ασφαλείας και οι ενημερώσεις κυκλοφορούν για κάποιο λόγο, συνήθως για να ενημερώνονται για τις σύγχρονες μεθόδους κυβερνοεπίθεσης διορθώνοντας τρύπες στην ασφάλεια. Εάν δεν ενημερώσετε το πρόγραμμα περιήγησής σας, ενδέχεται να κινδυνεύετε από επιθέσεις phishing μέσω γνωστών τρωτών σημείων που θα μπορούσαν εύκολα να είχαν αποφευχθεί.

7. Εγκαταστήστε τείχη προστασίας

Τα τείχη προστασίας είναι ένας αποτελεσματικός τρόπος αποτροπής εξωτερικών επιθέσεων, λειτουργώντας ως ασπίδα μεταξύ του υπολογιστή σας και ενός εισβολέα. Τόσο τα τείχη προστασίας επιφάνειας εργασίας όσο και τα τείχη προστασίας δικτύου, όταν χρησιμοποιούνται μαζί, μπορούν να ενισχύσουν την ασφάλειά σας και να μειώσουν τις πιθανότητες διείσδυσης χάκερ στο περιβάλλον σας.

8. Μην δελεάζεστε από αυτά τα αναδυόμενα παράθυρα

Τα αναδυόμενα παράθυρα δεν είναι απλώς ενοχλητικά. Συχνά συνδέονται με κακόβουλο λογισμικό ως μέρος απόπειρας επιθέσεων phishing. Τα περισσότερα

προγράμματα περιήγησης σάς επιτρέπουν πλέον να κάνετε λήψη και εγκατάσταση δωρεάν λογισμικού αποκλεισμού διαφημίσεων που θα αποκλείει αυτόματα τα περισσότερα από τα κακόβουλα αναδυόμενα παράθυρα. Αν κάποιος καταφέρει να αποφύγει τον αποκλεισμό διαφημίσεων, μην μπείτε στον πειρασμό να κάνετε κλικ! Περιστασιακά, τα αναδυόμενα παράθυρα θα προσπαθήσουν να σας εξαπατήσουν με το σημείο που βρίσκεται το κουμπί "Κλείσιμο", επομένως πάντα να προσπαθείτε να αναζητάτε ένα "x" σε μια από τις γωνίες.

9. Μην δίνετε σημαντικές πληροφορίες στο διαδίκτυο

Ως γενικός εμπειρικός κανόνας, εκτός και αν εμπιστεύεστε 100% τον ιστότοπο στον οποίο βρίσκεστε, δεν πρέπει να δίνετε πρόθυμα τα στοιχεία της κάρτας σας. Βεβαιωθείτε, εάν πρέπει να δώσετε τα στοιχεία σας, ότι επαληθεύετε ότι ο ιστότοπος είναι γνήσιος, ότι η εταιρεία είναι πραγματική και ότι ο ίδιος ο ιστότοπος είναι ασφαλής.

10. Έχετε μια πλατφόρμα ασφαλείας δεδομένων για να εντοπίζετε σημάδια επίθεσης

Εάν είστε αρκετά άτυχος να πέσετε θύμα μιας επιτυχημένης επίθεσης phishing, τότε είναι σημαντικό να είστε σε θέση να εντοπίσετε και να αντιδράσετε έγκαιρα. Η ύπαρξη μιας πλατφόρμας ασφάλειας δεδομένων βοηθά στην απομάκρυνση της πίεσης από την ομάδα IT/Security, ειδοποιώντας αυτόματα για ανώμαλη συμπεριφορά των χρηστών και ανεπιθύμητες αλλαγές στα αρχεία. Εάν ένας εισβολέας έχει πρόσβαση στις ευαίσθητες πληροφορίες σας, οι πλατφόρμες ασφαλείας δεδομένων μπορούν να βοηθήσουν στον εντοπισμό του επηρεαζόμενου λογαριασμού, ώστε να μπορείτε να λάβετε μέτρα για να αποτρέψετε περαιτέρω ζημιές.)

