Πλοήγηση στο πεδίο του κυβερνοχώρου με ασφάλεια και ενίσχυση των ψηφιακών «οχυρών»

Ελευθέριος Αθουσάκης
Μέντορας ΑΛΛΗΛΟΝ (Τομέα Κυβερνοασφάλειας)
Ειδικός σε θέματα Κυβερνοασφάλειας
Eleftherios A. | Linkedin

Περίληψη

Στον διαρκώς εξελισσόμενο κόσμο της κυβερνοασφάλειας, το 2023 σηματοδότησε ένα κομβικό σημείο. Καθώς τα ψηφιακά σύνορα διευρύνονταν με την αυξανόμενη χρήση Τεχνητής Νοημοσύνης, προέκυπταν νέες προκλήσεις για τους χρήστες της τεχνολογίας, τόσο για τους ιδιώτες όσο και για τις επιχειρήσεις. Σε αυτό το άρθρο εξετάζουμε τις εξελιγμένες επιθέσεις στον κυβερνοχώρο, καθώς και τις τεχνολογικές ανακαλύψεις στον τομέα της ασφάλειας. Δεν είναι απλώς μια αναδρομή στα γεγονότα, είναι ένας καθοδηγητικός φάρος μέσα από την ομίχλη της κυβερνοαβεβαιότητας, προσφέροντας προληπτικά μέτρα και στρατηγική πρόβλεψη. Με την κατανόηση του κυβερνοτοπίου του 2023, οι αναγνώστες γίνονται συμμέτοχοι στη διαμόρφωση ενός πιο ασφαλούς ψηφιακού μέλλοντος.

Ο σιωπηλός πόλεμος στον κυβερνοχώρο

Στην αχανή έκταση του ενός και του μηδέν, μαίνεται ένας σιωπηλός πόλεμος, μια μάχη που δεν διεξάγεται με σπαθιά και ασπίδες, αλλά με γραμμές κώδικα και κρυπτογραφημένους αλγορίθμους. Η κυβερνοασφάλεια, η τέχνη της προστασίας της ψηφιακής μας ύπαρξης, αποτελεί το τελευταίο μας προπύργιο ενάντια σε έναν αόρατο αντίπαλο. Πρόσφατα περιστατικά κατέδειξαν το διακύβευμα: κλεμμένα κρυπτονομίσματα στα οποία κάποιοι ίσως είχαν επενδύσει τους κόπους μιας ζωής, παραβιασμένες εταιρικές "πύλες", με λεία που υπολογίζεται ότι για το 2022 έφτασε τα 8,44 τρισεκατομμύρια Δολάρια Αμερικής **(1)**, και διαρκείς προσπάθειες διείσδυσης σε κρίσιμες υποδομές, όπως συστήματα υγείας, κυβερνητικές υπηρεσίες και εκπαιδευτικά ιδρύματα. Καθώς εμβαθύνουμε στις επιπλοκές αυτού του πολέμου, ας αποκρυπτογραφήσουμε πρώτα το λεξικό της άμυνας στον κυβερνοχώρο μέσα από κάποιες από τις τελευταίες επιθέσεις.