3. Επίθεση Man-in-the-Middle (MITM)

Μια επίθεση που ονομάζεται άνθρωπος στη μέση (MITM) είναι όπου ένας εισβολέας παρεμποδίζει την επικοινωνία μεταξύ δύο μερών σε μια προσπάθεια να κατασκοπεύσει τα θύματα, να κλέψει προσωπικές πληροφορίες ή διαπιστευτήρια ή ίσως να αλλάξει τη συνομιλία με κάποιο τρόπο. Οι επιθέσεις MITM είναι λιγότερο συχνές αυτές τις μέρες, καθώς τα περισσότερα συστήματα email και συνομιλίας χρησιμοποιούν κρυπτογράφηση από άκρο σε άκρο, η οποία εμποδίζει τρίτα μέρη να παραβιάζουν τα δεδομένα που μεταδίδονται μέσω του δικτύου, ανεξάρτητα από το αν το δίκτυο είναι ασφαλές ή όχι.

Πώς να αποτρέψετε τις επιθέσεις MITM

Εάν τα πρωτόκολλα επικοινωνίας που χρησιμοποιείτε δεν διαθέτουν κρυπτογράφηση από άκρο σε άκρο, σκεφτείτε να χρησιμοποιήσετε ένα VPN (ένα εικονικό ιδιωτικό δίκτυο) όταν συνδέεστε στο δίκτυό σας, ειδικά εάν συνδέεστε από δημόσιο σημείο πρόσβασης Wi-Fi. Προσοχή στους ψεύτικους ιστότοπους, τα παρεμβατικά αναδυόμενα παράθυρα και τα μη έγκυρα πιστοποιητικά και αναζητήστε "HTTPS" στην αρχή κάθε διεύθυνσης URL.

4. Κατανεμημένη επίθεση άρνησης υπηρεσίας (DDoS).

Μια επίθεση DDoS είναι όπου ένας εισβολέας ουσιαστικά πλημμυρίζει έναν διακομιστή στόχο με κίνηση σε μια προσπάθεια να διακόψει, και ίσως ακόμη και να καταρρίψει τον στόχο. Ωστόσο, σε αντίθεση με τις παραδοσιακές επιθέσεις άρνησης υπηρεσίας, τις οποίες τα περισσότερα εξελιγμένα τείχη προστασίας μπορούν να ανιχνεύσουν και να ανταποκριθούν, μια επίθεση DDoS είναι σε θέση να αξιοποιήσει πολλαπλές παραβιασμένες συσκευές προκειμένου να βομβαρδίσει τον στόχο με κίνηση.

Πώς να αποτρέψετε τις επιθέσεις DDoS

Η αποτροπή επιθέσεων DDoS είναι δύσκολη επειδή υπάρχουν λίγα προειδοποιητικά σημάδια που πρέπει να προσέξετε και λίγοι τρόποι να σταματήσετε πραγματικά την επίθεση μόλις ξεκινήσει. Η χρήση ενός τείχους προστασίας επόμενης γενιάς ή ενός συστήματος αποτροπής εισβολής (IPS) θα

σας δώσει πληροφορίες σε πραγματικό χρόνο για τυχόν ασυνέπειες στην κυκλοφορία, ζητήματα απόδοσης δικτύου, διακοπτόμενα σφάλματα ιστού και ούτω καθεξής. Θα ήταν επίσης καλή ιδέα να τοποθετήσετε τους διακομιστές σας σε διαφορετικά κέντρα δεδομένων, καθώς αυτό θα σας επιτρέψει να μεταβείτε σε άλλο διακομιστή εάν αποτύχει ο τρέχων. Με πολλούς τρόπους, ο καλύτερος τρόπος για να υπερασπιστείτε το δίκτυό σας από επιθέσεις DDoS είναι να έχετε ένα δοκιμασμένο σχέδιο απόκρισης, το οποίο θα σας επιτρέψει να επαναφέρετε τα συστήματά σας στο διαδίκτυο το συντομότερο δυνατόν και να διατηρήσετε τις επιχειρηματικές λειτουργίες. Θα πρέπει να σημειωθεί ότι πολλοί πάροχοι υπηρεσιών που βασίζονται σε σύννεφο προσφέρουν δυνατότητες πλεονασμού δικτύου, οι οποίες περιλαμβάνουν τη δημιουργία διπλότυπων αντιγράφων των δεδομένων σας, στα οποία μπορείτε να μεταβείτε γρήγορα εάν είναι απαραίτητο.

5. SQL Injection

Η ένεση SQL είναι ένας τύπος επίθεσης που είναι συγκεκριμένος για βάσεις δεδομένων SQL. Οι βάσεις δεδομένων SQL χρησιμοποιούν εντολές SQL για να υποβάλουν ερωτήματα στα δεδομένα και αυτές οι δηλώσεις εκτελούνται συνήθως μέσω μιας φόρμας HTML σε μια ιστοσελίδα. Εάν τα δικαιώματα της βάσης δεδομένων δεν έχουν ρυθμιστεί σωστά, ο εισβολέας ενδέχεται να μπορεί να εκμεταλλευτεί τη φόρμα HTML για να εκτελέσει ερωτήματα που θα δημιουργήσουν, θα διαβάσουν, θα τροποποιήσουν ή θα διαγράψουν τα δεδομένα που είναι αποθηκευμένα στη βάση δεδομένων.

Πώς να αποτρέψετε την επίθεση SQL Injection

Ο μόνος τρόπος για να αποτρέψετε επιθέσεις SQL injection είναι να διασφαλίσετε ότι οι προγραμματιστές ιστού έχουν απολυμάνει σωστά όλες τις εισόδους. Με άλλα λόγια, τα δεδομένα δεν μπορούν να ληφθούν απευθείας από ένα πλαίσιο εισαγωγής, όπως ένα πεδίο κωδικού πρόσβασης, και να αποθηκευτούν σε μια βάση δεδομένων. Αντίθετα, ο εισαγόμενος κωδικός πρόσβασης πρέπει να επικυρωθεί για να διασφαλιστεί ότι πληροί προκαθορισμένα κριτήρια.

6. Zero-day Exploit

Ένα zero-day exploit είναι όπου οι εγκληματίες του κυβερνοχώρου μαθαίνουν για μια ευπάθεια που έχει ανακαλυφθεί σε ορισμένες ευρέως χρησιμοποιούμενες εφαρμογές λογισμικού και λειτουργικά συστήματα και, στη συνέχεια, στοχεύουν οργανισμούς που χρησιμοποιούν αυτό το λογισμικό για να εκμεταλλευτούν την ευπάθεια πριν γίνει διαθέσιμη μια επιδιόρθωση.

Πώς να αποτρέψετε τις εκμεταλλεύσεις Zero-Day

Οι παραδοσιακές λύσεις προστασίας από ιούς δεν είναι αποτελεσματικές έναντι των απειλών μηδενικής ημέρας, καθώς δεν είναι ακόμη γνωστές. Ως εκ τούτου, δεν υπάρχει κανένας ανόητος τρόπος αποτροπής τέτοιων επιθέσεων. Ωστόσο, οι λύσεις προστασίας από ιούς επόμενης γενιάς (NGAV) μπορούν να βοηθήσουν στην αποτροπή των εισβολέων από την εγκατάσταση άγνωστου λογισμικού στον υπολογιστή του θύματος. Φυσικά, η διατήρηση όλου του λογισμικού ενημερωμένο θα βοηθήσει στην εξάλειψη των τρωτών σημείων και η ύπαρξη ενός δοκιμασμένου και δοκιμασμένου σχεδίου αντιμετώπισης περιστατικών θα σας βοηθήσει να ανακάμψετε γρήγορα σε περίπτωση μόλυνσης.