Πρόσφατες επιθέσεις στον κυβερνοχώρο: Μια ματιά στην άβυσσο

1. Κυβέρνηση της Κόστα Ρίκα. Το μέγεθος του "Κάστρου" δεν μετράει

Η κυβέρνηση της Κόστα Ρίκα **(2)** κήρυξε στα τέλη Απριλίου του 2022, κατάσταση έκτακτης ανάγκης μετά από εβδομάδες επιθέσεων Ransomware σε κρίσιμα συστήματά της. Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που κρυπτογραφεί τα δεδομένα ή τη συσκευή του θύματος, καθιστώντας τα μη προσβάσιμα μέχρι να καταβληθούν τα λύτρα τα οποία ο επιτιθέμενος ζητά από το θύμα, απειλώντας ότι θα κρατήσει τα δεδομένα ή τη συσκευή κλειδωμένα. Ως αποτέλεσμα, η κυβέρνηση δεν μπορούσε να πληρώσει εγκαίρως τους εργαζομένους της και τους ζήτησε να υποβάλουν αίτηση πληρωμής μέσω ηλεκτρονικού ταχυδρομείου ή με έντυπες μεθόδους. Η επίθεση διέκοψε επίσης τα φορολογικά και τελωνειακά συστήματα, προκαλώντας την κατάρρευση της εφοδιαστικής αλυσίδας εισαγωγών/εξαγωγών της χώρας. Η συμμορία Conti απαίτησε την καταβολή λύτρων ύψους 20 εκατομμυρίων δολαρίων Αμερικής, ισχυριζόμενη ότι οι επιθέσεις έγιναν για να ανατρέψουν την κυβέρνηση. Η εγκληματική συμμορία δημοσίευσε περίπου το 50% των δεδομένων που εκλάπησαν κατά τη διάρκεια της επίθεσης που διήρκεσε εβδομάδες. Η κυβέρνηση της Κόστα Ρίκα δεν κατέβαλε τα λύτρα. Όπως καταλαβαίνετε κανένα κάστρο, εικονικό ή φυσικό, δεν είναι αδιαπέραστο.

2. Η ληστεία κρυπτονομισμάτων της Crypto.com: Αποκρυπτογράφηση της παραβίασης

Επίσης στις αρχές του 2022, το Crypto.com, ένα από τα μεγαλύτερα κέντρα συναλλαγών κρυπτονομισμάτων, έπεσε θύμα μιας σχολαστικά ενορχηστρωμένης παραβίασης **(3)**. Σχεδόν 500 ψηφιακά πορτοφόλια χρηστών παραβιάστηκαν, με αποτέλεσμα την κλοπή 18 εκατομμυρίων δολαρίων Αμερικής σε Bitcoin και 15 εκατομμυρίων δολαρίων Αμερικής σε Ethereum, δύο από τα πιο γνωστά κρυπτονομίσματα παγκοσμίως. Οι επιτιθέμενοι κατάφεραν και παρέκαμψαν τον έλεγχο ταυτότητας δύο παραγόντων, εκθέτοντας την τρωτότητα ακόμη και των φαινομενικά απόρθητων συστημάτων. Το περιστατικό αυτό χρησιμεύει ως μια υπενθύμιση ότι η επαγρύπνηση είναι η πανοπλία μας και ο εφησυχασμός η αχίλλειος πτέρνα μας.

3. Εθνική Υπηρεσία Υγείας του Ηνωμένου Βασιλείου (NHS)

Το NHS παρέχει υποδομές για δεκάδες χιλιάδες οργανισμούς υγείας. Από τον Απρίλιο του 2022 και σε διάστημα έξι μηνών, μια επίθεση παραβίασε πάνω από 100 λογαριασμούς υπαλλήλων του NHS και τους χρησιμοποίησε για την αποστολή μηνυμάτων ηλεκτρονικού "ψαρέματος" **(4)**. Ορισμένες από τις εκστρατείες phishing, όπως είναι γνωστές, επιχείρησαν να υποκλέψουν διαπιστευτήρια της Microsoft. Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου ήταν κατά κύριο λόγο ψεύτικες ειδοποιήσεις λήψης εγγράφων, συνοδευόμενες από μια δήλωση αποποίησης ευθυνών του NHS στο τέλος κάθε μηνύματος. Ο πόλεμος κατά των απειλών στον κυβερνοχώρο μαίνεται αδιάκοπα, απαιτώντας διαρκή επαγρύπνηση.