7. DNS Tunneling

Η σήραγγα DNS είναι ένας εξελιγμένος φορέας επίθεσης που έχει σχεδιαστεί για να παρέχει στους εισβολείς μόνιμη πρόσβαση σε έναν δεδομένο στόχο. Δεδομένου ότι πολλοί οργανισμοί αποτυγχάνουν να παρακολουθήσουν την κυκλοφορία DNS για κακόβουλη δραστηριότητα, οι εισβολείς μπορούν να εισάγουν ή να «διώξουν» κακόβουλο λογισμικό σε ερωτήματα DNS (αιτήματα DNS που αποστέλλονται από τον πελάτη στον διακομιστή). Το κακόβουλο λογισμικό χρησιμοποιείται για τη δημιουργία ενός σταθερού καναλιού επικοινωνίας που τα περισσότερα τείχη προστασίας δεν μπορούν να ανιχνεύσουν.

Πώς να αποτρέψετε το DNS Tunneling

Δεδομένου ότι τα παραδοσιακά τείχη προστασίας και το λογισμικό AV δεν είναι σε θέση να ανιχνεύσει τη σήραγγα DNS, πιθανότατα θα χρειαστεί να επενδύσετε σε εξειδικευμένα εργαλεία, όπως το TunnelGuard, το Zscaler και το DNSFilter. Θα

πρέπει να βεβαιωθείτε ότι τα εργαλεία που χρησιμοποιείτε μπορούν να εμποδίσουν αυτόματα την εκτέλεση κακόβουλου λογισμικού που περιέχεται σε κακόβουλα ερωτήματα DNS. Θα πρέπει επίσης να καταγράφει στη μαύρη λίστα προορισμούς που είναι γνωστό ότι χρησιμοποιούνται για εξαγωγή δεδομένων και να παρέχει ανάλυση σε πραγματικό χρόνο όλων των ερωτημάτων DNS για ύποπτα μοτίβα.

8. Business Email Compromise (BEC)

Μια επίθεση BEC είναι όπου ο εισβολέας στοχεύει συγκεκριμένα άτομα, συνήθως έναν υπάλληλο που έχει τη δυνατότητα να εξουσιοδοτεί οικονομικές συναλλαγές, προκειμένου να τους εξαπατήσει να μεταφέρουν χρήματα σε έναν λογαριασμό που ελέγχεται από τον εισβολέα. Οι επιθέσεις BEC συνήθως περιλαμβάνουν σχεδιασμό και έρευνα προκειμένου να είναι αποτελεσματικές. Για παράδειγμα, οποιαδήποτε πληροφορία σχετικά με τα στελέχη, τους υπαλλήλους, τους πελάτες, τους επιχειρηματικούς συνεργάτες και τους πιθανούς επιχειρηματικούς συνεργάτες του οργανισμού-στόχου, θα βοηθήσει τον εισβολέα να πείσει τον υπάλληλο να παραδώσει τα κεφάλαια. Οι επιθέσεις BEC είναι μια από τις πιο επιζήμιες οικονομικά μορφές κυβερνοεπίθεσης.

Πώς να αποτρέψετε τις επιθέσεις BEC

Όπως και με άλλες επιθέσεις phishing, η εκπαίδευση ευαισθητοποίησης για την ασφάλεια είναι ο καλύτερος τρόπος για την πρόληψη του BEC. Οι εργαζόμενοι πρέπει να εκπαιδευτούν ώστε να προσέχουν μηνύματα ηλεκτρονικού ταχυδρομείου με ψεύτικο τομέα ή μηνύματα ηλεκτρονικού ταχυδρομείου που υποδύονται έναν προμηθευτή, εμφανίζουν μια αίσθηση επείγοντος και οτιδήποτε άλλο φαίνεται ύποπτο.

9. Cryptojacking

Το Cryptojacking είναι όπου οι εγκληματίες του κυβερνοχώρου παραβιάζουν τον υπολογιστή ή τη συσκευή ενός χρήστη και τον χρησιμοποιούν για την εξόρυξη κρυπτονομισμάτων, όπως το Bitcoin. Το Cryptojacking δεν είναι τόσο γνωστό όσο

άλλοι φορείς επίθεσης, ωστόσο, δεν πρέπει να υποτιμάται. Οι οργανισμοί δεν έχουν μεγάλη ορατότητα όταν πρόκειται για αυτόν τον τύπο επίθεσης, πράγμα που σημαίνει ότι ένας χάκερ θα μπορούσε να χρησιμοποιεί πολύτιμους πόρους δικτύου για την εξόρυξη ενός κρυπτονομίσματος χωρίς ο οργανισμός να το γνωρίζει. Φυσικά, η απόπλυση πόρων από ένα εταιρικό δίκτυο είναι πολύ λιγότερο προβληματική από την κλοπή πολύτιμων δεδομένων.

Πώς να αποτρέψετε το Cryptojacking

Για να προστατεύσετε το δίκτυό σας από το Cryptojacking, θα χρειαστεί να παρακολουθείτε τη χρήση της CPU όλων των συσκευών δικτύου, συμπεριλαμβανομένης οποιασδήποτε υποδομής που βασίζεται σε σύννεφο που χρησιμοποιείτε. Είναι επίσης καλή ιδέα να εκπαιδεύσετε τους υπαλλήλους σας να προσέχουν τυχόν προβλήματα απόδοσης ή ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, τα οποία μπορεί να περιέχουν κακόβουλο λογισμικό Cryptojacking.

10. Drive-by Attack

Μια επίθεση «drive-by-download» είναι όταν ένα ανυποψίαστο θύμα επισκέπτεται έναν ιστότοπο ο οποίος με τη σειρά του μολύνει τη συσκευή του με κακόβουλο λογισμικό. Ο εν λόγω ιστότοπος μπορεί να είναι αυτός που ελέγχεται άμεσα από τον εισβολέα ή αυτός που έχει παραβιαστεί. Σε ορισμένες περιπτώσεις, το κακόβουλο λογισμικό εμφανίζεται σε περιεχόμενο όπως πανό και διαφημίσεις. Αυτές τις μέρες, είναι διαθέσιμα κιτ εκμετάλλευσης που επιτρέπουν στους αρχάριους χάκερ να εγκαταστήσουν εύκολα κακόβουλους ιστότοπους ή να διανέμουν κακόβουλο περιεχόμενο με άλλα μέσα.

Πώς να αποτρέψετε τις επιθέσεις Drive-by

Για να ελαχιστοποιήσετε την πιθανότητα σύλληψης σε επίθεση με αυτοκίνητο, πρώτα αφαιρέστε τυχόν περιττά πρόσθετα του προγράμματος περιήγησης, καθώς μερικές φορές μπορούν να χρησιμοποιηθούν σε τέτοιες επιθέσεις. Εγκαταστήστε ένα πρόγραμμα αποκλεισμού διαφημίσεων ή χρησιμοποιήστε ένα πρόγραμμα περιήγησης ιστού που εστιάζει στο απόρρητο/την ασφάλεια. Φυσικά, η

απενεργοποίηση τόσο της Java όσο και της JavaScript στο πρόγραμμα περιήγησης θα βελτιώσει την ασφάλεια, αν και κάτι τέτοιο θα περιορίσει τη λειτουργικότητα του προγράμματος περιήγησης. Είναι πάντα μια καλή ιδέα να θυμάστε να μην χρησιμοποιείτε ένα προνόμιο