4. Η διαρκής πολιορκία της News Corp: Η παραβίαση που αντηχεί στο χρόνο

Η News Corp, ο παγκόσμιος κολοσσός των μέσων ενημέρωσης, αντιμετώπισε παραβιάσεις των διακομιστών του που χρονολογείται ότι ξεκίνησαν από τον Φεβρουάριο του 2020 **(5)**. Η κλίμακα της επίθεσης υπογραμμίζει την επιμονή των κυβερνοεγκληματιών, οι οποίοι συνεχίζουν να εκμεταλλεύονται τα τρωτά σημεία πολύ καιρό μετά την αρχική παραβίαση. Γι' αυτό και οι τακτικοί έλεγχοι ασφαλείας, η διαχείριση ενημερώσεων και η ισχυρή κρυπτογράφηση αποτελούν τα προπύργιά μας απέναντι στους αδυσώπητους αυτούς αντιπάλους.

Επίγνωση της ασφάλειας στον κυβερνοχώρο: Η ασπίδα μας ενάντια στην καταιγίδα

1. Εκπαίδευση και κατάρτιση: Ο φάρος της ανθεκτικότητας

1.1. Μείνετε ενημερωμένοι

Η γνώση είναι η πρώτη γραμμή άμυνάς μας. Μείνετε ενήμεροι για τις αναδυόμενες απειλές μέσω ενημερωτικών δελτίων ασφαλείας, ιστολογίων και διαδικτυακών σεμιναρίων. Κατανοήστε τις τακτικές των εγκληματιών του κυβερνοχώρου, τις τεχνικές ηλεκτρονικού ψαρέματος, τα τεχνάσματα κοινωνικής μηχανικής και τις εκμεταλλεύσεις ευπαθειών άγνωστων μέχρι την ημέρα εύρεσής τους; γνωστές και ως zero-day. **Θυμηθείτε**: η άγνοια είναι σύμμαχός τους - η ευαισθητοποίηση είναι δική μας.

1.2. Προγράμματα κατάρτισης: Η σφυρηλάτηση των Φρουρών

Ενδυναμώστε το προσωπικό σας με εκπαίδευση για την ασφάλεια στον κυβερνοχώρο. Από τη γραμματεία μέχρι τη διοίκηση, ο καθένας παίζει το ρόλο του. Διδάξτε τους να διακρίνουν τα ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, να αναγνωρίζουν τις επικίνδυνες ενδείξεις και να υπερασπίζονται την τήρηση των κανόνων ασφαλείας. Θυμηθείτε, μια καλά εκπαιδευμένη ομάδα είναι το ισχυρότερο αμυντικό προπύργιο ενός οργανισμού.

2. Ισχυροί μηχανισμοί πιστοποίησης: Οχυρώνοντας τις "Πύλες"

2.1. Αυθεντικοποίηση δύο παραγόντων (2FA)

Εφαρμόστε αυθεντικοποίηση δύο παραγόντων όπου είναι εφικτό. Προσθέτει ένα επιπλέον επίπεδο ασφάλειας, απαιτώντας μια δεύτερη μορφή επαλήθευσης πέρα από τους κωδικούς πρόσβασης. Είτε πρόκειται για κωδικό μηνύματος κειμένου είτε για βιομετρική σάρωση, η εφαρμογή της τεχνολογίας 2FA αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση.

2.3. Βιομετρικά στοιχεία: Η υπογραφή του Φύλακα

Αξιοποιήστε τον βιομετρικό έλεγχο ταυτότητας για κρίσιμα συστήματα. Οι σαρώσεις δακτυλικών αποτυπωμάτων, η αναγνώριση προσώπου και τα μοτίβα ίριδας παρέχουν μοναδικά αναγνωριστικά. Δεν ενισχύουν μόνο την ασφάλεια, αλλά και βελτιώνουν την εμπειρία των χρηστών, ένα πλεονέκτημα για τις ψηφιακές μας "εστίες".

3. Τακτικοί έλεγχοι ασφαλείας: Η επαγρύπνηση του Φύλακα

3.1. Δοκιμές διείσδυσης: Αποκάλυψη τρωτών σημείων

Οι ηθικοί χάκερ προσομοιώνουν επιθέσεις που θα εκτελούσαν κακόβουλοι στην υποδομή σας, εξετάζοντας τις άμυνες των συστημάτων σας. Τα ευρήματά τους αποκαλύπτουν πιθανές ρωγμές στη θωράκιση σας. Αντιμετωπίστε τα αμέσως, ο εφησυχασμός προκαλεί συμφορές.