11. Cross-site Scripting (XSS) Attacks

Οι επιθέσεις δέσμης ενεργειών μεταξύ τοποθεσιών είναι αρκετά παρόμοιες με τις επιθέσεις SQL injection, αν και αντί για εξαγωγή δεδομένων από μια βάση δεδομένων, συνήθως χρησιμοποιούνται για να μολύνουν άλλους χρήστες που επισκέπτονται τον ιστότοπο. Ένα απλό παράδειγμα θα ήταν η ενότητα σχολίων σε μια ιστοσελίδα. Εάν η εισαγωγή του χρήστη δεν φιλτραριστεί πριν από τη δημοσίευση του σχολίου, ένας εισβολέας μπορεί να δημοσιεύσει ένα κακόβουλο σενάριο που είναι κρυμμένο στη σελίδα. Όταν ένας χρήστης επισκέπτεται αυτήν τη σελίδα, το σενάριο θα εκτελεστεί και είτε θα μολύνει τη συσκευή του είτε θα χρησιμοποιηθεί για την κλοπή cookies ή ίσως ακόμη και για την εξαγωγή των διαπιστευτηρίων του χρήστη. Εναλλακτικά, μπορεί απλώς να ανακατευθύνουν τον χρήστη σε έναν κακόβουλο ιστότοπο.

Πώς να αποτρέψετε την επίθεση δέσμης ενεργειών μεταξύ τοποθεσιών

Η δέσμη ενεργειών μεταξύ τοποθεσιών είναι ένα σύνθετο θέμα και απαιτεί βασική κατανόηση των εννοιών και των τεχνολογιών ανάπτυξης ιστού, όπως HTML και JavaScript. Ωστόσο, με απλά λόγια, οι τεχνικές που χρησιμοποιούνται για την αποτροπή επιθέσεων XSS είναι παρόμοιες με αυτές που χρησιμοποιούνται για την αποτροπή επιθέσεων SQL injection. Ουσιαστικά, πρέπει να βεβαιωθείτε ότι όλες οι είσοδοι έχουν απολυμανθεί σωστά για να διασφαλίσετε ότι οι αντίπαλοι δεν μπορούν να εισάγουν κακόβουλα σενάρια σε ιστοσελίδες. Πρέπει να βεβαιωθείτε ότι τυχόν ειδικοί χαρακτήρες που εισάγονται από τους χρήστες δεν αποδίδονται στην ιστοσελίδα σας.

12. Password Attack

Μια επίθεση με κωδικό πρόσβασης, όπως ίσως έχετε ήδη μαντέψει, είναι ένας τύπος κυβερνοεπίθεσης όπου ένας εισβολέας προσπαθεί να μαντέψει ή να «σπάσει» τον κωδικό πρόσβασης ενός χρήστη. Υπάρχουν πολλές διαφορετικές τεχνικές για το σπάσιμο του κωδικού πρόσβασης ενός χρήστη, αν και η εξήγηση αυτών των διαφορετικών τεχνικών ξεφεύγει από το πεδίο εφαρμογής αυτού του άρθρου. Ωστόσο, ορισμένα παραδείγματα περιλαμβάνουν την επίθεση Brute-Force, την επίθεση Dictionary, την επίθεση Rainbow Table, Credential Stuffing, Password Spraying και την επίθεση Keylogger. Και φυσικά, οι επιτιθέμενοι θα προσπαθήσουν συχνά να χρησιμοποιήσουν τεχνικές Phishing για να αποκτήσουν τον κωδικό πρόσβασης ενός χρήστη.

Πώς να αποτρέψετε τις επιθέσεις με κωδικό πρόσβασης

Το πρώτο βήμα για την αποτροπή επιθέσεων με κωδικό πρόσβασης είναι να διασφαλίσετε ότι έχετε εφαρμόσει μια ισχυρή πολιτική κωδικών πρόσβασης και να χρησιμοποιήσετε τον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) όπου είναι δυνατόν. Είναι επίσης καλή ιδέα να πραγματοποιήσετε δοκιμές διείσδυσης για τον εντοπισμό τρωτών σημείων. Χρησιμοποιήστε μια λύση ελέγχου σε πραγματικό χρόνο που μπορεί να παρακολουθεί και να ανταποκρίνεται σε ύποπτες προσπάθειες σύνδεσης.

13. Eavesdropping Attacks

Μερικές φορές αναφέρεται ως "snooping" ή "sniffing", μια επίθεση υποκλοπής είναι όπου ο εισβολέας αναζητά μη ασφαλείς επικοινωνίες δικτύου σε μια προσπάθεια υποκλοπής και πρόσβασης σε δεδομένα που αποστέλλονται μέσω του δικτύου. Αυτός είναι ένας από τους λόγους για τους οποίους ζητείται από τους εργαζόμενους να χρησιμοποιούν VPN όταν έχουν πρόσβαση στο δίκτυο της εταιρείας από ένα μη ασφαλές δημόσιο σημείο πρόσβασης Wi-Fi.

Πώς να αποτρέψετε τις επιθέσεις υποκλοπής

Όπως και με τις επιθέσεις MITM, ο καλύτερος τρόπος για να αποτρέψετε τις επιθέσεις υποκλοπής είναι να διασφαλίσετε ότι όλα τα ευαίσθητα δεδομένα είναι κρυπτογραφημένα, τόσο σε κατάσταση ηρεμίας όσο και κατά τη μεταφορά. Τα

τείχη προστασίας, τα VPN και οι λύσεις κατά του κακόβουλου λογισμικού παρέχουν μια ουσιαστική άμυνα έναντι τέτοιων επιθέσεων. Εξετάστε το ενδεχόμενο να τμηματοποιήσετε το δίκτυό σας και υιοθετήστε ένα μοντέλο μηδενικής εμπιστοσύνης, όπου όλα τα εισερχόμενα πακέτα απαιτούνται για τον έλεγχο ταυτότητας. Χρησιμοποιήστε μια λύση αποτροπής εισβολής για να παρακολουθείτε το δίκτυό σας για ύποπτη κίνηση και να απορρίψετε τυχόν πακέτα με πλαστές διευθύνσεις. Δεδομένου ότι πολλές επιθέσεις υποκλοπής βασίζονται σε κακόβουλο λογισμικό για να μολύνουν κανάλια επικοινωνίας, οι εργαζόμενοι πρέπει να είναι επαρκώς εκπαιδευμένοι για να εντοπίζουν απόπειρες ηλεκτρονικού ψαρέματος.

14. AI-Powered Attacks

Η χρήση της Τεχνητής Νοημοσύνης για την εκτόξευση εξελιγμένων επιθέσεων στον κυβερνοχώρο είναι μια τρομακτική προοπτική, καθώς δεν γνωρίζουμε ακόμη τι μπορούν να κάνουν τέτοιες επιθέσεις. Η πιο αξιοσημείωτη επίθεση με τεχνητή νοημοσύνη που έχουμε δει μέχρι σήμερα περιλάμβανε τη χρήση botnets με τεχνητή νοημοσύνη, τα οποία χρησιμοποιούσαν slave μηχανές για να εκτελέσουν μια τεράστια επίθεση DDoS. Ωστόσο, είναι πιθανό να δούμε πολύ πιο εξελιγμένους φορείς επίθεσης στο μέλλον. Το λογισμικό που λειτουργεί με τεχνητή νοημοσύνη είναι σε θέση να μάθει ποια είδη προσεγγίσεων λειτουργούν καλύτερα και να προσαρμόσει τις μεθόδους επίθεσης ανάλογα. Μπορούν να χρησιμοποιούν τροφοδοσίες πληροφοριών για να εντοπίζουν γρήγορα τρωτά σημεία λογισμικού, καθώς και να σαρώνουν τα ίδια τα συστήματα για πιθανές ευπάθειες. Το κείμενο, ο ήχος και το βίντεο που δημιουργείται από την τεχνητή νοημοσύνη θα χρησιμοποιηθούν για την πλαστοπροσωπία των στελεχών της εταιρείας, τα οποία μπορούν να χρησιμοποιηθούν για την πραγματοποίηση πολύ πειστικών επιθέσεων Phishing. Σε αντίθεση με τους ανθρώπους, οι επιθέσεις με τεχνητή νοημοσύνη μπορούν να λειτουργούν όλο το εικοσιτετράωρο. Είναι γρήγορα, αποτελεσματικά, οικονομικά και προσαρμόσιμα.