3.2. Διαχείριση διορθώσεων: Σφράγιση σημείων παραβίασης

Οι ενημερώσεις λογισμικού δεν είναι απλώς ενοχλήσεις, είναι ζωτικής σημασίας. Οι διορθώσεις αυτές συχνά αποκαθιστούν ευπάθειες που εκμεταλλεύονται οι επιτιθέμενοι στον κυβερνοχώρο. Η παραμέληση των ενημερώσεων είναι σαν να αφήνετε τις πύλες του "κάστρου" σας μισάνοιχτες.

4. Κρυπτογράφηση δεδομένων και δημιουργία αντιγράφων ασφαλείας

4.1. Κρυπτογράφηση: Η διασφάλιση των "περγαμηνών" μας

Θα πρέπει να γίνεται κρυπτογράφηση ευαίσθητων δεδομένων τόσο κατά τη μετάδοση όσο και κατά την αποθήκευση. Εμπιστευτικά μηνύματα ηλεκτρονικού ταχυδρομείου, οικονομικά αρχεία, πνευματική ιδιοκτησία - όλα αξίζει να επενδυθούν με τον μανδύα της κρυπτογράφησης. Έτσι ακόμα και αν υποκλαπούν, θα παραμείνουν ακατανόητα και άχρηστα για τους κακόβουλους.

4.2. Τακτικά αντίγραφα ασφαλείας: Οι "περγαμηνές" της ανθεκτικότητας

Το Ransomware μπορεί να σας χτυπήσει, αλλά τα αντίγραφα ασφαλείας μπορούν να αποκαταστήσουν τα κρυπτογραφημένα δεδομένα σας χωρίς να χρειαστεί να υποκύψετε σε εκβιασμούς. Δημιουργείστε τακτικά αντίγραφα ασφαλείας των κρίσιμων πληροφοριών. Ο πλεονασμός είναι η ασπίδα μας ενάντια στο χάος.

Η Αποφασιστικότητα του Φύλακα

Καθώς πλοηγούμαστε στα ύπουλα νερά του κυβερνοχώρου, ας λάβουμε υπόψη μας τα λόγια του μεγάλου κρυπτογράφου Bruce Schneier:

"Ο μόνος ασφαλής υπολογιστής είναι αυτός που είναι αποσυνδεδεμένος από την πρίζα, κλειδωμένος σε ένα χρηματοκιβώτιο, και θαμμένος 20 πόδια κάτω από το έδαφος σε μια μυστική τοποθεσία... και δεν είμαι καν πολύ σίγουρος γι' αυτό".

Η επαγρύπνησή μας και η δέσμευσή μας για ευαισθητοποίηση στον τομέα της κυβερνοασφάλειας μπορούν να μεταμορφώσουν αυτό το ζοφερό σενάριο. Ας οχυρωθούμε κατάλληλα.

Πηγές – Βιβλιογραφία

1. https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety
2. Costa Rica State of Emergency Declared After Ransomware Attacks (securityintelligence.com)
3. Crypto.com Admits $35 Million Hack (forbes.com)
4. https://www.netsec.news/113-email-accounts-compromised-in-nhs-phishing-attack/
5. Hack of News Corp Emails Is Believed to Be Linked to China - The New York Times (nytimes.com)

Βιογραφικό

Ο Ελευθέριος Αθουσάκης έχει πάνω από 20 χρόνια συνολικής εμπειρίας στο χώρο των Επικοινωνιών-Πληροφορικής και της ασφάλειας πληροφορίων με πολυετή εμπειρία σε διεθνής οργανισμούς (NATO, ΕΕ).
Είναι κάτοχος MSc στην Ασφάλεια Πληροφοριών και Ηλεκτρονική Εγκληματολογία και μέλος του ISC2 Hellenic Chapter.
Εργάζεται στο Γενικό Επιτελείο Εθνικής Άμυνας.