Πώς να αποτρέψετε την επίθεση με τεχνητή νοημοσύνη

Δυστυχώς, δεν υπάρχει απλός τρόπος για την πρόληψη επιθέσεων AI. Φυσικά, η καλή υγιεινή του κωδικού πρόσβασης, οι ισχυροί έλεγχοι πρόσβασης, η παρακολούθηση δικτύου και όλες οι άλλες λύσεις που αναφέρονται παραπάνω, αναμφίβολα θα βοηθήσουν. Ωστόσο, το πρόβλημα με το AI είναι ότι είναι πολύ απρόβλεπτο. Με άλλα λόγια, δεν έχουμε ιδέα τι είδους υπερ-ιοί θα εμφανιστούν τα επόμενα χρόνια και δεν έχουμε ιδέα πώς θα χρησιμοποιηθεί η τεχνητή νοημοσύνη για την καταπολέμησή τους. Το καλύτερο που έχετε να κάνετε είναι να προσέχετε τις λύσεις ασφαλείας που υποστηρίζονται από AI.

15. IoT-Based Attacks

Όπως έχει σήμερα, οι συσκευές IoT είναι γενικά λιγότερο ασφαλείς από τα περισσότερα σύγχρονα λειτουργικά συστήματα και οι χάκερ είναι πρόθυμοι να εκμεταλλευτούν τα τρωτά σημεία τους. Όπως και με την τεχνητή νοημοσύνη, το Διαδίκτυο των πραγμάτων εξακολουθεί να είναι μια σχετικά νέα έννοια, και έτσι δεν έχουμε ακόμη να δούμε ποιες μεθόδους θα χρησιμοποιήσουν οι εγκληματίες του κυβερνοχώρου για να εκμεταλλευτούν συσκευές IoT και με ποιον σκοπό. Ίσως οι χάκερ να στοχεύσουν ιατρικές συσκευές, συστήματα ασφαλείας και έξυπνα θερμόμετρα ή ίσως να επιδιώξουν να υπονομεύσουν συσκευές IoT προκειμένου να εξαπολύσουν επιθέσεις DDoS μεγάλης κλίμακας. Υποθέτουμε ότι θα το μάθουμε στα επόμενα χρόνια.

Πώς να αποτρέψετε τις επιθέσεις IoT

Οι συσκευές IoT είναι συνήθως διασυνδεδεμένες, πράγμα που σημαίνει ότι εάν μια συσκευή παραβιαστεί, είναι πιθανό η επίθεση να εξαπλωθεί σε άλλες συσκευές. Για να γίνουν τα πράγματα χειρότερα, οι συσκευές IoT δεν έχουν σχεδόν καμία ενσωματωμένη ασφάλεια, γεγονός που τις καθιστά τέλειο στόχο για τους αντιπάλους. Εκτός από την εφαρμογή γενικών μέτρων ασφαλείας, θα πρέπει να βεβαιωθείτε ότι αλλάζετε τις προεπιλεγμένες ρυθμίσεις του δρομολογητή, χρησιμοποιείτε ισχυρό και μοναδικό κωδικό πρόσβασης, αποσυνδέετε συσκευές IoT όταν δεν χρησιμοποιούνται και βεβαιωθείτε ότι έχουν εγκαταστήσει τις πιο πρόσφατες ενημερώσεις κώδικα.